МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ
ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова
праця на правах рукопису

ГОНЧАР МАКСИМ ВОЛОДИМИРОВИЧ

УДК 327.56:316.472.4(4-672EU)(043.3)

ДИСЕРТАЦІЯ
СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ВПЛИВУ НА ПОЛІТИЧНУ СТАБІЛЬНІСТЬ ТА БЕЗПЕКУ ЄС

052 «Політологія»

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____Гончар М.В

Науковий керівник:
Барановський Фелікс Володимирович,
доктор політичних наук, професор,
професор

Київ, 2026 рік

АНОТАЦІЯ

Гончар М.В. Соціальні мережі як інструмент впливу на політичну стабільність та безпеку ЄС. — Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 052 «Політологія». — Державний торговельно-економічний університет, Київ, 2026.

Сучасний етап розвитку глобального інформаційного суспільства та стрімка цифровізація політичних процесів актуалізують проблему трансформації соціальних мереж із комунікаційних майданчиків на потужний інструмент впливу на політичну стабільність та безпеку міжнародних об'єднань, зокрема Європейського Союзу. Зокрема в роботі визначено особливості «веапонізації» (перетворення на зброю) соціальних мереж, що надає можливість вповні розглядати загрози, які створюють авторитарні режими для європейської безпеки та політичного ладу, використовуючи цифровий простір.

Необхідність вивчення механізмів використання соціальних медіа як засобів гібридної війни, дезінформації та маніпуляції громадською думкою є нагальною для аналізу стійкості демократичних систем у сучасному геополітичному контексті. Дисертація присвячена переосмисленню ролі соціальних мереж у архітектурі безпеки Європейського Союзу. В роботі концептуалізовано феномен «інфраструктурної заплутаності» як фактора обмеження цифрового суверенітету держав ЄС у взаємодії з приватними технологічними гігантами.

Ретроспективний аналіз глобальних загроз, які постають перед ЄС та поступова трансформація європейських безпекових стратегій свідчить про необхідність переосмислення ролі соціальних мереж як однієї з ключових технологій у безпековій сфер. З урахуванням повномасштабного вторгнення Росії в Україну та системного інформаційного тиску з боку авторитарних систем на європейський інформаційний простір особливої актуальності набуває питання здатності ЄС формувати єдину політику захисту свого цифрового суверенітету. Ця необхідність актуалізує проблематику стійкості демократичних інститутів

витримувати атаки алгоритмічної «цифрової зброї» без утрати основоположних цінностей, зокрема свободи слова. Ці питання потребують переосмислення класичних теорій постіндустріального суспільства через призму новітніх концептів «техноавторитаризму» та «мережевої влади». У роботі доведено, що традиційні підходи до вивчення соціальних мереж як засобів міжособистісної взаємодії мають бути доповнені аналізом їхньої ролі в мобілізації протестних рухів («Арабська весна», «Революція Гідності», протести в Гонконзі, тощо) та у поступовому зростанні їх впливу на політичну сферу. В дисертації розглянуті виклики сучасних алгоритмів соціальних мереж, які формують «бульбашки дезінформації», розмиваючи довіру до офіційних інституцій та традиційних медіа. Окремо висвітлена роль нової технологічної еліти та моральні дилеми, викликані архітекторами цих систем. В дисертаційному дослідженні проаналізовано основні етапи формування безпекової політики ЄС у цифровій сфері: від добровільних кроків окремих країн членів ЄС, у регуляції цих медіумів, до поступовог о жорсткого регулювання та санкційних політик, зокрема через Акт про цифрові послуги (DSA).

Визначено особливості національних підходів країн-членів до регулювання соцмереж: від жорсткого юридичного примусу в Німеччині (закон NetzDG) та захисту виборів у Франції до стратегій «психологічної оборони» та медіаграмотності в країнах Балтії, Королівства Швеції. Систематизовано типи «цифрової зброї» (інфраструктурна, психологічна, алгоритмічна, соціальна) та проаналізовано методи їх застосування в сучасних міждержавних конфліктах. Удосконалено розуміння поняття «веапонізація соціальних мереж» у контексті концепції «стовпів підтримки» Джина Шарпа, що дозволяє розглядати інформаційні операції як спосіб руйнування легітимності демократичних режимів без прямого застосування військової сили. На основі аналізу досвіду наявного досвіду європейських країн запропоновано модель «цифрової громадянської оборони», яка передбачає напрацювання спроможності громадян «відмовляти у співпраці» кампаніям з дезінформації в соціальних мережах.

Практичне значення результатів дослідження полягає у визначенні факторів, що впливають на вразливість демократичних систем до зовнішніх інформаційних атак, та розробці рекомендацій для зміцнення стратегічних комунікацій у країнах, що перебувають під гібридним тиском.

Отримані результати надають можливості їх інтеграції в політики оборонних стратегій та при розробці політик у сфері інформаційного безпеки.

Актуальність проведеного дослідження відповідає критичним викликам сучасної політології та міжнародних відносин в умовах глобального протистояння демократичних та авторитарних систем. Дослідження створює підґрунтя для розробки довгострокових стратегій захисту демократії від «гострої сили» автократій та сприяє формуванню нового концепту цифрової безпеки як невід'ємної складової національної безпеки сучасної держави.

Ключові слова: соціальні мережі, цифрова стійкість, політична безпека, інформаційна безпека, Європейський Союз, цифрова оборона, гібридні загрози, війна, стала демократія, керована демократія, інформаційні операції, дезінформація, пропаганда, кібербезпека, веапонізація.

SUMMARY

Honchar M.V. Social networks as an instrument of influence on the political stability and security of the EU. — Qualification scientific work on the rights of a manuscript. Dissertation for the degree of Doctor of Philosophy in specialty 052 «Political Science». — State University of Trade and Economics, Kyiv, 2026.

The current stage of the global information society's development and the rapid digitalization of political processes underscore the transformation of social networks from mere communication platforms into a powerful tool for influencing the political stability and security of international unions, specifically the European Union. This research identifies the features of the «weaponization» of social networks, which allows for a comprehensive examination of the threats posed by authoritarian regimes to European security and the political order through the exploitation of digital space. The necessity of studying the mechanisms of using social media as instruments of hybrid warfare, disinformation, and public opinion manipulation is urgent for analyzing the resilience of democratic systems within the contemporary geopolitical context.

This dissertation is devoted to redefining the role of social networks in the security architecture of the European Union. The study conceptualizes the phenomenon of «infrastructural entanglement» as a factor limiting the digital sovereignty of EU member states in their interaction with private technological giants. A retrospective analysis of global threats facing the EU and the gradual transformation of European security strategies demonstrate the need to rethink the role of social networks as a key technology in the security sphere. Given Russia's full-scale invasion of Ukraine and the systemic informational pressure from authoritarian systems on the European information space, the question of the EU's ability to form a unified policy for protecting its digital sovereignty becomes particularly relevant. This necessity highlights the issue of democratic institutions' resilience in withstanding attacks from algorithmic «digital weapons» without compromising fundamental values, such as freedom of speech. These issues require a re-evaluation of classical theories of post-

industrial society through the lens of emerging concepts like «techno-authoritarianism» and «network power.»

The work proves that traditional approaches to studying social networks as means of interpersonal interaction must be supplemented by an analysis of their role in mobilizing protest movements (e.g., the Arab Spring, the Revolution of Dignity, protests in Hong Kong) and their growing influence on the political sphere. The dissertation examines the challenges of modern social media algorithms that create «disinformation bubbles,» eroding trust in official institutions and traditional media. The role of the new technological elite and the moral dilemmas posed by the architects of these systems are highlighted separately.

The research analyzes the main stages of the EU's security policy formation in the digital sphere: from voluntary steps by individual member states in regulating these media to gradual «hard» regulation and sanction policies, notably through the Digital Services Act (DSA). The study identifies the specifics of national approaches of member states toward regulating social networks: from strict legal enforcement in Germany (the NetzDG law) and election protection in France to strategies of «psychological defense» and media literacy in the Baltic states and the Kingdom of Sweden.

The types of «digital weapons» (infrastructural, psychological, algorithmic, social) are systematized, and the methods of their application in modern interstate conflicts are analyzed. The understanding of the concept of «weaponization of social networks» is refined within the context of Gene Sharp's «pillars of support» concept, which allows for viewing information operations as a means of undermining the legitimacy of democratic regimes without the direct use of military force. Based on the existing experience of European countries, a model of «digital civil defense» is proposed, which involves developing the capacity of citizens to «refuse cooperation» with disinformation campaigns on social networks.

The practical significance of the research results lies in identifying factors that influence the vulnerability of democratic systems to external information attacks and developing recommendations for strengthening strategic communications in countries

under hybrid pressure. The results obtained provide opportunities for their integration into defense strategies and the development of policies in the field of information security.

The relevance of the conducted research aligns with the critical challenges of modern political science and international relations amidst the global confrontation between democratic and authoritarian systems. The study establishes a foundation for developing long-term strategies to protect democracy from the «sharp power» of autocracies and contributes to the formation of a new concept of digital security as an integral component of a modern state's national security.

Keywords: social media, digital resilience, political security, information security, European Union, digital defense, hybrid threats, warfare, sustainable democracy, managed democracy, information operations, disinformation, propaganda, cybersecurity, weaponization.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях:

1. Гончар М. В. Вплив соціальних мереж на політичну стабільність та національну безпеку: досвід Королівства Швеція / М. В. Гончар // Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методики викладання соціально-політичних дисциплін. – 2023. – Вип. 33. – С. 54–63. – URL: https://enpuir.udu.edu.ua/entities/publication/bf3f2944-179a-4200-ada6-8e4e152e2239
2. Гончар М. В. Вплив соціальних мереж на політичні системи у контексті суперництва демократичних та авторитарних режимів / М. В. Гончар // Політикус : наук. журнал. – 2024. – № 5. – С. 11–18. – URL: http://dspace.pdpu.edu.ua/bitstream/123456789/21502/1/Social%20networks%20impact%20on%20political%20systems%20in%20the%20context%20of%20the%20democratic%20and%20authoritarian%20regimes%20competition.pdf
3. Гончар М. В. Між згодою та спротивом: адаптація теорії Джина Шарпа для протидії цифровим загрозам у Європейському Союзі / М. В. Гончар //

Український політико-правовий дискурс. – 2025. – № 17. – DOI: https://doi.org/10.5281/zenodo.17839092

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Гончар М. В. Проблематика самоорганізації суспільства у соціальних мережах. Політичний вимір / М. В. Гончар // Проблематика самоорганізації суспільства у соціальних мережах : тези доп. Всеукр. наук.-практ. конф. (Київ, 24 листоп. 2022 р.) / відп. ред. А. Кравченко. – Київ : Держ. торг.-екон. ун-т, 2022. – С. 160–164.
2. Гончар М. В. Європейський союз як постачальник глобальної безпеки. Відродження забутої ідеї / М. В. Гончар // Європейський союз як постачальник глобальної безпеки : тези доп. Всеукр. наук.-практ. конф. (Київ, 16 листоп. 2023 р.) / відп. ред. Н. В. Крохмаль. – Київ : Держ. торг.-екон. ун-т, 2023. – С. 191–195.
3. Гончар М. В. Революція даних. Цифрове майбутнє та сьогодення / М. В. Гончар // Революція даних. Цифрове майбутнє та сьогодення : тези доп. Міжнар. наук.-практ. конф. (Київ, 11 квіт. 2024 р.) / відп. ред. А. Кравченко. – Київ : Держ. торг.-екон. ун-т, 2024. – С. 223–227.
4. Гончар М. В. Цифровий вимір глобальної безпеки: непомітні революції / М. В. Гончар // Політичні трансформації сучасного суспільства : зб. матеріалів V Всеукр. наук.-практ. конф. (Полтава, 22 лют. 2024 р.). – Полтава : ПДАУ, 2024. – С. 148–152.
5. Гончар М. В. Соціальні мережі як виклик для української демократії / М. В. Гончар // Україна в умовах російської агресії: уроки сьогодення та прогнози майбутнього : матеріали Всеукр. наук.-практ. конф. (XXXVIII Харків. політол. читань) (Харків, 27 груд. 2024 р.) / Аналіт. центр сучас. гуманітаристики; Харків. асоц. політологів. – Харків : Право, 2025. – С. 24–28.
6. Гончар М. В. Соціальні мережі та демократичний виборчий процес: сучасні тенденції / М. В. Гончар // Фундаментальні та прикладні проблеми суспільства: історія, сьогодення, майбутнє [Електронний ресурс] : тези доп.

ІІ Міжнар. наук.-практ. конф. (Київ, 17 квіт. 2025 р.) / відп. ред. А. Кравченко. – Київ : Держ. торг.-екон. ун-т, 2025. – С. 339–344.

ЗМІСТ

ВСТУП

Актуальність дослідження. На сучасному етапі розвитку глобального інформаційного суспільства та стрімкої цифровізації політичних процесів соціальні мережі перестали бути суто комунікаційними майданчиками. Сьогодні вони трансформувалися у потужний інструмент впливу на політичну стабільність та безпеку міжнародних об'єднань, зокрема Європейського Союзу. У контексті глобального протистояння демократичних та авторитарних систем соціальні медіа дедалі частіше використовуються як засоби гібридної війни, дезінформації та стратегічної маніпуляції громадською думкою.

Процес «веапонізації» (перетворення на зброю) цифрового середовища створює прямі екзистенційні загрози демократичному ладу європейських держав. Європейський Союз, зіштовхнувшись із системним інформаційним тиском з боку Російської Федерації та КНР, а також із викликами внутрішньої поляризації суспільства, вимушений форсовано розробляти нові стратегії захисту власного цифрового суверенітету. Повномасштабне вторгнення Росії в Україну у 2022-му році остаточно довело, що інформаційні операції в соціальних мережах є невід'ємною частиною сучасної збройної агресії, що спрямована на руйнування основних стовпів, на яких ґрунтуються демократичні відкриті системи: дестабілізацію суспільної свідомості, підрив довіри до легітимності влади, підсилення скепсису щодо демократичних процесів.

Актуальність теми посилюється появою нових форм «техноавторитаризму», де алгоритми соціальних мереж та платформ стають інструментом впливу, що імітують підходи, якими керуються сталі демократичні суспільства. Незважаючи на активну розробку європейськими інституціями законодавчих механізмів, таких як Акт про цифрові послуги (DSA) та «Стратегічного компасу», залишається відкритою проблема ефективності цих заходів та пошуку балансу між колективною безпекою та фундаментальними цінностями свободи слова.

Особливого значення набуває адаптація класичних теорій ненасильницького спротиву та безпекових стратегій минулого (періоду Холодної війни) до умов сучасної цифрової ери. Україна, перебуваючи під постійним гібридними загрозами, вже володіє унікальним практичним досвідом протидії алгоритмічній «цифровій зброї». Інтеграція цього досвіду в безпекову політику ЄС та розробка моделі «цифрової громадянської оборони», що поєднує технологічний захист із соціальною та психологічною стійкістю суспільства, є критично важливою для забезпечення стабільності всього євроатлантичного регіону.

Проблему впливу інформаційних технологій та мережевих структур на трансформацію політичних систем досліджували такі засновники теорії постіндустріального суспільства, як Д. Белл, Е. Тоффлер, П. Друкер та М. Мак-Люен. Вагомий внесок у розуміння архітектури мережевого суспільства та «мережевої влади» зробили М. Кастельс, Дж. Рамо, М. Грановеттер, С. Мілграм, а також математики П. Ердос та А. Реньї.

Процеси демократичних транзитів та ризики «відкатів» в умовах цифрової доби розглядаються через призму праць С. Гантінгтона, Ф. Шміттера, Д. Маркоффа та Ф. Фукуями. Феномен «веапонізації» соціальних мереж та їх використання як «цифрової зброї» перебуває у центрі уваги П. Сінгера, Е. Брукінга, Е. Лукаса, П. Померанцева, М. Ґалеотті, а також К. Вокера та Дж. Людвіг, які запровадили концепт «гострої сили». Ризики алгоритмічного контролю та загрози «техноавторитаризму» для демократії досліджують Ю. Н. Харарі, Ш. Зубофф, Р. Макнамі та Е. Лафранс. Питання безпеки ЄС, протидії дезінформації та формування стратегічних комунікацій аналізують Т. Уайт, С. Гарольд, А. Полякова та Д. Фрід.

Морально-етичний вимір та соціальні наслідки мережевої комунікації розкриваються у працях Ю. Габермаса, С. Коена, П. Бергера, Т. Лукмана та П. Брюкнера.

Серед українських дослідників вагомий внесок у вивчення гібридних загроз, стратегічних комунікацій та політичних трансформацій зробили Д.

Дубов, О.Кондратенко, Г. Почепцов, С. Даниленко, С. Віднянський, А. Чайковський, О. Романюк. Проблематика новітніх цифрових платформ та того як вони стають інструментами «гібридної» боротьби та які виклики це ставить перед фахівцями з комунікацій розкрита в роботах І. Пронози та Новакової О. Питання віртуалізації політичного простору, функціонування соціальних медіа та мережевої взаємодії перебувають у центрі уваги О. Дзьобаня, А. Данька, а також Н. Гусєвої та Н. Шуст, чиї праці дозволяють глибше розкрити соціокомунікативний потенціал цифрових платформ.

Зв'язок дослідження з науковими програмами, планами, темами. Дисертаційну роботу виконано відповідно до плану науково-дослідної роботи кафедри філософії, соціології та політології Державного торговельно-економічного університету. Результати дослідження відображені у темах НДР: «Геополітичний порядок у XXI ст. в умовах пост-ковіду», номер державної реєстрації – 0122U200187, «Сучасні виклики демократії: український, європейський та глобальний виміри», номер державної реєстрації – 0125U001350.

Об'єкт дослідження. Процес використання соціальних мереж як інструменту політичного впливу в сучасному цифровому середовищі.

Предмет дослідження. Теоретико-методологічні засади та практичні механізми впливу соціальних мереж на політичну стабільність та формування безпекової політики Європейського Союзу.

Мета та завдання дослідження. Метою дослідження є визначення ролі соціальних мереж як інструменту впливу на політичну стабільність та безпеку ЄС, а також обґрунтування необхідності випрацювання моделі цифрової стійкості демократичних систем в умовах гібридних загроз.

Завдання дослідження:

1. Проаналізувати еволюцію теоретичних підходів до вивчення соціальних мереж у контексті інформаційного суспільства.
2. Дослідити лінгво-комунікаційну парадигму соціальних медіа як політичного інструменту.

3. Провести ретроспективний аналіз глобальних загроз ЄС у цифровому середовищі та еволюції безпекових стратегій (від «Маастрихту» до «Стратегічного компасу»).
4. Розкрити морально-етичний вимір впливу алгоритмів соціальних медіа на політичні кризи та соціальне напруження.
5. Систематизувати типи «цифрової зброї» (інфраструктурна, психологічна, алгоритмічна).
6. Проаналізувати національні підходи країн ЄС (Німеччини, Франції, Швеції, Естонії) до регулювання соцмереж.
7. Оцінити ефективність регуляторних механізмів ЄС, зокрема Акту про цифрові послуги (DSA).
8. Адаптувати теорію «стовпів підтримки» Джина Шарпа до умов цифрового середовища.
9. Розробити модель «цифрової громадянської оборони» на основі досвіду та країн Балтії та Швеції.

У дослідженні висувається гіпотеза, що стабільність сучасних демократій в умовах «веапонізації» соцмереж залежить не лише від жорсткого юридичного регулювання, а від здатності держави сформувати систему «цифрової громадянської оборони», де соціальна стійкість суспільства є ключовим запобіжником проти маніпуляцій.

Методи дослідження. У роботі використано: метод системного аналізу — для вивчення безпекової архітектури ЄС; порівняльний аналіз — для зіставлення національних моделей регулювання соцмереж; ретроспективний метод — для вивчення генези безпекових стратегій; моделювання — для розробки концепту цифрової оборони; соціологічний аналіз — на основі даних індексів довіри та звітів (Edelman Trust Barometer, Freedom House).

Інформаційна база дослідження — нормативно-правові акти ЄС (GDPR, DSA, Стратегічний компас), доповіді міжнародних організацій, аналітичні звіти RAND Corporation, CEPA, а також результати власних публікацій автора.

Наукова новизна результатів дослідження. У дослідженні вперше:

- Здійснено ретроспективний аналіз безпекової політики Європейського Союзу, у межах якого виокремлено перехід від сприйняття соціальних мереж технологій як простору свободи та інструменту демократизації (1990-ті – 2010-ті рр.) до їх визначення як інструменту геоплитичного протистояння. Виявлено, що повномасштабне вторгнення Росії в Україну стало каталізатором переосмислення політик щодо соціальних мереж в ЄС.
- Проведено порівняльний аналіз національних підходів країн-членів ЄС до регулювання соціальних мереж та визначені засадничі відміннності в безпекових моделях: виокремлено модель жорсткого юридичного примусу (Німеччина), судового захисту виборчих процесів (Франція) та «психологічної оборони» з акцентом на включення кожного громадянина у (країни Балтії, Швеція).
- Доведено, що стратегія «вічної оборони» та «гасіння пожеж» у цифровому просторі є завідомо програшною для демократичних систем, оскільки вона дозволяє агресору постійно володіти ініціативою. Аргументовано, що демократичні держави мають легітимне право на проведення активних заходів-відповідей та наступальних інформаційних операцій для захисту власного цифрового суверенітету.
- Розроблено трирівневу модель «цифрової громадянської оборони», де безпека забезпечується через:

1. Індивідуальну неспівпрацю: культивація медіагігієни як відмови громадяними бути «провідником» ворожих або шкідливих наративів.
2. Мережеву солідарність: створення горизонтальних альтернативних каналів комунікації, незалежних від алгоритмічних маніпуляцій приватних платформ.
3. Інституційну готовність: інтеграцію досвіду волонтерських та OSINT-спільнот у державні оборонні доктрини (на основі унікального досвіду України).

- Систематизовано типи «цифрової зброї»: проведено класифікацію інструментів впливу за характером ураження (інфраструктурна, психологічна,

алгоритмічна та соціальна), що дозволяє державам готувати специфічні та пропорційні сценарії відсічі для кожного типу загрози.

- Визначено феномен «інфраструктурної заплутаності»: розкрито механізми, за яких критична залежність державних інституцій від приватної цифрової інфраструктури (Amazon, Google, Starlink) розмиває державний суверенітет і потребує нових форм «спільного регулювання».

Удосконалено:

- Розуміння поняття «веапонізація соціальних мереж»: воно розширене від простого поширення пропаганди до системного процесу руйнування «стовпів підтримки» демократичного ладу (легітимності, авторитету, довіри) через алгоритмічне маніпулювання когнітивним простором громадян.
- Уточнено концептуальні засади техноавторитаризму, який розглядається як специфічна форма політичного домінування цифрових еліт. Доведено, що через доктрину «техноoптимізму» відбувається легітимізація втручання приватних корпорацій у ціннісно-нормативну сферу суспільства. Обґрунтовано, що наслідком цього є виникнення «алгоритмічної тиранії» — системи прихованого управління суспільною поведінкою, яка функціонує поза межами демократичного контролю та національного суверенітету урядів.
- Періодизацію безпекової політики ЄС: виокремлено перехід від сприйняття цифрових технологій як суто економічного ресурсу (1990-ті – 2010-ті) до їх визначення як фронтиру глобального геополітичного протистояння в рамках стратегії «Стратегічного компасу. Запропонований поділ дозволяє простежити трансформацію підходів ЄС до регуляції соціальних мереж, яка полягає у поступовому відході від стратегії ліберального саморегулювання та пасивного спостереження до моделі в якій соціальні мережі розглядаються як критична інфраструктура політичної стабільності, що потребує переосмислення безпекових стратегій та розробку оновлених політик для сфери соцмереж.

Набуло подальшого розвитку:

- Дістала подальшого розвитку концепція «гострої сили» (sharp power) авторитарних режимів. На відміну від існуючих підходів, фокус зміщено на

інструменталізацію демократичної відкритості європейських суспільств. Проаналізовано, що операції «hack-and-leak» та алгоритмічне створення «інформаційних бульбашок» є не просто дезінформацією, а специфічною формою експлуатації правових і етичних норм ЄС з метою дестабілізації стійкості союзу та деструктивного впливу на демократичні процеси.

- Здійснено критичний аналіз правозастосування Акту про цифрові послуги (DSA). Виявлено та обґрунтовано парадигмальний перехід від моделі добровільного саморегулювання платформ до режиму жорсткої юридичної відповідальності. Аргументовано, що цей перехід є ключовим інструментом для цифрового публічного простору, який дозволяє державі повернути контроль над безпековими аспектами функціонування соціальнх мереж, що раніше належали виключно приватним корпораціям.
- Обґрунтовано зміну ролі Європейського Союзу «постачальника безпеки» у глобальному вимірі. Доведено, що в умовах мережевого протистояння стабільність євроатлантичного регіону неможлива в межах ізоляціоністської оборони. Запропоновано концепцію експорту цифрової стійкості, згідно з якою ЄС має перейти до проактивного просування власних наративів у глобальних мережах як єдиного способу зберігати стійкість демократичних процесів в умовах протистояння авторитарних та демократичних систем.

Теоретичне значення дослідження полягає у розширенні наукових уявлень про механізми впливу цифрових технологій на політичну стабільність та безпеку міжнародних організацій.

Практичне значення результатів — можливість використання рекомендацій для розробки стратегій захисту виборчих процесів, зміцнення медіаграмотності та впровадження нових протоколів цифрової безпеки в Україні та країнах ЄС.

Апробація результатів. Основні положення дослідження доповідалися і обговорювалися на всеукраїнських та міжнародних конференціях: Всеукраїнська науково-практична конференція «Соціокультурні трансформації та геополітичні виклики в умовах багатополярного світу» (Київ, ДТЕУ, 24 листоп. 2022 р.),

Всеукраїнська науково-практична конференція «Соціокультурні засади економіки і політики: взаємозв'язки, тренди, суперечності» (Київ, ДТЕУ, 16 листоп. 2023 р.), V Всеукраїнська науково-практична конференція «Політичні трансформації сучасного суспільства» (Полтава, ПДАУ, 22 лют. 2024 р.), Міжнародна науково-практична конференція «Фундаментальні та прикладні проблеми суспільства: історія, сьогодення, майбутнє» (Київ, ДТЕУ, 11 квіт. 2024 р.), Всеукраїнська науково-практичній конференція (XXXVIII Харківські політологічні читання) «Україна в умовах російської агресії: уроки сьогодення та прогнози майбутнього» (Харків, 27 груд. 2024 р.) та II Міжнародна науково-практична конференція «Фундаментальні та прикладні проблеми суспільства: історія, сьогодення, майбутнє» (Київ, ДТЕУ, 17 квіт. 2025 р.).

Особистий внесок здобувача. Всі представлені наукові результати отримані автором самостійно (100% особистого внеску).

Публікації. За результатами дослідження підготовлено 9 публікацій: 3 наукові статті у фахових виданнях України (включно з Index Copernicus) та 6 тез доповідей на наукових конференціях.

Структура й обсяг роботи

Проблеми, які стали об’єктом даного дослідження, визначили логіку і структуру роботи. Дисертація складається із вступу, трьох розділів (які поділяються на 6 підрозділів), загальних висновків, списку використаних джерел. Список використаних джерел містить 250 позицій. Загальний обсяг дисертації становить 226 сторінок, основна частина дисертації — 183 сторіноки.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПІДХОДІВ ДО ВИВЧЕННЯ СОЦІАЛЬНИХ МЕРЕЖ ЩОДО ЇХНЬОГО ВПЛИВУ НА ПОЛІТИЧНУ СТАБІЛЬНІСТЬ ТА БЕЗПЕКУ ЄС

У розділі досліджується трансформація соціальних мереж: від теоретичних моделей «інформаційного суспільства» XX століття до їхньої сучасної ролі як передової лінії глобального протистояння. Розділ демонструє постовий перехід від ідеї первинного оптимізму щодо «цифрової свободи» поступово поступився місцем усвідомленню нових екзистенційних загроз. На основі ретроспективного огляду — від кібератак на Естонію у 2007 році до сучасних гібридних кампаній — розкрито механізми, за допомогою яких авторитарні режими (зокрема РФ та КНР) використовують алгоритми соціальних платформ для розмивання ідентичностей та підриву стійкості демократичних систем в Європейському Союзі.

1.1 Лінгво-комунікаційна парадигма соціальних мереж як політичного інструменту

Джерело появи соціальних мереж, ймовірно, варто шукати в природі індустріального – інформаційного суспільства. Активну роль в розробці сучасної теорії соціальних комунікацій відіграли Д. Белл, М. Кастельс, Е. Тоффлер, П. Друкер та ін. Сам термін «постіндустріальне суспільство» вперше ми знаходимо в працях Д. Белла з 1959-го року. Визначальним в його дослідженнях був той аргумент, що старі індустріальні потуги поступово втрачають свою важливість в житті суспільства. Натомість головну роль в житті соціуму починають займати технології та наука. Ці структурні зміни впливають на сам характер соціальних комунікацій, в яких тепер цінністю стає одиниця інформації (Bell, 1976). Виробництво, машинобудування та промисловість в цілому відходять на інший

план, а обмін, пошук та синтез інформації визначає життя людей, їхні доходи та особливості міжперсональної взаємодії.

На думку Д. Белла, новий уклад у постіндустріальному суспільстві буде побудований на знаннях, котрі штовхатимуть вперед технологічний прогрес. Виникнення епохальних інновацій в такій системі буде органічним процесом, котрий підштовхуватимуть висококласні фахівці та спеціалісти. В питанні дослідження соціальних мереж цікавими є тези Белла про те, що у новому суспільстві електронні засоби організації знань, їх поширення та ретрансляції будуть пріоритетними. Це, у свою чергу, ймовірно, викликатиме проблеми із контролем технологій з виробництва інформації (Raban,2011).

Помітним прихильником розробки концепції інформаційного суспільства є Е. Тоффлер. У 1970-х і 1980-х роках основоположні роботи Тоффлера, зокрема «Шок майбутнього», «Третя хвиля», підкреслювали ключову роль інформації в суспільстві. Тоффлер широко використовував термін «інформаційне суспільство» у своєму дискурсі (Тоффлер, 1996).

Формальна стандартизація терміну «інформаційне суспільство» відбулася в 1992-му році – його почали вживати американські політики. Ця концепція набула популярності та отримала помітне визнання. Крім того, у 1994-му році з’явилося всеосяжне визначення інформаційного суспільства, яке належить Європейській Комісії. Це визначення передбачає, що результатом діяльності такого суспільства є послуги, які поширюються через інформаційні технології та комп’ютерні системи, причому Інтернет стає головною технологією сучасності.

Таким чином, ми бачимо, що в економічній структурі суспільства відбуваються зміни, пов’язані з розподілом трудових ресурсів. Очевидною стає повсюдна важливість інформаційних технологій та їх широке визнання в суспільстві. Різноманітні професії нині є залежними від рівня володіння комп’ютерними та комунікаційними технологіями. Постійне зростання кількості комп'ютерів на душу населення в усьому світі є ще однією помітною тенденцією. Уряди багатьох країн активно підтримують розвиток передових комп’ютерних технологій і вбачають в цьому потенційні вигоди для своїх держав (Martin, 2016).

Якщо дослідити сучасні соціальні мережі, які є продуктом інформаційного суспільства, з точки зору Д. Белла, ми змушені будемо визнати, що вони стали великою базою даних, котрі містять кластери найрізноманітнішої інформації про своїх користувачів. Активна взаємодія користувачів та «цифровий слід», котрий лишається в мережі, дозволяє зовнішнім акторам впливати на поведінку, уподобання та життя цілих суспільств чи великих систем: держав, союзів та блоків.

Важливим є і той факт, що соціальні мережі постійно розвиваються, змінюють свою функціональну суть. Дослідники, котрі намагалися осмислити природу соціальних мереж в часи їх розквіту, розглядали їх скоріше як комунікаційний інструмент, не розглядаючи їх з точу зору впливу на політику чи суспільство. В працях Бойда та Еллісона соціальні мережі описані як інструмент, що дозволяє створювати персональні облікові записи, встановлювати контакти та стійкі зв’язки з іншими користувачами та формувати групи, з якими користувачі перебувають у соціальному зв’язку (Boyd, 2007). Такий підхід до вивчення соціальних мереж, вірогідно, був перенесений із соціології, адже сам термін «соціальна мережа» ми знаходимо у дослідника Д. Барнса вперше у 1954-му році. Барнс досліджував невеликі норвезькі общини, намагаючись встановити взаємозв’язки між конкретною людиною та колом її друзів. Схематично це можна зобразити як систему, в якій всі контакти людини перетинаються в певних точках, зв’язуючи їх між собою (Barnes, 1954).

Дослідження соціальних стосунків у людських групах почалося наприкінці XIX століття – початку XX століття. Перед появою Інтернету вивчення мережевих структур переважно входило до кола зацікавлень соціологів і філософів, особливо Еміля Дюркгейма та Георга Зіммеля. Філософи досліджували взаємопов’язані між собою соціальні структури людських спільнот, які ще не були переплетені з онлайн-середовищем, заклавши тим самим перші, базові принципи аналізу соціальних мереж. У ту епоху філософи та соціологи часто використовували термін «мережі відносин».

Одним із класиків досліджень мережевих спільнот став Дж. Морено, який у 1930-х роках виконав серію соціометричних досліджень, присвячених міжособистісним і міжгруповим стосункам. Морено представив новаторську соціологічну методологію, відому як соціограми, яка графічно окреслює взаємозв'язки між окремими людьми та різними соціальними групами. Дослідження Морено було обґрунтовано показовими експериментами, один з яких передбачав розподіл дітей у дитячому будинку на основі їхніх уподобань. Застосовуючи методологію опитування, дослідник збирав побажання щодо спілкування, співжиття тощо. Згодом були побудовані матриці на основі цих уподобань для кожного члена спільноти та розраховані їх індивідуальні індекси. Для зображення цих уподобань використовувалися схематичні діаграми, які з'ясовували «структуру» уподобань у групі за допомогою стрілок (Hale, 2009).

Пізніше, в середині 20-го століття, Пол Ердос і Альфред Реньї використовували математичні моделі для пояснення фундаментальних принципів, які керують появою соціальних мереж. Вчені запровадили концепцію стохастичних «графів» і ефективно використали її потенціал для формулювання методологій, здатних окреслювати складні соціокультурні структури без потреби в чітких, заздалегідь визначених принципах (Erdos & Renyi, 1960)

В 1970-х роках американський соціолог Марк Грановеттер розпочав емпіричні дослідження динаміки соціальних мереж з особливим наголосом на практичних контекстах зайнятості. Його емпіричні дослідження розкрили ключову роль, яку відіграють «слабкі» зв'язки — знайомі, колеги чи друзі друзів — у гобелені суспільства. Ці «слабкі» зв'язки мали більш суттєвий вплив, ніж «сильні» соціальні зв'язки, характерними для яких є спорідненість чи близька дружба. Грановеттер прискіпливо досліджував прямий зв'язок між близькістю соціальних зв'язків і швидкістю поширення інформації, зрештою встановивши, що інформація поширюється швидше через ці «слабкі» соціальні зв'язки (Granovetter. 1973).

Для глибокого розуміння базових механізмів, що керують сучасними цифровими соціальними мережами, важливими є і дослідження зі сфери

психології. У 1969 році американські психологи Стенлі Мілграм і Джеффрі Треверс запропонували теорію «шести ступенів поділу» або «теорії шести рукостискань», постулюючи, що в середньому будь-які дві людини на Землі пов’язані лише п’ятьма проміжними ступенями взаємного знайомства, що дало початок концепції шести ступені поділу (Travers & Milgrem, 1969). Ця концептуальна основа демонструє принципи, що керують формуванням потенційних зв’язків користувачів у сучасних соціальних мережах, а також дає змогу усвідомити, наскільки ефективною може бути суспільна мобілізація та гуртування в них. Мілграм і Треверс обґрунтували свою теорію за допомогою практичного експерименту, який передбачав розповсюдження 300 конвертів серед жителів Омахи, з чітким застереженням, що ці конверти можуть проходити лише через посередників, відомих відправнику. Експериментальні результати емпірично підтвердили теорію, підтвердивши в середньому п’ять посередників, які долають розрив між відправником і одержувачем. Паралельні експерименти, включно з експериментом, проведеним у 1998 році в Колумбійському університеті з використанням електронної пошти як середовища комунікації, постійно підтверджували уявлення про те, що приблизно 4,74 ступеня поділу розділяють будь-яких двох користувачів.

У світлі розвитку Інтернет-технологій і швидких темпів технологічного прогресу вивчення мережевих структур суспільства поступово перейшло зі сфери філософії та соціології в область інформатики. Ця зміна парадигми позиціонує мережеву структуру як центральну та ключову концепцію в наукових дослідженнях Мануеля Кастельса. Кастельс у своєму аналітичному дослідженні сучасних способів комунікації бачить появу «мережевих» структур як визначальну характеристику нашого глобалізованого суспільства. У рамках теоретичної бази Кастельса поняття «мережева структура» та «мережева культура» набувають першочергового значення (Castells, 2000).

Кастельс підкреслює, що «мережі являють собою відкриті конфігурації, які піддаються необмеженому розширенню шляхом включення нових вузлів, за умови, що вони володіють здатністю до зв’язку». Слід зазначити, що

першочергова роль соціальних мереж полягає в тому, щоб вони слугували провідниками для розподілу головного ресурсу сучасного суспільства – інформації. За словами Кастельса, логіка, що лежить в основі «мереж», стимулює трансформаційні зрушення не лише в сферах праці та виробництва, але також справляє глибокий вплив на різні сфери поведінки суспільства, охоплюючи повсякденне життя, культуру та динаміку взаємодії уряду та суспільства.

Окрім того, він обґрунтовує тезу про те, що історія цивілізації розділяється на три фази: аграрну, індустріальну та інформаційну. Основною рисою інформаційного етапу розвитку суспільства є поділ на дві «касти» – тих, хто має доступ до мережі та тих, хто цього доступу позбавлений. Схожа нерівність пролягає і між державами, адже їхній ступінь володіння інформаційними технологіями визначає пріоритет країни у світових економічних процесах. Кастельс стверджує, що загальний соціальний ландшафт поступово перетворюється на «мережеву» конфігурацію, а самі соціальні мережі не є суто новою конструкцією, яка виникла внаслідок появи мереж на основі Інтернету; радше, вони становлять органічну частину організації людських спільнот. Науковий внесок Мануеля Кастельса надзвичайно важливий, адже він, фактично, є першопрохідцем у теоретичному обґрунтуванні повсюдної присутності мережевої логіки, що лежить в основі аналізу різноманітних соціальних процесів і явищ (Castells, 2007).

Також в 1998-му році Стівен Строгатц і Дункан Воттс представили математичну модель, відому як теорія «малого світу». Їхнє дослідження емпірично продемонструвало, що включення обмеженої кількості випадкових з’єднань у соціальні мережі ефективно зменшило загальний діаметр мережі. Ця математична перевірка підтвердила теорію «шести ступенів поділу», яка у повній мірі узгоджується з мережевою моделлю «малого світу» (Watts & Strogatz, 1998). Ця теоретична основа служить путівником для інженерів і розробників соціальних мереж та цифрових платформ, допомагаючи їм у ретельному проєктуванні процесу підбору рекомендованих контактів для користувачів. Коли новий користувач реєструється та надає особисту інформацію, соціальна мережа

завчасно пропонує підбірку потенційних знайомих, часто на основі контактів електронної пошти, спільних інтересів або професійної приналежності. Користувачі, таким чином, наділені здатністю одразу зв'язуватися з особами, з якими вони, швидше за все, будуть брати участь у істотних і значущих взаємодіях.

Після свого поширення Інтернет досить активно почав проникати в сферу політичного, впливаючи на практики політичних комунікацій. Він пропонує унікальні можливості для прямого та інтерактивного спілкування між політичними акторами та їхніми виборцями, громадянами. На відміну від традиційних медіа, які можуть бути обмежені сильною авторитарною владою, соціальні мережі дозволяють зберігати простір вільного вираження думки. Крім того, сучасні соціальні мережі та цифрові платформи дозволяють використовувати складну інформацію: від відео- та фотоконтенту, до графіків, документів тощо. Цей процес дозволяє зберігати підзвітність урядів своїм громадянам, котрі відносно легко можуть здійснювати контроль за їх діяльністю. Відтак, можна говорити про те, що пильна увага громадян до політичного процесу в країні за допомогою соціальних мереж запускає їх новий вимір функціонування – це напрям політичного піару та медійної активності політиків (Данько, 2015).

Роль Інтернету в політичній комунікації швидко розвивалася в 1990-х роках, ставши життєво важливим інструментом політичних кампаній і джерелом політичної інформації. Такі терміни, як «мережевий активізм» і «кіберактивізм», з'явилися для опису використання електронних комунікаційних технологій, зокрема соціальних медіа, електронної пошти та обміну миттєвими повідомленнями, для адвокації, розбудови спільноти та політичної мобілізації. Існує два основні підходи до оцінки політичного впливу Інтернету: оптимістичний і песимістичний. Оптимісти стверджують, що Інтернет розширює можливості громадян, покращує пряму дію демократії та відкриває нові можливості для політичної мобілізації та участі (Гусєва, 2024). Песимісти

стверджують, що Інтернет збільшує прірву між політично заангажованими громадянами та політично неактивною більшістю (Адорно, 1972).

Нові політична комунікація в мережі створює як виклики, так і можливості. Громадяни мають можливість прямого контакту з політичними діячами та участі в мережевих політичних структурах чи організаціях. Інша сторона такого групування – поляризація інформації та точок зору, що підвищує ризики кампаній з дезінформації. Хоча Інтернет та соціальні мережі мають потенціал сприяти політичній активності, вони також призводять до зниження довіри до політичних інституцій та офіційних джерел інформації. Деякі дослідники також вважають, що значне проникнення соціальних мереж призводить до соціальної ізоляції (Данько, 2015).

Зростаючий вплив соціальних мереж на соціальні складові стає дедалі помітнішим у різних контекстах політики, наприклад, під час електоральних процесів, протестів, революцій тощо. Соціальні мережі надають комплексний інструментарій для передачі інформації, особливо в умовах обмеженого доступу до офіційної інформації. Вони також полегшують синхронізацію дій через застосунки обміну повідомленнями – месенджери чи спеціалізовані форуми, що дозволяє консолідувати прихильників того чи іншого політичного актора.

Значення та потенційний вплив соціальних мереж та Інтернету на суспільство не залишилися поза увагою впливових політиків (Дзьобань, 2015). Наприклад, Алекс Росс, радник держсекретаря США, порівняв Інтернет із «Че Геварою 21 століття», підкреслюючи його трансформаційний потенціал у формуванні сучасних соціально-політичних ландшафтів (Тараненко, 2013).

Під час протестів у Гонконзі 2019-го, викликаними новими законодавчими ініціативами, зокрема, у питані екстрадиції громадян, цей новий функціонал соціальних мереж проявився найкращим чином. Фактично, цей рух направлений на демократизацію та лібералізацію, існував без видимих лідерів чи жорсткої ієрархічної структури. Проте протягом багатьох місяців жителі Гонконгу зберігали спроможність до участі у демонстраціях, акціях та могли злагоджено протистояти поліції. Соціальні мережі дозволили уникнути анархії та

координувати свої дії через форуми. Таким чином, організація та ухвалення важливих рішень відбувалася спільнотою шляхом голосування та обговорення (Stewart, 2019).

Крім того, соціальні мережі є сприятливим ґрунтом для вербування нових учасників протесту та консолідації вже наявних симпатиків. За останні роки інтернет-канали та соціальні мережі перетворилися на першоджерела всебічного вивчення різноманітних протестних рухів. Примітно, що вони являють собою комунікаційне середовище, вільне від часових обмежень, цензури, технічних бар'єрів чи інших перешкод, уможливлюючи нестримне вираження думок і швидку передачу інформації.

Розвиваючись із цієї динаміки, термін «Twitter-революція» був введений американським дослідником білоруського походження – Е. Морозовим, який провів основоположне дослідження, вивчаючи її початок під час спірних виборів до Молодіжного парламенту 2009 року. Розслідування Морозова висвітлило трансформаційний вплив користувачів Twitter на національний протестний ландшафт. Слід зазначити, що українські події, зокрема Революція Гідності 2013-2014 рр., привернули увагу таких американських науковців, як Дж. А. Такер, М. Мецгер, П. Барбер. Їхнє дослідження «Українські протести 2013-2014 років» ретельно окреслило ключову роль Twitter та його контенту під час Євромайдану (Tucker & Metzger, 2014). Українські революції, в яких соцільні мережі традиційно були важливою складовою руху, прямо впливають на те, в який спосіб Україна представлена у світі. Демократичний розвиток та бренд країни на міжнародній арені може змінюватися під впливом соціальних мереж. Н. Шуст, наприклад, аналізує демократичні концепції через призму міжнародних індексів, доводячи, що рівень демократизації є визначальним чинником формування позитивного сприйняття держави світовою спільнотою. Таким чином, брендинг країни розглядається не лише як маркетинговий інструмент, а як стратегічний результат внутрішніх політичних реформ та інституційної стабільності (Шуст, 2022).

Подальше розуміння впливу соціальних медіа на колективні дії пропонує американський дослідник К. Ширкі в книзі «Сюди приходять усі». Ширкі пояснює унікальні характеристики проведення протестів за допомогою соціальних медіа, підкреслюючи, що ці онлайн-інструменти сприяють швидкому знайомству та колективній мобілізації без традиційних витрат часу на підготовку та залучення широких верств населення. Поєднання Інтернету та соціальних мереж прискорює виявлення однодумців і встановлення горизонтальних зв'язків (Shirky, 2008).

Ці дії часто здійснюються організаторами з частковим прийняттям відповідальності або навіть уникненням її за їхні наслідки. Показово, що використання соціальних мереж як високоефективного засобу для мобілізації значної кількості активних учасників, особливо серед молоді, є прикладом їх ролі в організації сучасних масових протестів. Ці мережі функціонують як канали для розповсюдження різноманітної інформації з можливістю тривалого діалогу, що сприяє виникненню спільних точок зору та спільних ідей (Shirky, 2008).

Всебічний аналіз широкомасштабних виборчих процесів чи політичних протестів і ролі нових медіа в їх розгортанні підкреслює, що соціальні мережі перетворилися на провідний канал для поширення та обміну інформацією між учасниками та тими, хто сприяє організації розрізнених груп людей. У дослідженні під назвою «Колективні дії в епоху Інтернету» розглянуті глобальні наслідки Інтернету для колективних зусиль учасників мережі. У цій роботі дослідники розрізняють дві різні категорії дій: віртуальні та фізичні. Віртуальні дії зазвичай охоплюють такі дії, як підтримка онлайн-петицій, участь в обговореннях на форумі або, в деяких випадках, участь у незаконній діяльності, прикладом якої є хакерські атаки. У ході цих скоординованих дій платформа соціальної мережі служить зв'язком для об'єднання безлічі розрізнених ресурсів, які є в розпорядженні користувачів. Відтак, збільшується вплив конкретного індивіда на сферу політики (Данько, 2015).

Цілком очевидно, що Інтернет є епіцентром координації глобальних протестів. Крім своєї ролі як засобу для обговорення та культивування

протестних настроїв, Інтернет став безпрецедентним інструментом для ефективної кооперації та «краудсорсингу», особливо в контексті стихійних лих. Дослідження моделей поведінки під час надзвичайних ситуацій провели Б. Макконнелл і Дж. Хуба. Результатом їхнього дослідження стала модель «4-F», яка класифікує активних користувачів у різних онлайн-спільнотах, класифікуючи їх за групами: «фільтри», «шанувальники», «функціонери» і «феєрверки». Ці окремі категорії осіб мають різний ступінь впливу на формування громадської думки та оцінювання різноманітних політичних явищ (Huba & McConnel, 2012)

Широке охоплення соціальних мереж сприяє поступовому зростанню політизації аудиторії. Ця політизація породжує трансформацію, за якої інструментальні соціальні мережі беруть на себе роль, традиційно пов'язану з інформаційними засобами, в яких раніше слугували джерелом консолідації громадської активності. Нові медіа-платформи відіграють ключову роль у політичних процесах, адже дають змогу прямої інтеракції з представниками політикуму, бізнесу тощо одразу на цифрових платформах. Таким чином, зменшується розрив між виборцями та їх кандидатами, тому впливові політики перетворили свої сторінки в соціальних мережах на персональні блоги, що спрощує виборцям можливість ідентифікувати себе із цим конкретним політиком, його ідеями та прихильниками. У цих цифрових спільностях користувачі є не просто пасивними споживачами інформації – вони є активними учасниками, які беруть участь у співтворенні контенту та скоординованих діях.

Для того щоб проаналізувати, в який спосіб соціальні мережі впливають на організацію суспільства та політичних систем, варто звернутися до ідей, які синтезував Маршал Мак-Люен у своїй праці «Галактика Гутенберга». Перед автором цієї роботи стало нелегке завдання – відслідкувати, в який спосіб поява передової технології, яка прискорює обмін інформацією та робить її доступною для широкого загалу, впливає на цілі суспільства і закладає трансформаційні зміни на цілі покоління уперед. В XV столітті винайдення нового методу друкування книг Йоганном Гутенбергом визначило політичні, історичні та суспільні тенденції на майже чотири сотні років (Мак-Люен, 2014).

Мак-Люен у своїй праці послідовно доводить, що будь-яка нова технологія поступово розширює одне або декілька відчуттів і, виносячи їх у простір суспільного, поступово змінює те, як ми сприймаємо світ. На прикладах неписемних африканських спільнот Мак-Люен демонструє, що західне абстрактне сприйняття мистецтва чи кіно є наслідком тривалого користування алфавітом та писемністю. Натомість для людини, що живе в племінному, переважно аудіальному та міфологічному світі, концентрація та розуміння образності кінематографу є недоступними та складними, а розуміння образів вимагає тривалої та кропіткої підготовки (Мак-Люен, 2014, с. 61). Окрім того, Мак-Люен цитує Бертрана Рассела, який говорить, що проривні теорії і відкриття, наприклад, ідеї Коперника чи Ейнштейна, будуть зрозумілішими поколінням, які зростатимуть разом із ними (Мак-Люен, 2014, с. 66).

Поширення переписуваного книжництва обґрунтувало відхід від сакрального, слухового способу розуміння світу до візуального, а вже на наступному етапі в XV столітті, разом із винаходом Гутенбергом книгодрукування, відбулося різке пришвидшення розвитку суспільства та політичних систем. Дослідження Мак-Люена чітко демонструє, що поступове наростання інформаційного потоку корелює із тим, в який спосіб у суспільстві відбувається зміна уявлень про світ та як організовуються знання про нього. Навіть в часи, коли книги переписувалися від руки, а спосіб їх читання залишався переважно «вголос» – люди вже отримували значну більшу кількість інформації у порівнянні з минулими історичними епохами.

В свою чергу, книгодрукування стало найголовнішим етапом розвитку алфавітної культури, яка відлучила індивіда від племінного, колективного сприйняття світу і перелаштувала людину на шлях індивідуалізму. Відкриття Адама Сміта чи Французька революція нерідко трактуються сучасними дослідниками як наслідок винайдення книгодрукування, що свідчить про те, що книгодрукування змінювало самі форми взаємодії між людьми у спільнотах. Книгодрукування, наприклад, відкрило світ національних мов та пресу, а доступ до друкованого слова став надбанням широкої публіки. Друкована книга стала

запорукою уніфікації розрізнених спільнот і заклала передумови до появи націй у майбутньому. В «Галактиці Гутенберга» зустрічаємо тезу, котра рівноцінно означує спільну для книгодрукування та сучасного інтернету, з його соціальними мережами, проблематику: «Дія будь-якої сили – катастрофа, якщо не усвідомлювати наслідків впливу, а надто тієї сили, яку ми самі створили» (Мак-Люен, 2014, с. 334)

Якщо наслідки появи книгодрукування, як найвищої точки еволюції алфавіту, вже піддавалися осмисленню, то ситуація з розумінням подібних наслідків появи соціальних мереж, як етапу розвитку Інтернету, потребує детальнішого огляду. Для Маршала Мак-Люена винайдення абетки відкрило «браму» до асиміляції неалфавітних культур. Алфавіт, на його думку, поглинав і трансформував культури, за своєю суттю це була агресивна технологія (Мак-Люен, 2014, с. 77). Ця комунікаційна інновація викликала трансформацію цілого способу суспільної організації – від племінної до національної. Поява націй – один із ключових етапів політичної творчості людини. У цьому контексті постає питання: в який спосіб ще одна комунікаційна інновація – соцмережі – трансформує політику та політичні системи?

В 2016-му році Мартін Белам в матеріалі для *The Guardian* спробував поєднати ряд явищ в інтернет-середовищі, які, на його думку, походять на «першу світову кібервійну». Автор розвідки розглядає 2007-й рік та хвилю кібератак з боку Росії на державні цифрові сервіси Естонії як відправну точку у новітньому протистоянні національних держав. Автор додає до своїх аргументів ще ряд показових епізодів, наприклад, обрив кабелів інтернет-з’єднання на дні Середземного моря в 2008-му році (Belam, 2016). Під час цього інциденту значна частина користувачів з Єгипту лишалася без доступу до мережі, а сама подія офіційно трактувала як «несправність».

В 2024-му році, після атак хуситів на підводні кабелі в Червоному морі, вже остаточно можна стверджувати, що розлогі мережі кабелів, які забезпечують підключення до мережі, однозначно є однією із потенційних цілей у цифровому протистоянні між національними державами та афілійованими до них

угрупуваннями (Johnson, 2008). Також в статті наведені приклади застосування хакерських атак для виведення з ладу ядерної програми Ірану в 2010-му році або атака Північної Кореї на компанію Sony – для досягнення агресивних дипломатичних цілей новими засобами. І звісно ж, одним із маркерів цього протистояння автор називає втручання у вибори в США у 2016-му році з допомогою різноманітних електронних систем. У підсумку, автор формулює гіпотезу, що для істориків майбутнього інтернет буде більш цікавим саме з погляду на нього як інструменту для військових цілей та простору, в якому одні держави намагаються отримати перевагу над іншими (Belam, 2016).

Такий погляд контрастує з оптимістичним поглядом Шмідта і Коена та з більш ранніми лібертаріанськими уявленнями про інтернет як простір повної свободи і запоруку позитивних трансформацій для суспільства (Фергюсон, 2018, с. 469). Бачення Мартіна Белама – це одна із переконливих варіацій для пояснення тих контраверсійних тенденцій, які розгортаються сьогодні в мережі. Вочевидь, в цьому аналізі не вистачає низки додаткових обставин та явищ, які після пандемії коронавірусу та російського широкомасштабного вторгнення в Україну стали більш видимими. Зокрема, автор не взяв до уваги значний пласт дій, які розробляють та реалізують урядові та неурядові сили в мережі.

Якщо уявити сучасне інтернет-середовище та соціальні мережі як ще одну площину протистояння національних держав, то маємо відзначити, що цей простір став полем, на якому держави будують свої стратегії «нападу» та «оборони», розгортають спеціалізовані відділи з проведення чи запобігання інформаційним операціям та шукають способи адаптувати власні стратегічні документи до інтенсивності комбінованих цифрових викликів, що наростають. Окрім того, поширення соціальних мереж частково посприяло тому, що світ «стиснувся». Тут йдеться не так про уявлювані нами інші суспільства чи держави із їхніми кордонами (адже притаманна індивідам ментальна географія чи стереотипи навряд чи зникли), а про те, з якою швидкістю ми дізнаємось новини чи інформацію з інших куточків світу і як ми з ними взаємодіємо (Гончар, 2024).

Яскравий приклад цієї нової глобалізованості – надзвичайно деталізованої, зафіксованої на фото та відео, можна спостерігати протягом російсько-української війни. Від самого початку російської агресії поширення інформації про перебіг війни в соціальних мережах стало одним із фокусів українського уряду, лідерів суспільної думки, волонтерів та військових. Важливою складовою в цьому контексті є вивчення інформаційної війни в сегменті інтернет-комунікацій. У спільних працях І. І. Пронози, С. Ю. Цимбала та О. здійснюється порівняльний аналіз українських та європейських практик протидії дезінформації. Автори обґрунтовують тезу, що пропаганда в цифровому середовищі є ключовим інструментом гібридної війни, спрямованим на дестабілізацію громадянського суспільства. Дослідження присвячені комплексному аналізу трансформації українського соціуму в умовах розбудови інформаційного суспільства та формування міжнародного іміджу держави. фокусує увагу на теоретичних і практичних аспектах становлення цифрової інфраструктури, визначаючи ключові виклики та перспективи, що постають перед Україною на шляху до глобального інформаційного простору (Проноза & Цимбал, 2025).

Соціальні мережі відіграють роль дипломатичного інструменту та є елементом тиску на уряди дружніх до України демократичних країн. Українські користувачі соціальної мережі Twitter (згодом X) використовують її для інформування західних суспільств та створюють дискусію про необхідність підтримки обороноздатності України. Така проактивна позиція українців в мережі є також одним із факторів того, що громадяни західних країн мають можливість краще уявляти реалії російської агресії, будувати власні висновки.

Кількість контенту, яка щодня створюється користувачами соціальних мереж і стосується війни, є надзвичайно великою, а на її опрацювання майбутніми істориками буде необхідна значна кількість часу та ресурсів. Можна говорити про те, що це військове протистояння отримало безпрецедентний рівень «цифровізації». Сучасні технології супутникового інтернету дозволяють отримувати матеріали безпосередньо з поля бою, створювати цифрові мапи лінії

фронту (один з найвідоміших проєктів – мапи від DeepState). Як наслідок, громадяни отримують щоденну інформацію про ситуацію на фронті, що було б неможливим у війнах минулого (Гончар, 2023)

Окрім того, соціальні мережі – один з найбільш дієвих інструментів, який дозволяє фіксувати та ділитися із західними суспільствами наслідками російських ракетних ударів або військових злочинів, частина з яких лишилася б невідомою за відсутності соціальних мереж та глобального покриття інтернетом. Все це свідчить про те, що російське вторгнення в Україну частково розмиває традиційний поділ на військову та цивільну сфери, соціальні мережі та месенджери стали медіумом, через який відбувається мобілізація та низова ініціатива громадян у сприяння обороні. Саме в цих неформальних мережах різні представники суспільства здатні реагувати швидше та підсилювати збройні сили через благодійні та волонтерські збори під термінові запити військових підрозділів. Традиційні ієрархічні та бюрократичні державні структури, в свою чергу, мають схильність до запізнілої реакції через помітну затримку системи (Гончар, 2024).

Відтак, російська агресія демонструє, що війни XXI століття відтепер будуть паралельно розгортатися і в цифровому просторі. Така тенденція призводить до якісно нового сприйняття війни суспільствами: через покриття «цифрою» вона стає ближчою, кількість інформаційного потоку зростає, зменшується кількість таємниць, а громадяни повсякчас перебувають під тиском інформаційних операцій, які застосовує інша сторона конфлікту. Цей останній фактор, не в останню чергу, впливає на спроможність суспільства до опору та його здатність протистояти значним кризам.

Згаданий раніше Маршал Мак-Люен вже передбачав ці зміни. Дослідник стверджував, що Гутенбергову галактику врешті замінить нова «Галактика Марконі», в якій електронні засоби передачі інформації та зображень будуть відігравати вирішальну роль. Сучасну добу він називав електронною і стверджував, що світ рухається до того, щоб стати «глобальним селом», праобразом якого є племінний лад дописемних культур. Важливим в цій

концепції є зауваження про те, що зникнення фрагментарного та розділеного світу може призвести до того, що людські спільноти опиняться перед ситуацією, коли в суспільствах панує «панічний страх», притаманний племінним спільнотам, в яких увесь простір та уявлення про навколишній світ є замкненими і взаємозалежним (Мак-Люен, 2014, с. 65). Така метафорична характеристика може виглядати як спроба футуристичного прогнозування майбутнього, яким його бачили в шістдесяті роки минулого століття. Аналізуючи сучасну «електронну добу», можемо стримано стверджувати, що візія Мак-Люена, побудована на блискучому аналізі минулого, дозволила йому передбачити, для яких завдань можуть бути використані електронні технології, що пришвидшують комунікацію та роблять її масовою. Щоб усебічно проаналізувати вплив соціальних мереж на людину, знадобилась би праця-відповідник «Галактиці Гутенберга».

Спостереження Пітера Померанцева, експерта з медіа та пропаганди, перегукуються із оптикою, яку Маршал Мак-Люен пропонував ще у минулому столітті. Померанцев вже на перших сторінках своєї роботи «Це не пропаганда» зазначає, що уявлення XX століття про те, що разом зі збільшенням кількості інформації рух за демократію та свободу отримає низку переваг над політичними режимами, які користаються з власного права на примус та впливовості спецслужб – підтвердились лише частково (Померанцев, 2015, с. 10). Надзвичайна насиченість інформаційного простору «грає» не тільки за «команду» активістів, опозиціонерів та громадян зацікавлених у захисті демократичних принципів, але й дає політичним режимам та впливовим політичним елітам нові ключі до консолідації влади та низку новітніх засобів до упокорення незгодних.

Померанцев, будучи професором Інституту глобальних питань Лондонської школи економіки, має за мету розкрити та проаналізувати ті суспільно-політичні зміни, які принесли із собою новітні цифрові технології. Ситуація з сучасними демократичними системами, як їх описує Померанцев, виглядає щонайменше кризовою. Спостереження автора про те, що ліберальний

світ переживає стагнацію, відзначається навіть в тому, який словник ми використовуємо. Знайомі слова, такі як «демократія», «свобода», «ліберал», втрачають той сенс, який був притаманний їм зовсім нещодавно – у часи «традиційних» медіа (Померанцев, 2015, с. 12). Вплив алгоритмів, таргетованої реклами, поширюваної в інтернеті дезінформації та теорій змов у соціальних мережах впливають не тільки на політичні процеси, але і на кожного окремого громадянина та його сприйняття світу. Останнім часом ми вже навіть не дивуємося розслідуванням про втручання у вибори третіми державами за допомогою цифрових засобів – це стало певною мірою новою «нормальністю», неможливою ще на початку 90-х років XX-го століття.

Пітер Померанцев припускає, що інтернет з його підсистемами змінює міжособистісну комунікацію, трансформує стосунки в родинах, і навіть змінює ідентичності людей (Померанцев, 2015, с. 13). Такий погляд вимагає серйозного ставлення та аналізу, адже ідентичність, особливо у суспільствах, які стикаються із екзистенційними викликами: війнами, епідеміями чи техногенними катастрофами, є джерелом стійкості та підґрунтям для виживання спільноти. Тому, досліджуючи сучасні соціальні мережі та інтернет, наприклад, в українському контексті, надзвичайно важливо відповідати на запитання: як те чи інше явище або система явищ та тенденцій впливають на громадянина та його ідентичність, хто є джерелом цього впливу та яка мета переслідується?

Аналізуючи працю Померанцева, можна зробити висновок, що описана ним криза в демократичних системах не в останню чергу пов’язана із тим, що традиційні медіуми інформаційного впливу втрачають позиції у «перегонах» із формування ідентичності. Радіо, телебачення, газети та книги створювали зрозумілі зразки поведінки та образи, які уніфікували розрізнених представників суспільства у ширші, за класичним вже поясненням Бенедикта Андерсона, – уявлені спільноти (Андерсон, 2001). Ці медіуми дозволяли формувати, зберігати та контролювати різні прояви ідентичності. Якщо галактика Гутенберга з її книгодрукуванням та газетами дала необхідну інерцію для унормування та поширення національних мов та націй, то електронна галактика Марконі навпаки

децентралізувала потоки інформації, створила спільний комунікаційний простір для кожного куточку світу, куди дістали кабелі телеграфу чи комп'ютерних мереж.

Вочевидь, пришвидшення появи нових проривних технологій призводить і до пришвидшеної появи нових «галактик», які заміняють із часом одна одну. Соціальні мережі від моменту своєї появи ще не привели нас до чогось, що можна було б назвати «галактикою Цукерберга», але вони мають потенціал стати такими. Не виключено, що наступні технологічні винаходи, які будуть пов'язані з масовими комунікаціями та зміною способу споживати інформацію, призведуть до конкуренції між новими «галактиками» за вплив на потенційних реципієнтів. Специфіка соціальних мереж та інтернету полягає в тому, що вони розглядалися як засіб звільнення та джерело до майже необмеженого прогресу. Перші мережеві ентузіасти, вочевидь, розуміли, що ефект від цих технологій може бути таким самим, як і винахід друкарського верстата, однак сьогодні ми можемо засвідчити легковажність таких уявлень.

Пітер Померанцев докладно описує, як у сучасних соціальних мережах відбувається формування «фейкової реальності» за допомогою фабрик тролів, зокрема однієї з найвідоміших – Ольгіно. Він говорить про те, що люди, яким раніше вдавалося протистояти дезінформації, продукованої телебаченням, тепер не мають необхідної спроможності критично сприймати дописи та коментарі в соціальних мережах, які штучно створюються підконтрольними урядам організаціями (Померанцев, 2015, с. 164)

Органічно ці мережеві структури з генерації неправдивої інформації спершу відпрацьовували внутрішню повістку в державах, де режим потребував переінакшити уявлення про «правду» та створити поле, в якому народжуються десятки різноманітних пояснень та теорій з будь-якого питання. Ця широта трактувань дозволяє владі розмивати віру громадян в те, що правду можливо встановити чи реконструювати. Цей підхід за направленістю нагадує методи пропаганди минулого століття. Згадаємо, на кого були розраховані візуальні елементи відточених пропагандистських машин минулого: плакати, символіка,

програми на державному телебаченні, пам’ятники, листівки та навіть поштові марки – були постійно присутніми у просторі та перед очима людей, які проживали в авторитарних чи тоталітарних режимах. Відтак, в першу чергу, державна пропаганда спрямована на власних громадян, вона переконує їх та мобілізує, забезпечує лояльність. Але чи здатні сучасні «класичні» пропагандистські потуги Північної Кореї переконати будь-якого громадянина Південної Кореї – питання, скоріше, риторичне (Радіо Свобода, 2020). Натомість соціальні мережі та фабрики тролів успішно долають цей бар’єр, вони вже досить давно вийшли на міжнародний рівень, а відпрацьовані інструменти та прийоми вдало застосовуються авторитарними режимами проти демократичних систем.

Як було зазначено раніше, вплив на волевиявлення громадян третіми країнами з використанням дезінформації та мереж тролів у соціальних мережах вже стали частиною нової цифрової реальності. Таким чином, національна держава, яка не реалізовує власної стратегії в цифровому просторі, втрачає спроможність ефективно протистояти зовнішньому впливу. Адже інші сили чи держави здатні захоплювати її інформаційний простір і створювати у соцмережах ту «реальність», яка відповідає їхнім інтересам. Західні дослідники поступово уводять нові концепції та термінологію під цей процес цифрового зіткнення – від «веапонізації» соціальних мереж до теорії «розмитих кордонів».

Для авторитарних режимів, які активно шукають прогалини у демократичних процедурах та принципах, соціальні мережі – зброя, якою можна розігрівати невдоволення владою в іншій країні, провокувати революції та акції непокори, підривати довіру до уряду та окремих політиків. Формування атмосфери недовіри – одна з ключових стратегій тих зацікавлених сил, які прагнуть встановити контроль або у внутрішній політиці, або поширити її на інше суспільство. Для такої задачі якнайкраще підходять теорії змов (Померанцев, 2015, с. 75). Найбільш дієвий спосіб вплинути на сприйняття світу власними громадянами або громадянами інших держав – живити їх теоріями змов.

На цю проблематику звернув увагу О.Кондратенко, у роботах якого комплексно проаналізовано роль іномовлення як інструменту зовнішньої політики авторитарних держав. Дослідник фокусує увагу на системних особливостях функціонування медіаресурсів таких країн, як Російська Федерація, КНР та КНДР, виявляючи специфічні механізми, за допомогою яких автократії намагаються легітимізувати власні політичні режими на міжнародній арені та здійснювати деструктивний інформаційний вплив на закордонні аудиторії. У контексті вивчення російського кейсу, автор деталізує специфіку іномовлення РФ, розглядаючи його не лише як засіб поширення інформації, а як повноцінний складник гібридного протистояння та засіб утримання авторитарної стабільності. Науковець доводить, що трансформація медійних стратегій таких держав безпосередньо корелює з їхніми геополітичними амбіціями та внутрішньополітичною логікою виживання режимів (Кондратенко, 2025).

Давня стратегія використання різноманітних змовницьких теорій в ХХ-му столітті слугувала єдиній меті – підсилювати панівну ідеологію. Радянська влада, як і будь-який сучасний закритий чи популістський режим, активно користувалася пошуком змовників або «ворогів». Тиражовані теорії змови давали радянській людині чіткий образ «іншого», ворожого та дозволяли провести зрозумілий поділ на «ми» та «вони». Таким чином, відбувалася подальша консолідація суспільства та його мобілізація на підтримку офіційного «курсу», а будь-які невдачі радянської авторитарної системи можна було успішно перекладати на змовників чи «невидиму руку».

Сучасні авторитарні режими користуються більш софістикованими методами інформаційного контролю. Пітер Померанцев стверджує, що вони мають складнощі із формуванням монолітної ідеології. Відсутність єдиної цілісної ідеології дозволяє авторитарним лідерам оперувати різноманітними повідомленнями, створюючи для власних громадян альтернативну картину світу, яка сповнена небезпек (Померанцев, 2015, с. 75). Теорії змов ідеально пристосовуються до алгоритмів соціальних мереж. Аудиторію можливо деталізовано сегментувати, обирати групи найбільш уразливі до тієї чи іншої

інформації. Налаштування в середині мереж дозволяють транслювати повідомлення в потрібному місці у потрібний час з максимальною ефективністю. Сучасні авторитарні режими демонструють, як ця стратегія успішно атомізує суспільство.

Приклад російського режиму показовий, адже в умовах, коли тотальна цензура вже не є можливою, громадян оточують різновекторною інформацією, яка створює відчуття невпевненості та апатії. Громадяни в такий ситуації втрачають суб'єктність, адже в світі, де все визначено наперед – не існує альтернативи, вибори втрачають будь-який сенс, а єдиною цінністю стає персональна стабільність. Кремлівський режим вдало продукує зневірених громадян, які стають міцною опорою влади; ця модель призводить до деградації базової навички, необхідної для функціонування стійкої демократії – спроможності громадян бути відповідальними за власні рішення.

Інша небезпека цієї новітньої авторитарної стратегії – її привабливість для автократів в різних куточках планети. Кремль «експортує» вже відпрацьовані практики іншим авторитарним лідерам, які використовують їх для розмивання демократії у власних країнах. Модель «керованої демократії», вигадана росіянами, – це утілення ілюзії демократичності. Позірна демократична риторика, збереження формальних виборів, наявність «ручних» опозиційних політиків та контрольовані ЗМІ мають виглядати зовні як типова та унормована демократична система, а в середині – бути цілковито підконтрольними та забезпечувати авторитарному режиму стабільність і прогнозованість.

Така модель обгортається в щільну оболонку різнорівневого інформаційного впливу, в якій для кожної суспільної групи обирається необхідний канал інформації. Якусь частину суспільства режим спроможний кооптувати за допомогою телебачення чи поширення дезінформації в соціальних мережах, для іншої частини населення генеруються незліченні теорії змов (китайська мережа TikTok рясно сповнена таким контентом), для більш спроможних до інформаційного опору груп використовуються складніші набори контенту, які мають розхитувати усталену картину світу та принципи

громадянина, поступово підводячи його до узвичаєного, в інтернет-середовищі, способу пояснювати складні явища – «все не так однозначно» (Foy, 2021).

Поточна геополітична ситуація, що поступово нагадує про образ завершеної у минулому столітті Холодної війни, безперечно, породить ще не один спосіб використання соціальних мереж для отримання переваги над іншою стороною протистояння. Винайдення книгодрукування в XV столітті призвело до радикальних суспільних змін, кульмінацією яких було постання модерних націй. Жодних заперечень не викликає важливість друкарського верстату для розгортання доби Просвітництва, поширення ліберальних ідей – свободи та рівності, явищ які традиційно описуються в позивному ключі. Разом з тим, друкована книга породила і епоху Реформації та релігійних війн у різних куточках Європи, наслідки яких можна відслідковувати і до сьогодні. Трохи згодом нації, об'єднані національними літературами та пресою, зіткнулися в серії світових війн, «шрами» від яких відчутні століття після. Друкована книга, котра була покликана звільняти та поширювати знання, стала також і інструментом війни та пропаганди. Досвід минулого демонструє, що національні держави охоче використовують будь-яку проривну технологію, яка дозволяє отримати перевагу в міждержавному протистоянні.

Соціальні мережі та інтернет в цілому проходять схожий «маршрут» – від лібератівної технології до технології, яку вдало пристосовують для своїх завдань зацікавлені сторони. Авторитарні режими вдало адаптували можливості нових технологій до власних потреб, упровадивши нові форми цифрового контролю своїх громадян (LaFrance, 2021). По-друге, ускладнення технологій не призвело до очікуваного ефекту – закриті системи не перекривають доступ громадян до мереж та інтернету, а надають перевагу використанню їх для втручання в ідентичність та світогляд громадян. Підміна понять, теорії змови та пропаганда в соціальних мережах та месенджерах – лише деякі з найдієвіших інструментів знищення суб'єктності суспільства. Таке суспільство стає пластичним і дозволяє автократам керувати не з позиції сили, а з позиції «патріарха», який захищає своїх

громадян від ворожого світу, в якому панує «панічний страх» Маршала Мак-Люена.

Таким чином, зміцнення авторитарних режимів, озброєних соціальними мережами та новими технологіями, поступово розділяє світ на два табори – агресорів та тих, хто змушений захищатися. Оскільки демократичні системи ще не винайшли дієвих засобів для захисту своїх громадян від цих гібридних цифрових загроз, то можна констатувати, що на сьогоднішній день авторитарні режими мають більше можливостей та інструментів реалізовувати свою політику в мережі – вони не обтяжені міжнародними договорами чи демократичними цінностями та правилами. Від того, наскільки довго недемократичні системи гратимуть «першу скрипку» в соціальних мережах та інтернет-платформах, суттєво буде залежати те, наскільки стійкими будуть мир, міжнародне право та демократія у світі (Гончар, 2024).

Останніми роками визначним фокусом у західному науковому дискурсі є помітною спроба проблематизувати питання безпечності соціальних мереж. З'являється все більше голосів, які намагаються передбачити загрози, що їх створює нове цифрове середовище. Дослідники підкреслюють, що ці технології, окрім своєї традиційної ролі у сприянні комунікації, обміну думками та пошуку інформації, починають відіграють подвійну роль як об'єкти та інструменти для управління інформацією. Нерідко таке управління здійснюється із деструктивною метою. Західна наукова думка поступово осмислює ті процеси, які відбуваються разом із розвитком соціальних мереж. Дослідники Зінгер і Брукінг виводять в наукову спільноту ідею про їхню нову функцію – зброї, котра впливає на соціальне та політичне життя суспільства та формує умови, в яких кожен користувач знаходиться на постійному «полі бою». Вони пропонують новий термін «веапонізація» соціальних мереж. На їхню думку, соціальні мережі з їх глибиною проникнення прямим чином впливають на розгортання та перебіг різноманітних конфліктів та все більше стають частиною «арсеналу» урядів та армій, розмиваючи різницю між реальним світом та світом Інтернету (Singer & Brooking, 2019). Вже з середини 2000-х років соціальні мережі стали

інструментом гібридної війни та інформаційних кампаній з дезінформації. Об’єктами цих атак зокрема стають країни ЄС та НАТО.

З урахуванням тенденцій розвитку соціальних мереж, варто ствердити, що класичні теорії мережевого суспільства потребують актуалізації. Якщо, наприклад, М. Кастельс розглядав мережі як простір горизонтальної свободи, то сучасні реалії 2020-х років демонструють феномен «інфраструктурної заплутаності» (infrastructural entanglement). Цей концепт, розроблений дослідниками сфери безпеки та цифрового суспільства, описує стан, коли державні інституції стають критично залежними від приватної цифрової інфраструктури (хмарні сервіси Amazon, алгоритми Google, супутники Starlink, тощо). Це призводить до розмивання суверенітету: влада переміщується від урядів до тих, хто контролює вузли мережі та потоки даних (Javadi, 2015). У цьому контексті соціальні мережі перестають бути просто майданчиком для дискусії або «площею» у категоріях Ніла Фергюсона, а стають інфраструктурою подвійного призначення, яку держави не контролюють повністю, але без якої вже не можуть функціонувати.

1.2. Соціальні мережі та цифрове середовище у рамках ретроспективного аналізу глобальних загроз Європейського Союзу

7 лютого 1992 року в місті Маастрихт було підписано договір про створення Європейського Союзу. Фактично, нова європейська унія стала результатом довгого шляху Європи до подолання історичних суперечностей. Європейський Союз – уособлення європейської спільності та наочний приклад того, що великі інтеграційні проєкти є успішними та життєздатними в сучасному історичному контексті. Союз пройшов значний шлях у процесі консолідації, а сама ідея створення наднаціональної організації європейських країн проросла на ґрунті історичних викликів та минулих катастроф.

Дві світові війни, породжені крайніми формами націоналізму, поставили країни Європи перед фактом необхідності консолідації зусиль, солідаризації та взаємної підтримки. Ідеї про об'єднану Європу – не винахід XX століття. Згадаємо спроби імператора Наполеона Бонапарта зробити з Першої французької імперії глобального гравця, навколо якого був би спільний простір із дружніх до Франції країн. В схожому контексті можна пригадати і давніші приклади Карла Великого, який створив схожу імперію і, по суті, заклав фундамент для майбутніх Франції, Німеччини та Італії. Більше того, в європейській міфотворчості та історичній пам'яті відчувається сильний вплив греко-римської цивілізації, яка сполучала величезний простір та вплинула на формування цілого континенту.

Європа та Європейський Союз пройшли довгий шлях генезису та оформлення політичної думки, що дозволили врешті вийти на модель, в якій війна є неможливою в середині Союзу. На цьому довгому шляху було немало історичних діячів, котрих можна було б охарактеризувати як «батька Європи». Пошук цього «батька» є складним завданням та залежить від глибини, на яку ми віддаляємося в минуле. Як Карл Великий, так і імператор Наполеон чи Карл V могли би претендувати на цю роль, але в їхніх способах «об'єднання» силовий метод консолідації завжди переважав над діалогом та добровільною відмовою від частини суверенітету заради більшого проєкту. Традиційне перебування Європи в стані тривалих військових конфліктів та катастрофічні наслідки Другої світової війни на довгі роки витіснили дискусію про військову та безпекову роль Європи у світі. Натомість європейський суверенітет у військовому та безпековому вимірі був частково замінений американською «парасолькою», котра дозволила європейським урядам відкласти обговорення значення Європи у глобальній безпеці до сучасності.

Повернення війни на Європейський континент у 2022 році активізувало дискусію про роль Європейського Союзу в забезпеченні миру та безпеки у глобальному контексті. Це об'єднання 27 країн та 450 мільйонів громадян лишається одним із найбільших ринків, впливовим торговельним та інвестиційним партнером. Нині Євроунія постає перед новітніми та

ускладненими стратегічними викликами, які за комплексністю безпекових загроз є безпрецедентними.

Питання безпеки покладені в основу «Угоди про Європейський Союз» та є основоположними для функціонування усієї системи Союзу. Безпека проголошена фундаментальною цінністю в другій статті угоди, а у статті третій визначено, що Союз має за мету пропагувати мир та сприяти добробуту своїх громадян (European Union, 1997). Вочевидь, така амбітна мета нині підштовхує Європейський Союз діяти швидше та набувати нової ролі — постачальника глобальної безпеки, зважаючи на відкриту загрозу військового протистояння з РФ. Може здатися, що такий фокус у європейській політиці є відкриттям XXI ст., але насправді схожу візію можна віднайти, якщо повернутися на сто років у минуле.

Ідея можливості європейського об'єднання виникала у публічних дискусіях та інтелектуальних колах країн Європи в різні історичні періоди. Досить активно вона оприявнювалася в часи криз, політичних негараздів та економічного спаду. До прикладу, у міжвоєнний період помітним представником цієї амбітної ідеї був віденський інтелектуал Р. Куденгове-Калерґі. Цей австрійський граф був маніфестантом уявлення про «Пан-Європу». Добре розуміючи загальноєвропейський контекст та поруйнованість держав Європи після Першої світової війни, Куденгове-Калерґі говорив про необхідність економічного відновлення, яке може оформити майбутнє об'єднання. Окрім того, він застерігав європейців від можливої втрати свого місця у глобальній політиці через фінансову могутність американського капіталізму. Куденгове-Калерґі, вочевидь, був утопістом та випереджав свій час, пропонуючи європейцям спільні цінності та символи: від спільного паспорта, прапора та гімну до єдиної валютної системи. Загалом Куденгове-Калерґі чи не найпершим запропонував часто згадувану нині концепцію — Сполучених Штатів Європи, оперту на припинення національного протистояння між європейськими народами. Основою цього європейського «острова» між Британією та Росією (останні лишалися в його

баченні поза можливим об’єднанням) мали бути країни від Лісабона до Варшави (Гончар, 2023).

Особливим завданням було примирити Францію та Німеччину, адже Європа, на думку графа, має значну екзистенційну загрозу зі сходу — Росію. На сторінках його маніфесту чітко зазначено, що російське питання має лишатися у фокусі європейської політики. В іншому ж разі роз’єднані внутрішніми чварами європейські держави можуть бути завойовані цією потугою (Мартинов, 2015). Саме в контексті військової загрози Куденгове-Калерґі визначає другу фундаментальну основу європейського об’єднання — спільний безпековий простір та упорядковану систему відповіді на зовнішні загрози. На його думку, Європа в атомізованому стані є безпорадною у військовому вимірі. Забезпечити стійкість та виживання європейської цілості можливо лише тоді, коли буде утворено єдину військову інституцію із солідарним принципом участі. Відтак військово-політичне об’єднання держав Старого світу на початках було однією із головних ідей перших «пан’європеївців», адже увесь попередній досвід війн у Європі доводив важливість превенції нових військових конфліктів (Гончар, 2023).

Ідеї графа Куденгове-Калерґі не могли бути реалізованими в історичному контексті 20–30-х міжвоєнних років. Європейський континент схилився до авторитарного підходу у внутрішній та зовнішній політиці. Від Португалії з Салазаром до Речі Посполитої Юзефа Пілсудського — першу скрипку грали авторитарні режими та націоналістичні або фашистські рухи. Такий спосіб облаштування політичного життя передбачав закритість та вороже налаштування до сусідів, із якими до того ж були накопичені значні територіальні претензії (достатньо згадати питання про Саарський вугільний басейн). Підігрівала реваншистські настрої й недосконала Версальсько-Вашингтонська система договорів. Ідея Пан-Європи була відкладена у дальню шухляду, а згодом розпочалася Друга світова війна (Гончар, 2023).

Відродження ідеї об’єднання Європи бачимо по завершенню Другої світової. Саме тоді виникає нова загроза — СРСР, на яку західний світ уже буде

змушений реагувати активніше. Цікавим є той факт, що про загрозу радянської Росії граф фон Куденгове-Калерґі попереджав європейців ще на початку 20-х років. Критичною точкою у пошуках нового шляху розвитку для європейців та можливістю почати діалог стало завершення Другої світової війни. Вінстон Черчиль був прихильником європейської унії та широковідомої ідеї про створення Сполучених Штатів Європи. Усвідомлюючи кількість післявоєнних ризиків, включно зі зростанням загрози від СРСР, економічною розрухою, демографічними втратами, єдиним способом гарантувати та забезпечити вільне й стабільне європейське майбутнє було залучення народів Старого світу до співпраці та співтворення (Гончар, 2023)..

Вплив Черчиля на повоєнне облаштування Європи став визначним, проте сам проєкт об'єднаної Європи не одразу отримав свою завершену форму. В 1946 році Черчиль заявив, що «від Щецина на Балтиці до Трієста опустилася залізна завіса» (Wolff, 1994). В просторі ментального картографування відбулося створення нових категорій — постала Європа, розділена на східну та західну. Вплив Холодної війни та тривале протистояння ідеологічно непримиренних супротивників — Сполучених Штатів та Радянського Союзу — ще глибше вкорінювали думку про неоднорідність Європи; таким чином великий європейський проєкт був тимчасово неможливим.

Цю концептуальну хибу намагався осмислити Мілан Кундера, котрий у своєму есеї «Трагедія Центральної Європи» проілюстрував байдужість Заходу в питанні країн Європи, що опинилися в радянській сфері впливу. Він жалкував про те, що ці терени вирвані із європейського контексту та великою мірою «вкрадені» Радянським Союзом (Кундера, 1984). Своєю промовою Вінстон Черчиль позначить новий кордон між Заходом та Радянським Союзом, а згодом, того ж року, в університеті Цюриха знову нагадає європейцям про необхідність об'єднатися у форматі Сполучених Штатів Європи. Близькість цієї візії до шляху, запропонованого в маніфесті «Пан-Європа», досить легко пояснюється — співавтором промови стане той самий граф фон Куденгове-Калерґі.

В. Черчиль буде чітким прихильником створення нової європейської єдності та запропонує утворити унію, де лідерські позиції матимуть Німеччина та Франція. Це переконання підживлювалося страхом можливого збільшення кількості прихильників комунізму в Європі. Цей страх не був позбавленим сенсу, адже значна частина Центральної та Східної Європи вже була в радянській «сфері впливу», а інша частина Європи була поруйнована роками війни. У схожій ситуації економічної нестабільності, породженої Першою світовою та Великою депресією, соціалізм набував усе більше прихильників у міжвоєнний час (Кузь та ін., 2020).

Заклики Черчиля та графа Куденгове-Калергі все ж були почуті і сприйняті європейцями: 1948 рік увійде в історію європейської інтеграції як рік митного та економічного союзу Бельгії, Нідерландів та Люксембургу. Декілька років по тому, в 1951-му, було оформлено Європейське об’єднання вугілля і сталі. З цього часу і до утворення Європейського Союзу процес євроінтеграції відбувався за економічною логікою. Певний міф про ЄС як інституцію, що була утворена внаслідок економічного об’єднання та взаємного економічного інтересу, є досить поширеним у публічному та науковому просторі до сьогодні. Однак не варто забувати спадщину Р. Куденгове-Калергі та всіх прихильників пан’європейського руху, котрі під час перших спроб обґрунтувати необхідність європейського об’єднання наполягали на спільних безпекових правилах та єдиному військовому плануванні (Гончар, 2023).

Лише російське повномасштабне вторгнення в Україну відродило давні ідеї про відновлення військової і безпекової сили Європи. В оновлених стратегіях та заявах європейських політиків ЄС усе частіше розглядається як геополітичний гравець, котрий прагне до глобальної стабільності та повернення на лідерські позиції на світовій шахівниці. Водночас економіка лишається важливим чинником європейської політики — вона впливає на електоральні уподобання виборців та є джерелом активних політичних дебатів. Усередині ЄС усе більше усвідомлюють важливість вироблення нового підходу в реагуванні на зовнішні загрози. В європейському «Стратегічному компасі» від 2022 року визначається,

що ЄС прагне розширити власні військові можливості та створює військовий корпус швидкого реагування; запроваджується механізм регулярних спільних навчань та заявлене поглиблення співпраці з партнерами на базі міжнародних євроатлантичних структур, таких як НАТО. Загалом цей документ передбачає 12 кроків, які посилюють ЄС із безпекової та військової точок зору (A Strategic Compass for a stronger EU security and defence, 2022).

Цей помітний стратегічний поворот, вочевидь, є новою та важливою віхою в історії європейського інтеграційного проєкту: в ці дні ЄС повертається до первинної, але забутої у 20-ті роки XX століття візії — Європи як провідного постачальника безпеки та глобальної стабільності. Геополітична реальність, яка оформилася після Другої світової війни, диктувала необхідність відгородитися від впливу «країни рад» та комуністичної ідеології. Страх посилення комуністичного руху в зруйнованій війною Європі призвів до того, що значна частина країн нинішнього Європейського Союзу надовго лишилася поза європейським інтеграційним процесом.

Таким чином, політичні рішення минулого заклали частину сучасних викликів, адже досі відчутна нерівність між тими державами, котрі опинилися під впливом СРСР, та державами на захід від «залізної завіси». Ця нерівність проявилася на рівні економічного розвитку, у рівні зрілості інституцій чи, наприклад, у ставленні суспільства до корупції, основних принципів демократії тощо. Навіть об’єднання двох частин Німеччини стало непростим завданням, попри значні успіхи Західної Німеччини в демократизації та побудові сильної економічної моделі.

Поразка Радянського Союзу в Холодній війні та розпуск ОВД лише тимчасово призупинили протистояння двох полярних систем та подарували новоствореному європейському об’єднанню час для свого інституційного становлення. Разом із тим ЄС отримав у спадок значний перелік викликів, спричинений перебуванням різних частин Європи у двох протиборчих системах. В умовах наростання нової напруженості у світі ці культурні та ідеологічні розбіжності всередині європейської спільноти стають поживним ґрунтом для

діяльності євроскептиків та політичних режимів, які ззовні прагнуть розколоти та ліквідувати ЄС.

Тривалий період миру в Європі після Другої світової війни сформував у європейській політичній думці набір упереджень, які применшували значення військової сили у сфері безпеки ЄС. Війни в Югославії не призвели до переоцінки потенційних військових загроз для Європи, переважно й з причин, описаних вище, адже Балканський регіон в уявленнях західних європейців і не належав до того, що окреслюється як «європейський простір». Ця ситуація, додатково підсилена хибним фокусом на тому, що ЄС має тримати у центрі уваги лише економічне процвітання і підвищення добробуту європейських громадян, створила екзистенційну загрозу для усього об'єднання європейських держав. Для ЄС збройна агресія Російської Федерації проти України, вочевидь, стала несподіваною ілюстрацією стратегічної помилки — нехтування потенційними загрозами застосування сили проти ЄС або країн-партнерів.

Російська війна проти України демонструє готовність недемократичних режимів застосовувати військову силу як інструмент відновлення старих претензій та є продовженням ревізіоністської політики, яка в сучасних реаліях поєднана з гібридною тактикою, кібератаками, зовнішнім інформаційним маніпулюванням, економічним та енергетичним тиском, ядерною риторикою. Ці агресивні та ревізіоністські дії серйозно та прямо загрожують порядку європейської безпеки та безпеці європейських громадян, адже Російська Федерація послідовно дотримується радянської ідеї моральної та військової переваги над Європою та реалізує власні амбіції не лише в Європі, але і на інших театрах, де ЄС має свої політичні та економічні інтереси. Відтак, жодна з країн Європи, яка зараз є членом Європейського Союзу, не може перебувати в цілковитій безпеці. Існування мілітаризованої Росії, головним завданням якої лишається утримання своєї зони впливу, є однією з глобальних екзистенційних військових загроз для Європейського Союзу та його асоційованих членів.

Європейський Союз за час свого існування вже неодноразово стикався з наслідками військових конфліктів в безпосередній близькості до своїх

сухопутних та морських кордонів. Придністровський конфлікт, російсько-грузинська війна 2008-го, вторгнення Російської Федерації в Україну в 2014-му та повномасштабне вторгнення в лютому 2022-го року, війна в Сирії та довготривалі наслідки війни на Балканах. Кожен із цих конфліктів впливав та впливає на політичну та економічну стабільність Європи – зростають загрози міжнародної злочинності та тероризму, міграційні хвилі породжують соціальне напруження в середині країн-членів та підживлюють популярність ультраправих партій. Окрім того, зростають видатки на військову сферу та на заходи із переорієнтації енергетичного сектору та відмову від російських енергетичних ресурсів.

Питання захисту кордонів та всього європейського простору лежить не лише в площині прямих військових загроз. Відсутність внутрішніх кордонів та митниць в середині Союзу – суттєва перевага як з економічного боку, так і з ідеологічного: свобода пересування, можливість обирати країну проживання, вільне перетікання працездатного населення між країнами витворює унікальний простір свободи та економічної співпраці. Жан Моне – французький економіст та дипломат, ще один представник когорти «батьків Європи», вбачав в такій інтеграції шлях до консенсусу та створення спільних «правил гри» між європейськими державами. Разом із тим, спільний кордон і його контроль – проблемне питання, яке впливає на стійкість усього Союзу (Моне, 2017). Принципи, закладені в фундамент об’єднання європейських держав, переживають тривалий етап випробування часом та зовнішніми акторами. Багатовікова історія спроб об’єднання Європи силовим шляхом, зрештою, дозволила європейським урядам переглянути власні стратегії та заснувати нового політичного гравця, в основі якого лежить принцип спільних цінностей та інтересів. Саме ця основоположна ідея нині перебуває під безперервним тиском з боку сил, що мають вагу як усередині Унії, так і поза її межами.

До повномасштабного вторгнення Російської Федерації в Україну в лютому 2022-го року тема біженців була однією із найпомітніших в європейській політиці й нерідко підігрівалася ззовні через соціальні мережі, ЗМІ та голосами

різних політиків. В середині Унії країни-члени мають різне ставлення до відчутних хвиль міграції. Тривалий час основними напрямками, звідки прибували біженці, були країни Близького Сходу; окрім того, велика частина мігрантів потрапила на територію ЄС під час війн в Югославії, так само і в 2022-му році значна частина українців прибула до країн ЄС у пошуку притулку.

Напруження викликає нерівномірна включеність держав у процес розселення біженців та їхньої подальшої адаптації. В Європейському Союзу існує практика обов'язкових квот розподілу шукачів притулку, і такий підхід влаштовує не усі країни. Деякі з країн Східної Європи виступали проти квотного принципу, коли це питання гостро постало в 2015-му році під час однієї з найбільших «мігрантських криз». Фінансова та політична підтримка Російською Федерацією правих популістських націоналістичних партій, таких як «Національне об'єднання» Франції, «Північна ліга» в Італії, Партія свободи Австрії, «Фідес» в Угорщині та «Альтернатива для Німеччини», спрямована на створення умов соціального напруження. Російська сторона використовує повільну реакцію провідних політичних партій Європи на виклики, пов'язані з міграцією та адаптацією утікачів від війни, на свою користь (Корольчук, 2019).

Європейський Союз реагує на зростаючий рівень викликів та загроз, оновлюючи свою законодавчу базу та поступово формуючи нове стратегічне бачення власної безпеки. В червні 2020-го року вперше в історії ЄС розпочався процес аналізу різноманітних загроз та пошук можливих стратегій і пріоритетів для кожної країни-учасниці об'єднання. В підсумковому документі, який був першим кроком до підготовки нової безпекової стратегії ЄС, були визначені ключові безпекові загрози: конфронтація між глобальними гравцями та блоками, конфлікти в державах, що межують із Союзом, загрози, пов'язані із державними та недержавними політичними акторами. В цьому документі також відзначалися визначні тренди, які можуть вплинути на стабільність ЄС: від загальмовування глобалізації, економічного суперництва між світовими лідерами до атак, направлених на європейські країни із застосуванням руйнівних технологій,

дезінформації та інших невійськових способів впливу або терористичних загроз (A Strategic Compass for a stronger EU security and defence, 2022).

Ця стратегія мала бути впроваджена протягом двох років і адаптована на початку 2022-го року. Її фінальним документом є «Стратегічний компас», який має оновлюватися кожні три роки. Вочевидь, це свідчить про готовність ЄС реагувати на мінливе середовище та, великою мірою, є прямою дією, спрямованою на відновлення геополітичного впливу Європи (Council of the European Union, 2022). Завершення підготовки «Стратегічного компасу» припало на повномасштабне вторгнення Російської Федерації в Україну. В передмові до документу Голова Європейського парламенту Жозеп Боррель відзначає, що Європа стикнулася зі значною небезпекою після російського вторгнення, а ситуація на континенті вимагає рішучої відповіді від ЄС. На думку Борреля, «історія знову пришвидшилася», втім, ЄС має бути готовим захищати свою безпеку та безпеку своїх партнерів. В цій передмові голова Європейського парламенту приділяє увагу і новим загрозам: перетворення енергетики на зброю та деструктивний вплив Росії на Європу через енергетичний шантаж. Жозеп Боррель відзначає важливість європейських інтересів на Західних Балканах, Північній Африці, Близькому Сході та в Індо-Тихоокеанському регіоні, проблему інструменталізації мігрантів в політичних цілях, приватизацію армій та гібридні кампанії з дезінформації. В кіберпросторі, говорить голова Європарламенту, теж відбувається атака на «глобальну спільність», тому захист Європи потребує нового, комплексного концепту цифрової безпеки.

Разом із тим, цей стратегічний документ не є лише відповіддю на війну в Україні; по своїй суті – це рамковий трансформаційний інструмент ЄС, який тепер має у своєму фокусі не лише економічне процвітання (котре було основою об’єднання після Другої світової війни), але й підсилення безпекового елементу в наступні десять років. «Стратегічний компас» задає та описує набір дій та ключових принципів, яким має слідувати Союз. Діяти більш швидко та рішуче під час криз; захищати громадян від загроз, що швидко виникають; інвестувати в спроможності та необхідні технології; діяти в партнерській логіці із іншими

країнами, досягаючи спільних цілей. Конкретність і визначені часові рамки, запропоновані в цьому документі, демонструють намір Європейського Союзу стати впливовим «постачальником безпеки» у наступному десятилітті.

Для того щоб підкріпити свої наміри конкретними діями та підсилити власні можливості, ЄС розгортає 5000-й Корпус швидкого реагування. Для підсилення готовності військ відбуватимуться постійні навчання та заходи із підсилення спроможностей командування. Поруч із розгортанням спільного війська влада Європейського Союзу визнає, що має ефективніше протидіяти кіберзагрозам та дезінформації. Крім того, «Стратегічний компас» визначає, що має бути створений новий гібридний інструментарій та спеціальні підрозділи з кібербезпеки та цифрової дипломатії, а також інструментарій протидії іноземним інформаційним операціям. Російська Федерація та Китайська Народна Республіка визначені як джерело гібридних загроз, в тому числі навіть у космічному просторі. Протягом наступних років відбуватиметься поступовий процес удосконалення політик та інструментів, формування Об'єднаного кіберпідрозділу ЄС, котрий має запобігати атакам у цифровому просторі. Відтак, цифрові технології поряд із військовими загрозами розглядаються в «Стратегічному компасі» як одна із основних загроз для політичної стабільності та стійкості Європейського Союзу.

Таким чином, в «Стратегічному компасі» запропоновано всього близько 12 кроків, які мають посилити сферу безпеки:

1. Посилити цивільні та військові місії та операції, надавши їм більш надійні та гнучкі повноваження для більш гнучкого процесу прийняття рішень.
2. Розгортання Корпусу швидкого реагування ЄС, який дозволить швидко розгорнути до 5000 військових, які зможуть протидіяти різним типам загроз.
3. Зміцнити командні та контрольні структури, зокрема військові, а також запровадити регулярні навчання.

4. Розвивати розвідувальні можливості, такі як Єдина система розвідки та аналізу ЄС (SIAC), для покращення стратегічного аналізу та прогнозування.
5. Створення інструментарію протидії гібридним загрозам в цифровому середовищі.
6. Подальший розвиток Політики кіберзахисту ЄС, щоб бути краще підготовленими до кібератак і реагувати на них; посилення дій в морській, повітряній та космічній сферах, зокрема шляхом розширення Скоординованої морської присутності на інші території, починаючи з Індо-Тихоокеанського регіону, і шляхом розробки Космічної стратегії ЄС для безпеки та оборони.
7. Збільшення витрат на оборону та покращення підходів до планування.
8. Пошук спільних рішень в технологічній галузі: таких як високоякісні військово-морські платформи, новітні бойові авіаційні системи, засоби космічного базування та основні бойові танки.
9. Інвестування в технологічні інновації для оборони та створення нового Центру оборонних інновацій у рамках Європейського оборонного агентства.
10. Зміцнення стратегічного партнерства з НАТО та ООН шляхом політичного діалогу, а також оперативної та тематичної співпраці.
11. Розширення співпраці з регіональними партнерами. Розширення співпраці з двосторонніми партнерами, які поділяють спільні з Союзом цінності та інтереси, такими як США, Норвегія, Канада, Великобританія та Японія. Розвиток партнерств на Західних Балканах, Африці, Азії та Латинській Америці.
12. Розробка Форуму партнерства ЄС у сфері безпеки та оборони для більш тісної та ефективної співпраці з партнерами для вирішення спільних проблем.

В «Стратегічному компасі» визначено, що ЄС прагне до глобальної стабільності, яку можна досягти лише в синергії із союзниками, котрі сповідують

схожі цінності. Акцент робиться на трансатлантичних відносинах і партнерстві із сусідніми з ЄС регіонами, що відображає їх особливу важливість для блоку. Таким чином, в Європейському Союзі відбувається перегляд старих принципів взаємодії з НАТО та США – в бік більшої та глибшої співпраці у військовому вимірі (A Strategic Compass for a stronger EU security and defence, 2022).

«Стратегічний компас» позиціонує ЄС як сильного трансатлантичного партнера, що дуже контрастує з певним скептицизмом щодо НАТО, який був відчутний у європейській політиці та риториці роками раніше. Натомість, як неодноразово наголошується в документі, впровадивши 12 кроків, ЄС стане цінним партнером як для НАТО, так і для США. Для Сполучених Штатів як одного із головних донорів НАТО такий стратегічний поворот є важливим свідченням якісного нового підходу Європи до своєї безпеки. Крім того, увага приділяється Африці, зокрема Північній та Західній її частинам, а також безпосередньому сходу ЄС. Африка неодноразово згадана як регіон першочергового геостратегічного значення для ЄС, оскільки нестабільність на континенті впливає на Союз (A Strategic Compass for a stronger EU security and defence, 2022).

Додатковим джерелом можливої геополітичної нестабільності, яка суттєво вплине на ЄС, є КНР та постійна загроза ескалації військового конфлікту з Тайванем. Вочевидь, велика частина європейських країн може бути втягнута у це протистояння в статусі країн-членів НАТО. В середині ЄС існує бачення того, що наразі Китай є партнером для співпраці, але разом із тим і економічним конкурентом та системним суперником. Діалог з Китаєм важливий для ЄС через пов’язаність ринків та логістичних ланцюжків, водночас ця взаємодія є асиметричною і часом може бути загрозливою для національної безпеки європейських держав. Китай все більше грає з позиції сили та активно включений у створення регіональної напруженості навколо Тайваню. Китай також нарощує свої спроможності в економіці та демонструє здатність обмежувати доступ до свого ринку, а також активно просуває власні інтереси у світі, шляхом надання державам кредитів та формуючи економічні блоки на кшталт БРІКС. Ця стратегія

реалізується через різноманітні заходи, включаючи розширення своєї присутності в морському і космічному просторі, застосування кіберінструментів та розробки гібридних тактик впливу. Крім того, Китай суттєво розвиває свої військові засоби та прагне завершити загальну модернізацію своїх збройних сил до 2035-го року, що вплине на регіональну та глобальну безпеку (Drozdiak, 2019).

Розвиток китайських технологій та інтеграція в глобалізований світ визначатиме політичну стабільність протягом наступних десятиліть – Європейський Союз, в свою чергу, змушений враховувати активність Китаю, будуючи свою стратегію на найближчі роки. Економічний вплив Китаю досить швидко набуває сильного політичного впливу, поглиблюючи старі, згадані вище, розколи між Сходом та Заходом у європейському політичному просторі. Ці загрози системно розглядаються американськими аналітичними центрами, зокрема одним із найбільших аналітичних центрів у США – Rand Corporation. В своїх аналітичних записках дослідники визнають, що Китай займає важливі стратегічні позиції в Європі шляхом розширення своєї присутності на європейських ринках. Відповідно, що більше позицій Китай здобуде в Європі, тим простіше йому буде кинути виклик політичному суверенітету та інтелектуальній свободі європейців (Wyne & Harold, 2020).

До прикладу, в регіоні Центральної і Східної Європи декілька держав ЄС розглядають можливість співпраці із Китаєм, намагаючись залучити китайські інвестиції. Ще в 2012-му року в Будапешті був заснований формат співпраці КНР з Центрально-Східною Європою, котрий відбувається за формулою «17+1». Саміти у цьому форматі відбувають із щорічною інтенсивністю, офіційною метою цієї групи є сприяння розвитку торгівлі та інвестиційних зв'язків, культурних зв’язків тощо. Європейські країни вбачають в цьому партнерстві вигідні умови для побудови власної інфраструктури: портів, міждержавних магістралей та швидкісних залізничних колій. В свою чергу КНР отримує доступ до купівлі виробничих потужностей цих країн, наприклад, цивільної частини машинобудівного заводу у Польщі – «Huta Stalowa Wola» (Drozdiak, 2019).

Потенційні гібридні загрози для європейських урядів можуть надходити також із області китайських високих технологій. Один із яскравих прикладів – спроба Китаю отримати можливість встановити мобільні мережі п'ятого покоління у Великобританії, на що зреагували уряди Британії та Німеччини, висловивши своє занепокоєння. Урядовці цих країн допускають, що надати можливість компанії Huawei будувати інфраструктуру для 5G зв'язку означає поставити під загрозу власне цифрове середовище. Наприклад, Huawei заборонено постачати своє обладнання 4G і 5G чотирьом основним телекомунікаційним операторам США. Наприкінці 2018-го року уряд Японії теж заборонив державні закупівлі обладнання Huawei та ZTE, а Австралія та Нова Зеландія заборонили цим компаніям долучитися до розгортання цих новітніх мереж у своїх країнах. Національне агентство з кібербезпеки та інформаційної безпеки Чехії (NCISA), серед інших, визнало Huawei та ZTE можливим джерелом кіберзагроз, що відповідним чином позначилося на потенційних контрактах для цих кампаній в Чехії (Heath, 2019).

На цьому тлі варто згадати, що КНР має власне законодавство в питаннях телекомунікаційних мереж – китайський ринок лишається закритим для іноземних компаній, які пропонують такі рішення. Крім того, всі китайські компанії, включно з Huawei, працюють в політичному полі, яке організовує Комуністична партія Китаю. Запорукою успішності цих компаній є співпраця із партією та дотримання китайських законів і вимог до бізнесу. Серед законів, які можуть впливати на їхню роботу, можемо згадати «Закон Китаю про національну розвідку» від 2017-го року, який прямо вимагає від «усіх організацій і громадян» «підтримувати, допомагати та співпрацювати з державною розвідкою». Інший закон – «Закон Китаю про боротьбу зі шпигунством» від 2014-го року – так само стверджує, що «організації та особи» «не повинні відмовлятися» надавати інформацію під час антишпигунського розслідування (Tanner, 2017). Ці закони не роз'яснюють можливої широти «розвідувальної» та «антишпигунської» роботи, що може бути прямим сигналом до непрозорості дій китайського уряду для європейських держав (Heath, 2019).

Водночас не всі європейські держави мають однакову політику щодо китайських цифрових компаній. Huawei, до прикладу, протягом багатьох років співпрацює, зокрема, з німецькими постачальниками телекомунікаційних послуг. Ця співпраця породжує дискусію в середині Німеччині та інших європейських країнах стосовно впровадження мережі 5G і свідчить про зростаючу чутливість Європи до питань, які стосуються балансу між бізнес-інтересами та потребами безпеки в галузі цифрових технологій та штучного інтелекту (Wagstyl, 2016).

Прийдешня хвиля інновацій викликає в Європі жваве обговорення через пересторогу технологічної «колонізації» з боку передових корпорацій, котрі належать Китаю та США. Основне питання цих обговорень – чи варто залишати вільний доступ на ринках у критичних секторах, чи ж варто прийняти закони для збереження та захисту власних цифрових систем. Сучасний європейський ринок має розвинене виробництво в різних секторах: від ядерної енергетики, автомобілебудування, біотехнологій до виробництва чипів чи хімічної промисловості, проте європейські чиновники усвідомлюють, що в сфері цифрових технологій та новітніх розробок, як 5G-обладнання, Європейський Союз вже відчутно відстає від своїх партнерів. Цю ситуацію загострює і відтік навчених та кваліфікованих кадрів до інших країн, які після закінчення навчання в європейських інженерних школах від'їжджають за кордон працювати, наприклад, у Сінгапурі чи Силіконовій долині (Huawei Cyber Security Evaluation Centre [HCSEC] Oversight Board, 2018).

Цю ситуацію ілюструє звіт від 9 жовтня 2019-го року, в якому Європейський Союз представив документ, що має назву «Скоординована оцінка ризиків кібербезпеки мереж 5G». В цьому звіті йдеться про те, що технології 5G є ключовими у подальшій цифровій трансформації ЄС, але разом із тим несуть в собі деякі ризики. Одним з таких ризиків визнаються сценарії, коли ворожі треті країни можуть чинити тиск на постачальників 5G-обладнання та сприяти кібератакам, послуговуючись своїми власними національними інтересами. Укладачі звіту стверджують, що цей ризик напряму залежить від того, до якої міри постачальник обладнання має доступ до мереж і є залежним від політичної

кон’юнктури. Ба більше, допускається ймовірність того, що розробники цих мереж цілеспрямовано можуть лишати «слабкі» місця в захисті цього обладнання, що дозволить третім силам легко отримати до них доступ (NIS Cooperation Group, 2019)

У збільшенні власної суб’єктності КНР на цей час опирається на власну економіку та намагається нарощувати коло союзників через дипломатію та торгівлю. Нинішня ж Російська Федерація дотримується принципу правонаступництва зниклого СРСР; ба більше, російські еліти добре відчувають бажання власного народу до відновлення «історичної справедливості». Росія не відмовилася від військового панування, якнайменше у Східній Європі, та повсякчас намагається переграти результати Холодної війни. Реакція на агресивну стратегію Російської Федерації оформлена в стратегічних документах Європейського Союзу.

В ЄС відзначають, що головним прагненням Союзу завжди було прагнення зберегти справедливий міжнародний порядок, де в основі відносин лежать рівні права, права людини, свободи та універсальні цінності у міжнародному праві. В свою чергу, Російська Федерація, розгорнувши агресивну війну проти України, грубо порушує міжнародне право та принципи Статуту ООН, підриває європейську та світову безпеку та стабільність. Прагне до руйнування цих універсальних цінностей, на яких був заснований Європейський Союз, застосовуючи політику «права сильного». Таким чином, в європейському «Стратегічному компасі» визначено, що в сучасному світі існують сили, котрі кинули виклик системі безпеки західних країн; вони прагнуть збільшити свою «сферу впливу» із застосуванням примусу та сили, і Російська Федерація, разом із КНР, є однією із цих сил (A Strategic Compass for a stronger EU security and defence, 2022).

Від часу приходу Володимира Путіна до влади у 2000-му році Російська Федерація прагнула урівноважити свої можливості в традиційному військовому секторі шляхом розробки стратегій асиметричної боротьби. Влада РФ зробила акцент на нові методи гібридних атак: серед них дезінформаційні кампанії в

соціальних мережах, кібератаки, фінансування проросійських сил та рухів, торгові війни в Україні та країнах Балтії або підтримка праворадикальних сил у Західній Європі. Особливо активно Росія застосовує методи інформаційної війни в соціальних мережах з метою дестабілізації сусідніх держав та підривання довіри до західних урядів. Зокрема, у «Доктрині Герасимова», названій за прізвищем генерала та радника Володимира Путіна Валерія Герасимова, пропонується стратегія «розмивання різниці між війною та миром». Герасимов підкреслює, що політичне втручання, інформаційна війна та інші неконвенційні заходи можуть спільно та асиметрично використовуватися для підриву потужності Європи, Сполучених Штатів та інших супротивників (Jeangène Vilmer et al., 2018).

Російська Федерація за останнє десятиліття постійно практикує методи гібридного впливу, атакуючи західні структури та цінності. Україна та країни Балтії стали лабораторією для тестування цих методів. Крім системного інформаційного тиску через соціальні мережі, РФ активно послуговується втручанням у кіберпростір інших держав. На російські спроможності здійснювати кібератаки вперше звернули увагу ще в 2007-му році, коли естонські банки, урядові органи, ЗМІ та політичні партії стали ціллю постійних кібератак, здійснюваних із РФ. Після цих кібератак Естонія вирішила взяти на озброєння добровільний підрозділ, який можна використовувати для оборони кіберінфраструктури країни. Учасники цього підрозділу виділяють свій вільний час на регулярні тренування, в ході яких вони практикують захист від різних видів загроз: від онлайн-банкінгу до систем електронного голосування.

До інциденту кібератаки серйозно не розглядалися як безпосередня загроза для держави, її громадян чи всієї європейської спільності. Не існувало алгоритму поведінки чи універсальних політик протидії подібним атакам. Наприклад, не було визначено, чи такий вид злочину кваліфікуватиметься як напад на державу-члена НАТО і, отже, чи активуватиме колективну оборону згідно зі статтею №5. Не було навіть зрозуміло, чи може держава в законний спосіб реагувати на кібератаки. Естонія активно ділиться своїм досвідом та навчальними програмами

з іншими країнами-членами НАТО, а також організовує систематичні семінари щодо кібербезпеки, на яких союзники отримують навички реагування на симульовані кібератаки у реальних сценаріях, таких як відключення серверів, розповсюдження фейкових новин у соціальних мережах та вторгнення хакерів (Traynor. 2007).

Схожим чином на загрози, що походять із цифрового середовища та соціальних мереж, реагує ще одна країна ЄС – Королівство Швеція, котра одразу після анексії Росією Криму розпочала поступове відновлення структур та агенцій, пов'язаних із протидією пропаганді, що діяли в країні під час Холодної війни. Насамперед варто відзначити, що протидія інформаційним війнам є важливим елементом державної політики Швеції: це питання є фокусом спеціальних відомств і міністерств. На офіційному ресурсі Міністерства оборони Швеції можна знайти пряму мову Улофа Скуга на брифінгу Ради Безпеки ООН від 8 лютого 2018 р. Ця промова стосується загроз міжнародному миру та безпеці, спричинених терористичними актами. У ній шведський представник наголошує, що запобігання насильницькому екстремізму залишається критично важливим і має розглядатися як довгострокове завдання, над яким Швеція працює як всередині країни, так і в міжнародному полі (Skoog, 2018).

Важливим є і інший аспект цієї промови: він звертає увагу, що використання терористами інформаційно-комунікаційних технологій і соціальних медіа викликає все більше занепокоєння і є серйозним викликом для держави, адже впоратися із цим явищем необхідно ефективно, але не порушуючи повагу до прав людини чи верховенства права. У. Скуг відзначає, що Швеція зобов'язана захистити громадян, одночасно забезпечуючи глобальне підключення до мережі та відкритий, вільний, безпечний потік інформації. Ті самі права, які люди мають офлайн, також повинні бути захищені онлайн, зокрема й свобода вираження поглядів (Skoog, 2018).

Питання інформаційної та цифрової безпеки також є частиною проактивної стратегії Міністерства оборони Швеції. Періодично відомство публікує інформацію стосовно дезінформації, яка поширюється в соціальних мережах.

Один з прикладів, на який відреагувало Міністерство, – це поширення чуток і дезінформації про урядові ініціативи. Наприклад, в 2022-му році Міністерство оборони Королівства Швеція відзвітувало, що в шведських соціальних мережах поширюється неправдива інформація про те, що з мусульманських общин зникають діти, яких без законних підстав нібито забирають соціальні служби. В такий спосіб, йдеться в повідомленні міністерства, під загрозою опиняються працівники цих служб, які можуть зазнати агресивного ставлення до себе, та діти, котрі потенційно можуть не отримати необхідної допомоги.

Таким чином, відбувається нарощування соціального напруження в середині шведського суспільства та підривається легітимність та довіра до урядових структур в уявленні однієї з найбільших релігійних спільнот Швеції. Відомство повідомляє, що кампанія триває від зими 2021-го року а співробітники соціальних служб отримували протягом певного часу отримують погрози (Government Offices of Sweden, 2023). Для нас цікава й інша сторона цього звіту, де йдеться про те, що Міністерство оборони доручає розробити засоби протидії цій інформаційній кампанії спеціальним інституціям – Шведському агентству психологічного захисту та Агентству з питань надзвичайних ситуацій (MSB). Обидва відомства на постійній основі готують матеріали та стратегічні документи, які покликані захищати шведських громадян перед обличчям сучасних інформаційних небезпек («Swedish Psychological Defence Agency», 2023).

Агентство з питань надзвичайних ситуацій відповідає за допомогу суспільству в підготовці до великих аварій, криз і наслідків війни. З метою заглиблення в особливості роботи цього відомства з інформацією та соціальними мережами можна проаналізувати «Комплексний план із кібербезпеки 2019–2022», оприлюднений Агентством. У звіті наголошено, що інформаційна та кібербезпека – це відповідальність кожного та кожної в суспільстві. Цей план має 77 пунктів, які покликані зміцнювати безпеку цифрового середовища та захищати шведське суспільство. План визначає шість стратегічних пріоритетів, які уряд Швеції визначив найважливішими в сфері цифрової безпеки: –

забезпечення систематичного та комплексного підходу до заходів із кібербезпеки; – підвищення безпеки мереж, продуктів і систем; – розширення спроможності запобігати, виявляти та протидіяти кібератакам і подібним інцидентам; – підвищення можливостей запобігання та протидії кіберзлочинності; – підвищення рівня освіченості громадян та сприяння розвитку експертності; – розширення міжнародного співробітництва («Swedish Civil Contingencies», 2019).

Ці пріоритети, вочевидь, розширюють безпекову рамку, закладену в шведську доктрину «Тотальної оборони», відновлену королівством у 2015 р. Концепція з'явилася в часи Холодної війни, з урахуванням потенційного конфлікту з країнами Варшавського договору, та мала на меті підготувати й залучити все суспільство до протидії силам ворога. Навіть нова переосмислена версія цієї оборонної концепції передбачає, що кожен у віці від 16 до 70 років може бути задіяним у протидії супротивнику. Напад Росії на Україну в лютому 2022 р. пришвидшив шведські інвестиції в переозброєння сил оборони та її курс на приєднання до НАТО (Ministry of Defence», 2021). Важливо, що оновлена шведська концепція «Тотальної оборони» враховує нові загрози, пов'язані з кіберпростором і значним рівнем оцифрування соціального життя. Одним із ключових прийомів потенційного противника, згідно з цією доктриною, є використання нових засобів масової інформації та соціальних мереж для ведення психологічної боротьби. Тому відновлення концепцій часів Холодної війни потребує додаткового зосередження на психологічному захисті суспільства від пропаганди, яка має на меті послабити волю шведського суспільства до спротиву.

Для досягнення бажаного ефекту в різних екстремальних умовах, включно із війною, важливою є робота зі суспільною свідомістю та готовністю протистояти дезінформації ще до початку таких криз. Тому не дивно, що серед інструкцій про те, як підготуватися до перших найважчих днів військового конфлікту, шведська влада вчить громадян, як не потрапити в оману фейковими новинами (Bryant, 2022). Додатково, для реалізації стратегічних оборонних доктрин, у королівстві працюють профільні структури, котрі забезпечують роботу з громадянами на

різним рівнях. Однією із таких інституцій є Агентство з питань надзвичайних ситуацій (MSB), яке в 2015 р. оприлюднило документ з назвою «Інформаційна безпека – тренди 2015: шведська перспектива». По суті, це документ, що покликаний окреслити рамку того, як держава діє в сфері інформаційної політики, які загрози та виклики має. З цього документу ми розуміємо, що для шведського уряду інформаційна безпека – це завжди про консенсус із іншими цінностями. Документ визначає, що інформаційна безпека нині належить не до сфери наукової зацікавленості технологіями, а є потужним інструментом для осіб, які формують управлінські рішення та є відповідальними за сектор безпеки та оборони («Swedish Civil Contingencies Agency», 2015).

Автори документу відзначають, що суперечливі цілі та неможливість діяти шляхом простих рішень в галузі інформаційної політики зумовлюють складність управління та вимагають нових підходів до роботи з інформацією. Одна з найважливіших візійних змін у підході до функціонування соціальних мереж – це примітка про те, що відбувається поступове зміщення акцентів у роботі з соціальними мережами: від захисту економічної та соціальної діяльності, притаманної більш мирному часу, до більш глобальних викликів, які загрожують національній безпеці (від втручання у вибори до проведення кібератак на об’єкти критичної інфраструктури). У питанні інформаційної безпеки шведські посадовці роблять акценти не лише на захисті мереж від вірусів або збереженні таємниць: вони розглядають цифрове середовище та соціальні мережі як життєво важливий для функціонування суспільства інструмент, який підвищує конкурентоспроможність економіки та є міцною основою процвітання держави.

Одна з важливих частин доповіді присвячена геополітичному виміру інформаційної безпеки. Автори документу достатньо широко описують виклики нової реальності, в якій соціальні мережі та дезінформація існують поряд із військовими конфліктами, електоральними циклами та протестними рухами. Інформаційні операції в соціальних мережах відтепер доповнюють військові дії; йдеться насамперед про анексію Криму Російською Федерацією в 2014 р. Відзначається, що вагому частину в успішності цієї операції зіграли саме

спеціальні інформаційні операції, а найближчий схожий приклад застосування мереж та дезінформації можна було зустріти в часи активності «Ісламської держави». Таким чином, в Агентстві з питань надзвичайних ситуацій Швеції визнають, що перетворення інтернету та соціальних мереж на своєрідний вид зброї зумовлює нові правила гри у міжнародній політиці:

1. Інформаційні операції, в яких інтернет-пропаганда поєднується з дипломатією, традиційними військовими діями, уведення противника в оману – стали звичним явищем у збройних конфліктах.
2. Кібершпигунство та кіберсаботаж є частиною «набору інструментів політики безпеки» у все більшій кількості країн.
3. Збільшення можливостей для вільної та неконтрольованої комунікації через Інтернет призвело до негативної реакції в багатьох країнах зі спробами ізолювати їхні національні мережі від Інтернету.

Ще один важливий висновок з аналізу цього документу – це всеохопність питання інформаційної безпеки і впливу соціальних мереж на суспільство. Окрім військового та політичного аспектів, що цікавить нас найбільше, автори зупиняються на потенційних ризиках для бізнесу та підприємництва, загрозах міжнародної злочинності, яка також інтегрується в нову цифрову реальність, складнощі для законодавців, що їх викликають питання приватності, зберігання даних і загалом питання дотримання основних принципів демократії та свободи слова.

Ці всі виклики та небезпеки, описані ще в 2015 р., органічно призвели до того, що шведський уряд демонструє системний підхід у протидії новим цифровим загрозам. Представники різних урядових структур Швеції відзначають, що держава зараз стикається зі зростаючою загрозою терактів та потенційних гібридних атак на шведське суспільство, включаючи хакерські атаки та кампанії в соціальних мережах. Відродження доктрини «Тотальної оборони», про що йшлося вище, – один із багатьох елементів державної системи безпеки, в якому вже враховуються небезпеки із цифрового простору (Sundelius, 2023).

Разом із тим, шведські урядовці поновили роботу і над «психологічним захистом» населення. У питанні психологічного захисту громадян Швеція накопичила достатньо великий досвід в силу того, що держава не була членом НАТО, але в часи ідеологічного протистояння з СРСР – опонента зі силою, що значно переважала, – представляла табір демократичних урядів. Від початку поява «психологічного захисту» була відповіддю на психологічну війну, яку ворог потенційно міг вести проти шведів у часи війни. Саме в часи Холодної війни і виник термін «психологічний захист», який в основному використовується у Швеції. По суті, його поява тісно пов'язана із бажанням влади відійти від дещо застарілого і часто негативного терміну – пропаганда, який за часи Другої світової війни та німецького нацистського режиму обріс яскраво негативними конотаціями (Rossbach, 2017).

Цей шведський «винахід», вперше представлений урядовим звітом у 1953 р., виявився вдалим рішенням – достатньо гнучким для того, щоб протягом років захистити фундаментальні принципи свободи і суверенітет Шведського Королівства. Концепція психологічно захисту має три основні компоненти, які відповідно до зовнішнього контексту можуть змінювати свою важливість. Ці три компоненти: – протидія обману та дезінформації, включно з поширенням чуток і пропаганди або будь-яких дій, які може вчиняти супротивник під час розгортання психологічної війни; – забезпечення стійкої та постійної можливості для урядів і владних органів безперешкодно доносити важливу інформацію населенню, включно зі ситуаціями криз та військових дій; – сприяння посиленню волі громадян до захисту Швеції (Rossbach, 2017).

Вочевидь, у профільних відомствах Королівства Швеція існує чітке розуміння того, що без комплексних заходів із психологічного захисту населення протидіяти супротивнику на полі бою буде надзвичайно складним завданням. Будуючи сучасну систему безпеки в Швеції, влада намагалася враховувати досвід комунікації під час Другої світової війни, який не завжди був вдалим, з важливою метою – уникнути звинувачень в намаганні маніпулювати суспільною думкою чи в спробах поширювати «пропаганду». Адже навіть в мирний час у Швеції є

поширеною практика проведення навчань не лише у вигляді військових маневрів, але й інформаційної роботи з громадянами в соціальних мережах («Swedish Civil Contingencies Agency», 2011).

Однією із таких форм підготовки громадян є тренування з психологічного захисту. Протягом 1970-80-х рр. такі заходи відбувалися з певною частотою, і їхньою метою було підвищити обізнаність шведського суспільства про заходи, котрі проводять в рамках роботи концепції «Тотальної оборони». Навіть зважаючи на досить мирні часи, урядовим агентствам доводилося стикатися зі звинуваченнями у веденні пропагандистської діяльності. Разом із тим, добре розуміючи, що супротивник може вести психологічну війну різними засобами та методами, використовуючи сучасні технології, шведські структури з психологічного захисту постійно експериментують зі способами ефективної взаємодії зі своїми громадянами – від проведення прямих етерів і пресконференцій про хід тренувань в 1950-х рр. до сучасних комунікаційних кампаній у соціальних мережах.

Профільна агенція з психологічного захисту завершила свою роботу в 2008 р. Завершення Холодної війни разом із розпадом Варшавського блоку та Радянського Союзу призвела до стабілізації безпекової ситуації, проте перерва в його роботі була недовгою. Незважаючи на збройну агресію Російської Федерації проти Грузії в 2008 р., європейські країни не ставили собі за пріоритет роботу з психологічного захисту населення. Разом із тим, відчутний вплив на шведську політику в цьому питанні спричинила анексія Криму Російською Федерацією. Саме із 2014 р. Швеція розпочала перебудовувати та оновлювати систему «Тотальної оборони», комбінувати класичні військові заходи разом зі заходами щодо психологічного захисту населення (Bryant, 2022). Вже в наступному 2015 р. Агенція із питань надзвичайних ситуацій опублікувала великий звіт про тренди в інформаційній безпеці, який ми розглядали вище. Поступова активізація іноземних держав в цифровому просторі змусила Швецію розпочати роботу з відновлення нової Агенції з психологічного захисту ще в 2016 р., але остаточне

закріплення її важливої функції в системі оборони Швеції відбулося одразу після широкомасштабного російського вторгнення в Україну в лютому 2022 р..

Це системний досвід Швеції як країни-члена Європейського Союзу, засвідчує той рівень стратегічних викликів, з якими нині стикаються усі учасники ЄС. Відзначимо, що уряд Швеції вчасно відреагував на наростаючу загрозу інформаційних операцій з боку Росії, де лютому 2017-го року міністр оборони Російської Федерації Сергій Шойгу оголосив про створення нового роду військ, в якому певні «спеціалізовані підрозділи» будуть вести війну на інформаційному полі. Шойгу наголосив на необхідності ефективної пропаганди, зазначивши, що ці спеціальні війська матимуть потенціал як для оборони, так і для наступу. Це було першим визнанням існування таких сил з боку російського військового керівництва. У минулому радянська комуністична пропаганда, проваджена Москвою, була грубою, неефективною та часто відштовхувала потенційну аудиторію через надмірну ідеологізованість. Проте сьогодні, завдяки вмілому використанню західних соціальних платформ та відсутності ідеологічних обмежень, російські хакери вдало використовують розбіжності в західному суспільстві. Наприклад, вони успішно проникають до різних цільових груп і поширюють повідомлення, котрі підривають довіру до західних урядів (Drozdiak, 2019).

Москва досягла відчутних результатів, ефективно використовуючи західні комерційні цифрові платформи та соціальні мережі, доступні широкому загалу. Наприклад, платформи, такі як YouTube, X (Twitter) та Facebook, використовувалися для поширення недостовірної інформації з метою пропаганди та спотворення західних виборів. Способи, якими Росія веде інформаційне протистояння в соціальних мережах, були сформовані кількома ключовими подіями. На це суттєво вплинула російсько-грузинська війна 2008-го року, коли Грузія фактично випередила Росію в інформаційній війні, змусивши Росію переглянути спосіб, в який вона провадить свої інформаційні операції. Опираючись іноземному вторгненню, Грузія систематично зображувала Росію як агресора, який впливає на світову думку через засоби масової інформації. В свою

чергу, російські спеціалісти з інформаційного впливу не змогли розробити переконливого контрнаративу, за допомогою якого можна було перехопити ініціативу на інформаційному полі.

Вочевидь, від війни в Грузії до початку анексії Криму Росія провела роботу над своїми підходами до ведення інформаційної війни. Після війни в Грузії Росія активувала численні засоби, щоб сформувати «потрібну» громадську думку західної публіки про події в Україні напередодні вторгнення. Згодом російська інформаційна війна розширилася до глобального масштабу, зміцнюючи свій режим – зазвичай через протиставлення себе західним країнам (Treyger et al., 2022).

Цей новий глобальний масштаб відзначило у 2017-му році розвідувальне співтовариство США, публічно оголосивши про втручання Росії у вибори в США 2016-го року. Такі дії РФ були значним підвищенням рівня ескалації та, фактично, небаченим раніше способом втручання у внутрішні справи США (Office of the Director of National Intelligence [ODNI], 2017). Основна частина впливу на процес виборів відбувалася саме через соціальні мережі. Російська Федерація застосовувала «фабрики ботів», створюючи таргетовані повідомлення для різних цільових груп населення, намагалася розколоти американське суспільство, граючи на темах, що викликають суспільне напруження. Ці таргетовані повідомлення поширювалися навіть в середовищі американських військовослужбовців. Цей вплив, вочевидь, здійснювався російськими агентами військової розвідки та представниками так званого «Агентства інтернет-досліджень», котре оперує цими «фабриками ботів» (Mueller, 2019).

Рівень впливу цих зусиль на результати виборів в Сполучених Штатах лишається малозрозумілим. Але для Росії навіть посередні результати можуть мати вигідний довготривалий ідеологічний ефект. Після подібних атак легітимність демократичних інститутів та основних західних цінностей, серед яких і вільні вибори, піддається сумніву певною частиною суспільства. Через поширення недостовірної інформації може відбуватися вплив на голосування, коли в соціальних мережах шириться переконлива дезінформація про кандидата,

яка поширюється напередодні виборів, і об’єкт цієї атаки має надто мало часу для розвінчання та протидії; витік даних чи закритого листування, до прикладу, може спричиняти політичні конфлікти в середині Європейського Союзу та між ЄС і його союзниками чи партнерами, зокрема з США або НАТО.

Іншим фактором, який сформував бачення російської стратегії взаємодії з соціальними мережами, – це розгортання «Арабської весни» та протестів у Москві в 2011-2012 роках. Важливим є той факт, що ці протестні рухи розглядалися в Росії як потенційне джерело небезпеки та національна загроза. Московські протести стали значним викликом для російського авторитарного режиму через їх мережеву організацію. Російські протестувальники користувалися соціальними мережами як засобом мобілізації нових учасників протесту; схожу практику пізніше можна прослідкувати на прикладі Революції Гідності в Україні та під час протестів у Гонконзі в 2019-році (Elder, 2012). В своїй риториці представники РФ давали зрозуміти, що покладають відповідальність за протести на західних спеціалістів зі спеціальних операцій; вони також звинувачували Захід в «підривній діяльності», проводячи паралелі з «Арабською весною» та «кольоровими революціями».

Породження терміну «Доктрина Герасимова», згаданого раніше, пов’язане не лише безпосередньо із військовими кампаніями, але стосується нових стратегій впливу на стабільність демократичних урядів через соціальні мережі та платформи вже з-середини. В 2013-му російський генерал наголошував на важливості використання «технологій впливу на державні структури та населення за допомогою інформаційних мереж». Він стверджував, що протести у Москві відбуваються за сценарієм «Арабської весни», що, на його думку, демонструє, як «процвітаючі держави» можуть стати жертвами «іноземного втручання» і «опуститися в глибину хаосу, гуманітарної катастрофи та громадянської війни». Саме ця промова породила термін «доктрина Герасимова» і фактично стала предтечею до перетворення соціальних мереж на зброю в руках авторитарних лідерів. Російська Федерація, усвідомивши всі ризики цифрового

середовища для свого власного режиму, перетворила їх на засіб впливу на іноземні уряди (Galeotti, 2018).

Російська Федерація повсякчас відчуває суттєву потребу у використанні асиметричних методів ведення гібридної війни, які дедалі частіше будуть здійснюватися на основі використання штучного інтелекту. Фахівці німецької розвідки наголошують, що Російська Федерація швидко розробляє синтетичний медіа-контент – відредаговані чи скомпільовані фотографії та несправжні відео, які дуже ефективно поширюються через різні відкриті платформи, такі як Facebook, YouTube, Instagram, WhatsApp, TikTok тощо. Найближчим часом кількість такого контенту буде постійно зростати, доповнюючи «фейкові новини» та залучаючи європейських користувачів смартфонів і працюючи на аудиторію країн, де російська пропаганда мала значний вплив. Донедавна прикладом такої країни була Німеччина, де російські медіа вели активну пропагандистську роботу (Treyger et al., 2022).

Широка робота в соціальних мережах та наявність власних інформаційних ресурсів в Європі дозволяє РФ просувати свої інтереси через політичні сили, що симпатизують Москві. Відомі європейські праві лідери, такі як Марін Ле Пен у Франції чи Маттео Сальвіні в Італії, виступали симпатиками Володимира Путіна й активно вимагали від західних країн відмінити введені після 2014-го року економічні санкції, ухвалені у відповідь на анексію Криму Росією та підтримку проросійських рухів на сході України. Сьогодні ми бачимо, що російська стратегія підкупу та маніпуляції через європейських політиків продовжується. Її розгортання спрощуються інформаційними операціями в мережі та кампаніями з дискредитації опонентів проросійських політиків. Навіть в умовах відкритого вторгнення Росії в 2022-му році угорський прем’єр Віктор Орбан зберігає промосковську риторику і систематично піддає критиці європейські санкції, які мають стримувати РФ.

Голова Європейської комісії в 2014–2019 роках Жан-Клод Юнкер вже в 2017-му році відзначав, що ЄС має розвивати цифрову економіку та цифрове суспільство. Разом із цим, він акцентував увагу, що небезпека кіберзагроз,

неправдивої інформації та тероризму ставить новий виклик перед європейським об’єднанням. Юнкер визнавав, що кількість кібератак проти ЄС постійно збільшується. Визначаючи пріоритети на 2018-й рік, йшлося й про те, що європейці мають бути не наївними прихильниками ідеї вільної торгівлі, а натомість мають проактивно захищати свої інтереси. Він запропонував встановити процес перевірки іноземних інвестицій в технологічний сектор, який допоміг би контролювати майбутні інвестиції та забезпечити стратегічну безпеку для країн ЄС (Juncker, 2017).

Після заяви Жан-Клода Юнкера в області європейської інформаційної безпеки та кібернетичної безпеки виникла специфічна ситуація, яку можна охарактеризувати як «сіру зону», адже ЄС на той момент ще не випрацював ефективної стратегії протидії новому типові викликів. Деякі провідні європейські лідери, зокрема президент Франції Еммануель Макрон, підтримували думку, що найоптимальнішим рішенням для відповіді кіберзагрозам є створення глобальної схеми управління, яка б об'єднала уряди та корпорації з метою нагляду за Інтернетом. В рамках Паризького форуму миру, організованого у листопаді 2018-го року з нагоди відзначення столітньої річниці перемир'я, яке поклало край Першій світовій війні, президент Франції запропонував світовим урядам та технологічним компаніям долучилися до створення нового набору загальних принципів, які визначатимуть засади поведінки в цифровому просторі (Macron, 2018). Увесь цей процес відбувався за підтримки понад п'ятдесяти держав та понад двох сотень компаній, серед яких Microsoft, Cisco, Samsung, Google та ін. В основі цієї ідеї лежить зрозуміла мета – розробити загальні норми, для того щоб Інтернет та цифровий простір були безпечними і прозорими. З високою ймовірністю ці домовленості не набудуть статусу глобальних договорів, а існуватимуть на декларативному рівні або на рівні індивідуальних домовленостей між країнами.

Разом із цими заходами, на рівні Європейського Союзу триває робота над оновленням та покращенням законодавства щодо заходів із безпеки користувачів в соціальних мережах та інтернеті. У травні 2018-го року Європейський Союз

увів у дію одні з найжорсткіших світових регуляторів конфіденційності. Ці нові правила, що відомі як Загальний регламент щодо захисту даних (GDPR), значно вплинули на діяльність великих технологічних корпорацій в Європі. Регламент обмежує обсяг особистих даних, що можуть бути зібрані, збережені та використані технологічними компаніями в 28 країнах ЄС. Він також включає в себе принцип, що надає громадянам право вимагати видалення персональних даних про них з мережі. Додатково будь-яка особа віком до 16 років повинна отримати письмову згоду батьків або опікуна перед користуванням цифровими послугами. У випадку виявлення порушень технологічним компаніям загрожують суворі адміністративні штрафи у розмірі 20 млн євро. Витік з Cambridge Analytica, під час якого були викрадені дані 87 млн користувачів Facebook, у багатьох випадках служить яскравим прикладом, який виправдовує впровадження жорстких правил конфіденційності. Схожий витік інформації відбувся в 2018-му році в Ірландії, коли було викрадено дані близько 30 мільйонів користувачів Facebook.

В 2022-му році Європейська комісія опублікувала спільне повідомлення для Європарламенту та держав ЄС – нову «Політику ЄС в сфері кіберзахисту». Комісія закликала держави-члени розробити спільні політики кіберзахисту, котрі підкріплювали би завдання, поставлені в «Стратегічному компасі». Про складність цього завдання свідчить кількість спеціалістів, яку планує залучити керівництво ЄС. В документі визначається, що «Європа зіткнулася з реальним і тривожним браком кіберспеціалістів». За оцінками Європейської організації з кібербезпеки (ECSO), наведеними в оновленій політиці, вже у 2022 році ЄС потребував 500 000 спеціалістів. Відсутність такої великої кількості спеціалістів перешкоджає спроможності ЄС розробляти нові технології та захищати критичну інфраструктуру (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2022).

У 2023 році Комісія планувала запустити ініціативу щодо «Академії кібернавичок». Фактично, вона буде основною інституцією, яка дозволить нарощувати кількості професіоналів, підготовлених у сфері кібербезпеки.

Передбачається, що ця Академія дозволить об'єднати розрізнені ініціативи із підготовки фахових спеціалістів, забезпечить координацію, інтеграцію в систему безпеки ЄС. Академія також зможе принести користь для державних структур, таких як міністерства оборони та військові відомства, які стикаються з браком кваліфікованих кадрів через жорстку конкуренцію за цих спеціалістів з приватним ринком (European Commission & High Representative, 2022),

Європа, хоча й прагне утвердити своє лідерство в сфері регулювання Інтернету та обмеження поведінки цифрових корпорацій-гігантів, все ж потребує великих зусиль для забезпечення майбутньої економічної міцності. Істинним проривом у досягненні інноваційного лідерства буде не лише підготовка значної кількості спеціалістів з кібербезпеки, а й створення власних національних технологічних гігантів, що здатні витримувати конкуренцію з китайськими та американськими суперкорпораціями. Китай, завдяки своїм стратегіям, вже зміг опонувати Google та Apple, масштабувавши на світовий ринок виробників високого рівня, таких як Huawei і Xiaomi, і вплинувши на Facebook, змушуючи його враховувати місцеві реалії через популярність WeChat, китайської альтернативи соціальним мережам. Поки Європа не зможе виростити власних глобальних технологічних гігантів, як це вже сталося у секторах автомобілебудування та біотехнологій, Старий Світ залишатиметься на других позиціях в контексті сфери соціальних мереж, штучного інтелекту та цифрових рішень.

Підсумовуючи, соціальні мережі – породження епохи інформаційного суспільства, дедалі глибше проникають в сфери суспільного життя. Їхня роль та функціонал постійно змінюється та зростає. Засновані як спосіб комунікації з друзями та знайомими, соціальні мережі та цифрові платформи починають впливати на політичне життя, створюють конкуренцію традиційним засобам масової інформації, а в останні роки – стають формою зброї, яку держави застосовують в гібридних атаках на своїх супротивників. За останнє десятиліття повсюдний розвиток Інтернету, особливо в сфері соціальних мереж, став джерелом численних випадків, коли громадяни різних країн світу

використовують онлайн-платформи, щоб спосіб висловлення своєї незгоди політичним режимам. Яскравими прикладами є «Революція Гідності» в Україні, «Арабська весна» на Близькому Сході та в Північній Африці та протести в Гонконзі в 2019-му році. Інтернет та соціальні мережі стали ефективним інструментом мобілізації ресурсів під час протестних кампаній. Крім того, соціальні мережі беруть на себе роль інформаційних каналів для зовнішньої аудиторії, слугуючи платформами для створення агітаційних матеріалів і повідомлень, що дозволяє учасникам протесту сформулювати обґрунтування свого невдоволення. Політичний радикалізм та мобілізація громадян прямо впливає на розвиток громадських інститутів. Стабільність демократичного транзиту безпосередньо залежить від здатності громадянського суспільства протистояти радикалізації та адаптуватися до нових соціополітичних реалій, у тому числі, викликаних революційними подіями (Новакова, 2024)

Сучасна Європа існує в умовах мінливого середовища та зазнає комплексу серйозних викликів. Виклики, пов’язані із військовими загрозами, міграційними процесами тощо, лишаються традиційними для Європейського Союзу. Проте можна вважати, що найглибше та найновітніше джерело потрясінь в Європі на даний момент – це триваючі революції в галузі інформаційних технологій, соціальних мереж та штучного інтелекту. Впровадження новітніх технологій може негативно позначитися на перспективах розвитку Європи, яка стоїть на позиціях наймогутнішого та економічно розвиненого об'єднання у світі та прагне бути глобальним гравцем.

Ці документи закладають трансформаційну рамку для ЄС, котрий раніше не мав єдиних політик, правил та положень, які би підштовхували європейську систему безпеки до скорочення розриву із іншими передовими технологічними державами. Серед цих документів одним із найголовніших є «Стратегічний компас», котрий описує, як інформаційні маніпуляції в соціальних мережах загрожують не лише державам-учасницям ЄС, а й її союзницям; ця стратегія розглядає цифровий простір як одну із головних загроз для Союзу поряд із загрозою військових конфліктів. Вперше в історії ЄС в цьому документі

закладаються основи для уніфікації засобів та підходів щодо реагування на нові загрози.

Європейський Союз, розробляючи нову правову базу, прагне зміцнити своє лідерство в регіоні та стати впливовим «постачальником» безпеки для своїх громадян. Незважаючи на свій вплив як видатної світової торговельної сили, Європейський Союз відстає у сферах, таких як безпека соціальних мереж, електронна комерція та хмарні технології. Серед цифрових чи інтернет-компаній найбільшими є американські чи китайські; серед перших 200 лише вісім є європейськими. Майбутнє Європейського Союзу значною мірою залежатиме від того, як Європа впорається з цими викликами, можливо, визначаючи його курс до економічного та політичного небуття.

Ці загрози виникають як з боку конкурентів, так і з боку партнерів. Агресивно налаштована Російська Федерація, використовує складні кампанії дезінформації, спрямовані на зміну політичного ландшафту Європи на користь російських інтересів. Китай намагається використовувати багатства, знання та технічну досконалість Європи в своїх інтересах. Його стратегія «Один пояс, один шлях» має на меті здобуття ключових інфраструктурних активів та підтримку стратегії, яка привертає найбільш талановитих інженерів Європи до роботи на китайський уряд. Водночас Європа переживає виклики, пов’язані з тим, що її економічне процвітання та демократичні цінності опиняються під загрозою через вплив американських технологічних гігантів і соціальних мереж. Ці корпорації отримують значні прибутки, але ставлять під питання збереження конфіденційності даних в Європі.

Нове покоління кібернетичної та іншої зброї, посилене зростанням штучного інтелекту, значно полегшить можливості недемократичних країн брати участь в асиметричних конфліктах проти Європейського Союзу та його союзників. Країни на кшталт КНР чи Російської Федерації можуть продовжувати атакувати демократичні країни, вважаючи кібератаки, широкі кампанії з дезінформації в соціальних мережах та інші форми гібридної війни оптимальним засобом конкуренції з арсеналом Європейського Союзу та країн НАТО у конвенційної

зброї. Питання про те, чи можна вважати кібератаки класичною формою війни, з яким ще в 2007-му році стикнулася Естонія, є складним і викликає необхідність опрацювання міжнародним правом, що обґрунтовує відповідь або захист союзників, як це передбачено статтею 5 НАТО.

Висновки до розділу 1

Проведений ретроспективний аналіз еволюції соціальних мереж та цифрового середовища дозволяє стверджувати, що за останні десятиліття природа цифрової комунікації зазнала фундаментальної трансформації: від інструменту демократизації та вільного обміну знаннями до одного з ключових театрів глобального геополітичного протистояння. Ідеї класиків інформаційного суспільства, зокрема Д. Белла та М. Кастельса та ін., які вбачали у мережевих структурах простір горизонтальної свободи, сьогодні потребують суттєвої актуалізації. Сучасне цифрове середовище стало інструментом реалізації асиметричних стратегій, де соціальні мережі використовуються авторитарними режимами для розмивання суспільної суб’єктності та делегітимізації демократичних інститутів Європейського Союзу.

Практичне впровадження «доктрини Герасимова», діяльність «фабрик тролів» та системне продукування теорій змов свідчать про те, що цифрові технології дозволяють агресору вести війну у «сірій зоні», де межа між миром і відкритою війною стає дедалі тоншою. Такий стан нових гібридних загроз, у поєднанні з більш «традиційними» викликами міграцій, економічної нерівності та війни поруч з європейськими кордонами, підштовхнув Європейський Союз до поступового перегляду своєї безпекову парадигми — відійти від ідеалістичної наївності 1990-х років у бік стратегічного реалізму, що знайшло своє відображення у положеннях «Стратегічного компасу» 2022 року.

Водночас однією з найгостріших загроз для суб’єктності ЄС залишається проблема «інфраструктурної заплутаності» та критичної залежності від технологічних рішень США та Китаю. Приклад впровадження мереж 5G та

спроба експансії компанії Huawei демонструють, що відсутність власних технологічних гігантів перетворює європейський цифровий простір на об’єкт стороннього впливу, де бізнес-інтереси часто вступають у суперечність із вимогами національної безпеки.

У цьому контексті «цифровий суверенітет» стає не просто гаслом, а необхідною умовою виживання європейської політичної моделі. Нарешті, досвід окремих країн-членів, як-от Естонії у сфері кібероборони чи Швеції у розбудові системи «психологічного захисту», доводить, що ефективна протидія гібридним викликам неможлива без комплексного залучення всього суспільства. Відновлення концепцій «тотальної оборони» та фокус на підвищені спроможності громадян у сфері цифрової гігієни є одним із ключових факторів, який дозволяє демократичним системам зберігати стійкість перед обличчям агресивних інформаційних операцій. Подальший розвиток Європейського Союзу як глобального «постачальника безпеки» прямо залежатиме від спроможності Брюсселя поєднати жорстке регулювання технологічного сектору із розбудовою власних інноваційних спроможностей.

РОЗДІЛ 2. СОЦІАЛЬНІ МЕРЕЖІ ТА ЦИФРОВІ МЕДІА ЯК ГЛОБАЛЬНА ЗАГРОЗА ТА ВИКЛИК У СУЧАСНИХ ЄВРОПЕЙСЬКИХ ПОЛІТИЧНИХ СИСТЕМАХ

У другому розділі дослідження здійснюється деконструкція впливу соціальних мереж на архітектуру сучасних європейських демократій та етичний фундамент суспільства. Політична сфера представлена крізь призму теорії «хвиль демократизації» С. Гантінгтона, доводячи, що нині ми спостерігаємо масштабний «відкат», де цифрові платформи перетворилися з інструментів свободи на засоби зміцнення «фасадних демократій» та авторитарних режимів. На прикладі «керованої демократії» В. Суркова та іліберальної моделі В. Орбана розкрито, як автократи імітують демократичні процедури, використовуючи соціальні мережі для маніпуляції виборчим процесом та придушення несистемної опозиції. Особлива увага приділена моральному виміру технологічного прогресу. У розділі протиставлено невідповідність європейських демократичних принципів та сучасного явища «техноавторитаризму», де алгоритми емоційного зараження замінюють раціональну дискусію. У розділі детально аналізується, як соціальні мережі створюють феномен «самотності у натовпі» та підривають автономію особистості, трансформуючи громадянина-суб’єкта на пасивного споживача алгоритмічно відфільтрованого контенту.

2.1 Соціальні мережі у політичній сфері: виклики для сучасних європейських демократичних принципів.

Процес становлення європейських демократій та демократичних принципів налічує не одне століття. Народжена в античній Греції ідея про «владу народу» значно видозмінилася від давнини: стала інклюзивною,

загальнодоступною, адже сучасна демократія, на відміну від грецької, передбачає, що всі громадяни-суб'єкти мають можливість впливати на політичне життя. Становлення сучасних демократичних підходів відбувалося разом з розвитком суспільства та політичної думки.

Найбільших здобутків на європейському континенті демократія досягла, за визначенням Самуеля Гантінгтона, внаслідок «трьох хвиль демократизації». Гантінгтон виділяв три етапи впровадження демократичних принципів у різних країнах. Перший – період з 1820-х до 1920-х: в цей час громадяни здобули широкі виборчі права, активно формувалися інституції, необхідні для представницької демократії – парламенти та партійна система. Другий період – післявоєнний час, 1940-ві–1960-ті роки; головним рушієм до поширення демократії стало остаточне руйнування колоніальних систем та присутність військ союзників у ряді держав. Демократичні інституції впроваджувались в Німеччині, Італії, Японії тощо. Третя хвиля демократизації – 1970-ті – значна кількість країн Латинської Америки, Азії та Європи стають демократичними. Процеси, що відбувалися перед розпадом СРСР в частині країн Варшавського блоку, які отримали назву «осінь народів», також відносяться до цієї хвилі (Huntington, 1993)

Концепція Самуеля Гантінгтона, вочевидь, може містити неточності, враховуючи значні часові проміжки, які вона охоплює. Разом із тим, вона є надважливою, бо виводить процеси демократизації на глобальний рівень та зв'язує єдиною логікою ті перетворення, котрі відбуваються синхронізовано у різних частинах світу.

Теорію Гантінгтона також доповнювали та уточнювали Ф. Шміттер та Д. Маркофф. Шміттер запропонував точнішу хронологію та прив'язав початок цих хвиль до «Весни народів» 1848-го року. В свою чергу, Д. Маркофф розширив рамку теорії «хвиль», включивши в неї ідеологічну частину, яку супроводжує процес демократизації. Вочевидь, цей підхід є одним із багатьох можливих на шляху до пояснення логіки, за якою відбувався демократичний перехід (Гаврилюк, 2001)

Важливою частиною цієї теорії є її інша сторона, адже хвилі демократизації передбачають зворотній «відкат». Це свого роду маятник, який спрацьовує також в інший бік – згортаючи частину демократичних здобутків та виводячи на передній край політичного процесу авторитарні, недемократичні режими. Яскравий приклад — 20–30-ті міжвоєнні роки. Європейський континент у цей час переважно схилявся до авторитарних, фашистських або націоналістичних підходів, а географія цих режимів поширювалася від Португалії до Другої польської республіки. Цей факт є додатковим нагадуванням, що демократичні принципи не встановлюються навічно, а завоювання демократії можуть згортатися під впливом популістських чи авторитарних лідерів. Для сучасної європейської політики зростання популярності популістських партій та політиків є однією із форм цього «відкату», котрий, за логікою Гантінгтона, наслідує третю хвилю демократизації.

Одним із наслідків глобальної демократизації можна вважати саме створення Європейського Союзу Візія про проєкт європейського об’єднання є давньою, вона виринала у публічних дискусіях та в ідеях інтелектуалів країн Європи протягом довгого часу (Мартинов, 2015). Катаклізми, війни та економічні негаразди завжди підживлювали спроби знайти рішення їх можливому запобіганню у майбутньому. Європейський Союз став кульмінацією третьої хвилі демократизації та уособленням європейських принципів демократичності. Його існування міцно пов’язано із сталістю демократичного облаштування простору в середині кожної окремої країни-члена ЄС.

Саме питання захисту демократії в середині європейського об'єднання теж не є новим. Європейська унія бере свій початок ще з часів Холодної війни. Союз вугілля та сталі, піддавався системному впливу із соціалістичного табору. Радянський Союз був зацікавлений у формуванні власної мережі агентів, які би просували радянські інтереси в західних демократіях. Ряди новостворюваних європейських інституцій поповнювалися представниками, у тому числі, соціалістичних чи інших лівих партій, що мали симпатії або отримували допомогу напряму від Радянського Союзу (Безверха та ін., 2020). Радянська

держава мала і прихильників із середовища європейської інтелігенції; частина західних інтелектуалів симпатизувала СРСР та марксизму до моменту придушення радянською військовою машиною Празької весни. Певне розвінчання радянського міфу відбулося лише в момент, коли комуністична система продемонструвала європейським симпатикам свою істину природу як антидемократичної системи, яка придушує будь-які спроби до лібералізації та поширення альтернативних ідей (Кузь та ін., 2020).

Дезінформація та пропаганда до винайдення соціальних мереж поширювалася через телебачення, журнали та пресу – ці медіуми були елементом інформаційної війни проти Європи, що проходила свій шлях до об'єднання. Держави-супротивники демократичного табору у Холодній війні користувалися усім арсеналом засобів, спрямованим на підрив європейської демократичної системи: від прямої присутності агентів спецслужб до підкупу чиновників. Головною метою було поширення власного впливу на політичні процеси у Європі. Противники європейської демократії прагнули знайти слабкі місця в цих системах та порушити здатність європейських держав захищати себе, свої політичні системи та своїх громадян.

З розпадом СРСР ці атаки були тимчасово припинені. Разом із цим, проголошений Френсісом Фукуямою «кінець історії» передбачав, що світ дедалі більше буде схилятися до західної ліберально-демократичної моделі та продовжить уніфікуватися та глобалізуватися (Перепелиця, 2019). Аналізуючи сучасний стан міжнародної політики, можна твердити, що демократичні принципи не стали основною цінністю та універсальною максимою, яка може об'єднати більшу частину світу.

Інший парадокс, котрий піддається емпіричному спостереженню, – це той факт, що після розпаду комуністичної системи в міжнародній політиці були оформлені такі умови, в яких відданість, реальна чи формальна, демократичним принципам була ключем та необхідною умовою для участі в міжнародній співпраці (Smeltzer, 2012). Така невідповідність породила не один авторитарний

режим, що своєю суттю нагадував типову та унормовану демократичну європейську країну.

Гібридна війна Російської Федерації в 2014-му проти України та повернення широкомасштабної війни на Європейський континент в 2022-му році знову гостро поставило питання існування демократичних систем та їх адаптивності. Проте нині суттєво змінилася природа режимів, що протистоять ринковим демократіям – тепер це авторитарні режими, що озброєні усіма засобами та інструментами, які має у своєму арсеналі демократія. Ці авторитарні режими тепер не мають планової економіки, а користуються елементами вільного ринку, ба більше, ці авторитарні режими озброєні демократичною риторикою і вдало застосовують принцип «фасадної демократії». Ці режими зовні можуть виглядати як відкриті системи, але їх сутність визначає надзвичайний рівень контрольованості усіх процесів в державі та відсутність активного громадянського суспільства (Романюк, 2010). Користуючись цим, авторитарні режими здійснюють різнорівневі атаки на європейські демократичні принципи, зберігаючи надзвичайно високий рівень контролю у власній внутрішній політиці.

Концептуалізована ідеологом Кремля В. Сурковим концепція «контрольованої різноманітності» описує систему, в які збережені вибори, наявні кандидати, виборці можуть здійснювати голосування тощо. Натомість результат цих виборів завжди носить передбачуваний характер (Foy, 2021). У такий спосіб автократи забезпечують своїм режимам певну долю легітимності, апелюючи до «голосу народу». Такі штучні виборчі кампанії чи фіктивні референдуми – в Криму у 2014-му році або на території частково окупованих півдня та сходу України в 2022-му – завжди передбачувано завершуються надзвичайно високим рівнем підтримки. Разом із тим, головною цінністю «керованої демократії» проголошується стабільність держави. Для досягнення якої впроваджується контроль над засобами масової інформації, платформами соціальних мереж та месенджерами. Оминаючи факт тотального контролю Москви над традиційними засобами масової інформації, варто підкреслити, що російський режим вже встановив контроль над рядом соціальних мереж (VK), обмежим доступ до

відеохостингів (YouTube) та активно розробляє власний державний месенджер на противагу слабко контрольованому WhatsApp та Telegram (Marrow, 2025). Домінування держави в інформаційному просторі, згідно концепції Суркова, передбачає, що доступ до медіа мають лише ті політики, які співпрацюють із режимом. Всі ці дії спрямовані на встановлення специфічної форми контролю над громадянами та повзучого відсікання «шкідливих інформаційних впливів», яка маскується під гаслами набуття «цифрового суверенітету».

Авторитарний режим таким чином створює копію демократичних інституцій, кожний елемент яких перебуває під щільним наглядом держави – створюється ілюзія присутності справжньої демократії. Ця концепція передбачає розділення опозиції на системну та несистемну. Системна опозиція існує в межах тих правил та законів, які встановлює режим, та не має співпрацювати із іноземними структурами та урядами (Foy, 2021). Несистемна опозиція підлягає, в свою чергу, руйнуванню та репресується силовими органами. Ця ілюзія демократії, до того ж, поєднується із ринковою економікою: громадяни мають доступ до технологій, можуть користуватися банківськими послугами, подорожувати, вести підприємницьку діяльність тощо. В такий спосіб оформлюється система, яка маніпулює демократичними принципами у своїх інтересах та працює на знищення істинної демократії, відтворюючи штучний демократичний «фасад». Найбільша небезпека такого підходу в тому, що він будується та упроваджується на найвищому смисловому рівні – на рівні самого поняття, чим є демократія насправді, якими є її ознаки та основоположні принципи. Загрози інспіровані такими «керованими» режимами, вочевидь, становлять значний рівень загрози для Європейського Союзу, здійснюючи атаки з-за меж європейського об’єднання. Разом із тим, відтестована Росією модель вдаваної демократії має інший вимір небезпеки – вона вдало застосовується подібними режимами навіть в середині самого Союзу.

Сучасні авторитарні режими здатні імітувати та користуватися демократичною риторикою, уводячи в оману прихильників демократичних підходів облаштування суспільства. Яскравий приклад – прем’єрство Віктора

Орбана в Угорщині, яка раніше, за рейтингом Freedom House, відносилася до країни з консолідованою демократією, а нині перебуває у категорії гібридних режимів. Угорський прем'єр у своїй риториці не відмовляється від демократії, але намагається переконати власне суспільство, що сучасна європейська демократія перебуває в стані занепаду. Скочування Угорщини до авторитаризму відбувалося не водночас: Віктор Орбан від початку своєї каденції маніпулював демократичною системою та її слабкостями – поступовими, непомітними кроками руйнуючи систему стримувань та противаг, які є основою будь-якої сталої демократії.

Переломним моментом в угорській історії можна вважати 2010 рік, коли партія Орбана повернулася до влади на хвилі безпрецедентної підтримки з боку виборців. Використовуючи популістські гасла, партія «Фідес» почала відкат тих структурних та демократичних реформ, котрі досить успішно були розгорнуті після падіння радянського режиму. Такий спосіб облаштування політичного життя разюче відрізняється від тих засад, на яких будується відкрите суспільство та сучасна європейська демократія (Бокрош, 2015).

Freedom House визначає критерії, за якими можна виокремити електоральні демократії: вони мають багатопартійну систему, що керується принципом змагальності, виборче право є загальнодоступним, вибори проводяться регулярно та відбуваються за принципом конкуренції, а політичні сили, в свою чергу, мають доступ до ЗМІ і можуть проводити активну політичну агітацію (Гаврилюк, 2010). Відповідно до цих підходів, можна стверджувати, що «керовані демократії» суттєво випадають із подібної логіки. Натомість, вони створюють ілюзію демократичного процесу, маніпулюючи суспільною думкою та вдаючись до системного порушення основних демократичних принципів.

Цей спосіб управління окреслює найголовнішу загрозу європейським демократіям – пропонує удавану стабільність, котра підміняє собою реальний інструментарій впливу громадян на політичний процес у власній країні. Ці гібридні підходи поширюються на усе суспільство, проникають у цифровий простір та стають продовженням політики автократів, які здійснюють свій вплив

через ті медіуми, котрі в останні десятиліття були основою демократичного процесу. У працях Н. Ю. Гусєвої розглядається фундаментальний вплив цифрових технологій на розвиток сучасного суспільства, з особливим акцентом на трансформацію політичних і соціокультурних процесів. Дослідниця ґрунтовно аналізує природу політичної комунікації в цифрову епоху, виокремлюючи суттєві ризики для стабільності демократичних інститутів. Дослідниця показу, що відбувається зміна парадигми взаємодії між владою та суспільством, де цифрові платформи стають не лише інструментами діалогу, а й середовищем для нових форм політичного маніпулювання. Гусєва акцентує увагу на викликах, що постають перед сучасною культурою у зв'язку з тотальною цифровізацією, та обґрунтовує необхідність формування нової цифрової етики як механізму захисту людських цінностей. традиційних філософських підходів до розуміння культури, історії та релігії (Гусєва, 2024).

Соціальні мережі, народжені в умовах третьої хвилі демократизації, пройшли складний шлях від інструменту, що підсилює демократичні ініціативи та сподівання, до інструменту, котрий цю демократію руйнує. Більшість демократичних рухів та революцій останніх десятиліть доводили гіпотезу, що соціальні мережі є інструментом прямої демократії та інструментом, який дозволяв відстоювати демократичні принципи та був одним із засобів дієвого протистояння авторитарним режимам. Помітні рухи, спрямовані на демократизацію, що розгорталися нещодавно, мали сильний елемент мережевого єднання громадян. Активність у соціальних мережах та консолідація були важливим елементом громадянської активності під час протестів у Ірані в 2022-му році, під час опозиційного руху в Білорусі 2020–2021-го років, революції у Гонконгу у 2019-му та під час Революції Гідності 2013–2014-го. Ці мережеві революції розгорталися у несприятливих обставинах, коли доступ до інформаційної сфери був суттєво обмеженим та перебував у повному або частковому контролі з боку держави. Соціальні мережі в цій ситуації були тим засобом, який дозволяв обходити цензурування; вони створювали простір для поширення опозиційних думок та були прозорим джерелом інформації, що

дозволяло інформувати активну частину суспільства в альтернативний спосіб (Mei, 2021).

Соціальні мережі та платформи відігравали значну роль у захисті демократичних принципів під час кожної із цих масових акцій непокори, а громадяни винаходили безліч нових способів продовжувати свою політичну активність, гуртували громадянське суспільство не лише на площах, але й у мережі. Під час протестів у Гонконгу рівень горизонтальної самоорганізації досяг надзвичайного рівня, адже мережева структура протесту дозволила продемократичним силам діяти злагоджено та мобілізувати нових прихильників без очевидних публічних лідерів. Попри це, протест не мав стихійного характеру, не переростав у хаос, а натомість керувався через типові демократичні інструменти – голосування, обговорення; учасники протесту розділялися на малі кластери та вирішували нагальні задачі через форуми та месенджери. Значна частина дій протестувальників була направлена на те, щоб демонструвати правду в цілому світі, користуючись можливостями соціальних мереж (Banjo, et al., 2019).

Приклад цих протестів є показовим, адже соціальні мережі, вочевидь, стали неодмінним атрибутом сучасних революцій та процесів, котрі виникають у наслідок браку демократії та свобод. Вже у 2011-му році, під час «Арабської весни», соціальні мережі допомагали залучати нових прихильників та стали фактором, який дозволив об’єднати розрізнені групи невдоволених диктаторами громадян. Дослідники з Університету Вашингтона наводять цифри кількості твітів за тиждень до відставки Хосні Мубарака – їхня кількість на день зросла із 2300 до 230 000. Контент, записаний під час протестів, ставав вірусним, отримуючи мільйони переглядів. Активність в соціальних мережах до початку протестів теж мала важливий вплив – створювався майданчик для публічної дискусії, це дозволяло формувати громадську думку і легітимізувало запит суспільства на зміни (O'Donnell, 2011). Значний мобілізаційний потенціал закладений в архітектурі соціальних мереж, дозволяв протягом тривалого часу

відстоювати демократичні принципі в різних куточках світу, стверджуючи основоположне право громадян на протест.

Проте з часом змінювалося і сприйняття соціальних мереж європейськими суспільствами: під час «Арабської весни» чи «Революції парасольок» або Революції Гідності соціальні мережі виглядали в очах суспільства як інструмент звільнення, що дозволяє протидіяти автократіям, як інструмент, який надає можливість голосу незгодним та опозиції, — до засобу контролю та зброї, яку використовують іноземні уряди або реакційні політики у своїх цілях, що в свою чергу знижує довіру європейських громадян до будь-яких демократичних процесів та процедур.

Суспільного розголосу дедалі частіше набувають випадки маніпуляції громадською думкою із застосуванням соціальних мереж. Найгостріше ця проблематика, пов'язана із електоральним процесом, вперше постала не в Європі, проте в подальшому відобразилася на внутрішньо-європейській політиці. Соціальні мережі булі одним із інструментів маніпуляції публічною думкою під час президентських перегонів у Сполучених Штатах 2016-го року, які відзначилися російським втручанням у процес виборів президента, а пізніше позначились під час референдуму про вихід Великої Британії з Європейського Союзу. Соціальні мережі від цього часу стали одним із засобів втручання у виборчі процедури та у процес будь-якого волевиявлення громадян. Вільні вибори та свобода волевиявлення є одним із ключових принципів європейської демократії. Перелік дій, які можуть бути використані із метою впливу на результати виборів чи інших голосувань, є надзвичайно великим: кібератаки, блокування незалежних ресурсів та новинних сайтів, урядові ініціативи, що обмежують цифрову взаємодію та консолідацію, поширення неправдивої інформації, тощо (Polyakova, 2019). Проте всі вони завдають значної шкоди легітимності обраної влади та викривлюють сприйняття демократичної системи в очах виборців.

Поступова інтеграція будь-якої країни до євроатлантичної спільноти, вочевидь, передбачає тісну інтеграцію в цифровій сфері, яка оформлена за

певними правилами та законами. Європейські демократичні принципи передбачають, що громадяни мають отримувати доступ до цифрових засобів та інформації безперешкодно. Цей підхід також зумовлює те, що якомога ширший прошарок суспільства має бути залучений до політичного процесу через мережу та новітні інформаційні технології. Сьогодні можна говорити про те, що така відкритість має ряд переваг та недоліків, це доводить і наявний європейський досвід.

З впевненістю можна говорити, що загальнодоступні цифрові комунікації позитивно впливають на різних рівнях, від політики до економіки: прозорість держави зростає, збільшується довіра інвесторів, знижуються корупційні ризики. Це підвищує мобільність товарів та послуг, що позитивно впливає на ринкові відносини та загальний добробут громадян. Разом із тим, мережа є доволі агресивним середовищем, в середині якого відбувається постійна конкуренція між державами, політичними акторами тощо. Плюралізм думок, разом із відкритістю до дискусії – це важливий фундамент демократичного способу облаштування суспільства. Наявність дискусії може загартовувати та консолідувати громадянське суспільство, ефективніше здійснювати контроль за державними органами та інституціями. Важливим є і той фактор, що влада також відчуває тиск, який здійснюють мережеві активісти, та відповідно корегує свої рішення чи законодавство під суспільний запит. Для громадян соціальні мережі також є інструментом, який є помічним під час електоральних циклів та процесів: в демократичних системах політична комунікація в мережі є одним із факторів, котрий впливає на рішення виборців. Невдала комунікація в мережі легко може призводити до втрати частини електорату чи може сформувати опозиційну громадську думку.

Виклики, котрі соціальні мережі створюють для європейських демократичних принципів, лежать у площині глобального протистояння авторитарних та демократичних систем, описаного вище. Протистояння цих двох систем породжує сутичку наративів, поширення яких відбувається за різними моделями: у випадку демократій – маємо принцип відкритості та прозорості, у

випадку авторитарних систем – це принцип маніпуляції інформацією та застосування пропаганди. Швидкість поширення інформації в соціальних мережах та месенджерах створює обставини, в яких повідомлення чи наративи швидко проникають в інформаційний простір протиборчих суспільств. В такій ситуації уряди та політики, що оперують дезінформацією, мають тактичну перевагу над демократичними підходами до роботи з інформацією – вони мають можливість продукувати та поширювати інформаційні повідомлення в безперервному режимі, тоді як сторона, що піддається впливу, змушена діяти реакційно та розвінчувати дезінформацію та пропаганду. Ці відповіді є ресурсомісткими та потребують спеціальних центрів та спеціалістів, що здатні ефективно деконструювати неправдиві повідомлення. Цей гібридний спосіб атак на інформаційний простір демократій може відбуватися навіть за відсутності прямого чи відкритого військового протистояння. Відтак, відсутність війни – не є запорукою того, що суспільство чи країна не стикатимуться із агресивними діями в мережі у відносно мирний час (Гончар, 2024).

Ця боротьба «за розуми» є важливою, адже соціальні мережі мають значну частку проникнення у повсякденне життя громадян. Вони стають полем щоденної конкуренції між відкритими та закритими системами, кожна з яких має на меті залучити нових носіїв. В цих умовах у наукових та публіцистичних роботах можна зустріти дедалі більшу кількість явищ, які описують це інформаційне протиборство: «дезінформація», «неправдива інформація», «інформаційна війна», «фейкова інформація» тощо. Всі ці форми гібридної інформаційної агресії передбачають зловмисне втручання у внутрішню політику сторонньої держави; зручними приводами для цього стають ситуації суттєвого суспільного напруження.

До прикладу, пандемія коронавірусної хвороби COVID-19 нерідко використовувалася як спосіб збурення в демократичних суспільствах. Через те, що ця пандемія отримала детальне висвітлення в соціальних мережах від самого її початку, дезінформація, перекручена чи неправдива інформація ставали зброєю, що була покликана підривати довіру громадян до власних урядів.

Породжена глобальною пандемією інформаційна криза отримала назву «інфодемії» та характеризувалася безперервним потоком неперевіреної, часто неправдивої інформації (Simon & Camargo, 2023). Ситуація із розгортанням пандемії в двох вимірах (онлайн та офлайн) спричинила не лише інформаційну хвилю й поширення недовіри до національних урядів, але й доволі жорстку реакцію у відповідь.

Пандемія призвела до поглиблення кризи демократії в усьому світі. Звіт Freedom House від 2020-го року свідчить про те, що у 80-ти країнах світу становище демократії та прав людини погіршилося, а найбільше постраждали від цього країни, що лише стоять на демократичному шляху. Авторитарні системи, на зразок Китаю, намагалися заглушити невдоволення та соціальне напруження через посилення пропагандистських методів, розширювали спостереження за власними громадянами, використовуючи значний рівень цифровізації в країні, та жорстко придушували будь-які виступи супроти владної політики. Приховування інформації також стало одним із методів контролю над суспільною думкою (Repucci, 2020)

Інформаційний простір в демократичних країнах передбачає свободу від втручання влади у ЗМІ та соціальні медіа. Попри це, навіть європейські уряди нерідко використовували хворобу як спосіб розширення своїх повноважень та корегували власне законодавство, водночас зменшуючи рівень свобод, декларуючи ці дії як засіб боротьби із захворюванням. Також у звіті Freedom House проаналізований вплив пандемії на електоральні процеси та інші демократичні свободи. 158 країн уводили обмеження на протестну активність, але ці протести все одно мали силу навіть у країнах із високим рівнем демократії. За описаний у звіті період вибори мали відбуватися у 24-х країнах; сім країн переносили дату виборів, у чотирьох випадках відбулися зміни у законодавстві, що поставило під сумнів результати двох виборів. Таким чином, частина урядів намагалася відкласти вибори на невизначений час, а деякі уряди вдалися до нарощування репресій проти опозиційних сил. Яскраво це проявилося у згаданому раніше Гонконгу, де вибори були перенесені на 12 місяців, а згодом

була видана заборона брати участь в електоральному процесі для дванадцяти кандидатів від демократичних сил.

Пандемія показала, що політика компаній, що адмініструють соціальні мережі, в таких ситуаціях не є досконалою. Неефективна протидія платформ дозволила агентам інформаційного впливу тестувати різні підходи до поширення власних повідомлень; в свою чергу, це викликало хвилю збільшення заборон та обмежень, які накладаються на учасників онлайн-спільнот (Repucci, 2020).

Демократичним суспільствам найближчим часом доведеться суттєво інвестувати в розвиток стійкості до цифрової дезінформації, навіть якщо вони вживатимуть заходів для встановлення норм, які зменшують вразливість до використання дезінформації. Побудова соціальної стійкості в умовах зростаючого натиску авторитарних систем є одним із найважливіших безпекових викликів, перед яким постали європейські держави та Європейський Союз. Європейська унія зараз об'єднує 27 країн та майже півмільярда населення; окрім того, Союз має відчутний потенціал до розширення через країни-кандидати, серед яких є і Україна. Європейський Союз є провідним гравцем на європейському континенті, який задає політики та правила, котрі стають прикладом для інших країн. В цій ситуації державам, об'єднаним Маастрихтським договором, необхідно рішуче діяти у полі протидії дезінформації та кіберзагрозам.

Саме на законодавчі та демократичні принципи та ініціативи, які втілює ЄС, орієнтується значна частина світу – відтак стійкість у протидії «керованим демократіям» та авторитарним режимам має бути фокусом оновлених європейських безпекових політик. В середині Європи вже відчутна тенденція до перегляду ролі Союзу – в бік глобального постачальника та гарантера безпеки на континенті. Ця роль вже була концептуально закладена ще на етапі оформлення унії, адже безпека проголошена одним із ключових європейських принципів, про що свідчить друга стаття «Угоди про Європейський Союз» – в ній безпека визначена як базова цінність (Consolidated version of the Treaty on European Union, 1997). Європа нині все ще на шляху до пошуку рішень, які можуть ефективно

захищати демократію та виборчий процес в цифровому середовищі. Початково кампанії з дезінформації та кібератаки в мережі розглядалася як одиничні випадки, не пов'язані системністю. Згодом, після чергової активізації агресивної політики Російської Федерації та нових гібридних методів нападу на демократичні суспільства та принципи, проблему почали описувати, але дієвих механізмів протидії випрацювано не було, за деякими винятками деяких країн описаних у попередньому розділі.

Згодом активність російських служб, що проводять інформаційну війну, проявилася під час референдуму в Нідерландах та в ряді інших європейських держав; ці випадки поступово змінили уявлення європейців про характер проблеми та призвели до дискусій про необхідність випрацювання моделей, що дозволять ефективніше захищати демократію. Значний час авторитарним режимам вдавалося діяти в умовах, коли демократії надавали перевагу стриманій реакції. Європейський погляд на проблему кампаній з дезінформації продовжував різнитися від країни до країни. Частина з них продовжувала перебувати в пасивному стані – ігноруючи або заперечуючи небезпеку. Частина країн, окрім згаданих Британії та Нідерландів, також стикнулися із наслідками втручання Російської Федерації у внутрішню політику своїх держав, зокрема російський слід прослідковувався під час спроб Каталонії вийти зі складу Іспанії та під час підготовки відповідного референдуму. Спроби вплинути на хід переговорів між урядами Північної Македонії та Греції та зірвати ці переговори були теж інспіровані російським режимом (Безверха та ін., 2021).

Окрім втручання у справи окремих країн, суперники Європейського Союзу здійснюють свій вплив, розгортаючи деструктивні інформаційні кампанії, які стосуються контраверсійних тем у європейських суспільствах. Це питання зокрема міграції, підйому ультраправих партій, ісламофобії чи, навпаки, «ісламської загрози». Суперники Європи, зокрема Росія, Китай та Іран, використовують кампанії з дезінформації як недорогі та малоризикові методи для розпалювання ворожнечі, екстремізму та просування своїх наративів, створюючи негативне тло і образ європейських суспільств, зображаючи їх неефективними,

надто бюрократичними чи неповороткими. Європейська конвенція з прав людини захищає основоположні свободи, такі як свобода совісті, свобода вираження поглядів, свободу пересування, декларує заборону дискримінації, забороняє колективне вислання іноземців. Саме ці принципи намагаються зруйнувати автократи, вказуючи на їх нібито неефективність чи застарілість (Корольчук, 2019).

Попри зволікання та певні дебати в середині Європи, Європейська Комісія працює у напрямку протидії дезінформації в мережі. В 2018-му році Комісія підготувала ряд рішень та документів, котрі заклали нові підходи до подолання впливу дезінформації на політику та громадян ЄС. Ці документи є важливим етапом у формуванні нової системи інформаційної безпеки. Одним із найважливіших у цьому переліку документів є «Кодекс практики щодо дезінформації», який започаткував перший стандарт саморегулювання для технологічних компаній. Кодекс встановив вимоги підзвітності, були описані правила прозорості політичної реклами та зобов'язання демонетизації сторінок, що поширюють дезінформацію. Серед компаній, що погодили цей документ, були Facebook, Google та Twitter, а також представники платформ, що представляють рекламну індустрію (Code of Practice on Disinformation, 2018). Після хвилі COVID-19 цей документ був допрацьований самими підписантами та отримав нову версію у 2022-му році, що засвідчило важливість залучення спільнот фактчекерів, покращеної звітності та системи моніторингу.

Вагомим доповненням до Кодексу стало ухвалення закону про цифрові послуги (DSA) в квітні 2022-го року. Фактично, цей закон покликаний регулювати практики, що застосовуються для модерації контенту в соціальних мережах під час виборів. Технологічні компанії отримали нові зобов’язання, які стосуються безпеки даних користувачів, полегшення демократичного контролю і нагляду за платформами. Цей закон привів до консенсусу національні законодавства країн-членів ЄС та дозволив випрацювати правила та рамки для соціальних мереж, які діють на територію усього Союзу (European Commission, [DSA], 2018)

ЄС, вочевидь, керувався нагальною необхідністю вжити рішучих принаймні попередніх захисних заходів до виборів у Європарламент у травні 2019 року, особливо з огляду на те, що російські кампанії з дезінформації посилюють європейські екстремістські групи, підриваючи при цьому позиції правлячих партій та центристів. Агресивне використання Росією дезінформації після повномасштабного вторгнення в Україну в 2022-му році демонструє потенціал авторитарних режимів та засобів, якими вони можуть користуватися у своїх спробах підривати стійкість європейських демократій. Росія Володимира Путіна однією з перших почала масштабне застосування методів державної дезінформації для цифрового середовища — навмисного поширення неточної інформації, призначеної для впливу на суспільства. Інші державні суб'єкти з, можливо, більшими можливостями, такі як Китай, і недержавні суб'єкти, такі як терористичні групи з більшою толерантністю до ризику, адаптуватимуть інструментарій дезінформації для підриву демократії або вже роблять це.

Соціальні мережі демонструють нам інший тип викликів та небезпек, коли суспільство організується в мережах з екстремістськими цілями і також застосовує їх як зброю нового типу. До прикладу, терористичне угрупування «Ісламська держава» мало значний вплив на західне суспільство; шляхом поширення шокуючих відеоматеріалів воно виконувало декілька стратегічних завдань: залучало послідовників та психологічно впливало на свого супротивника. Кампанії в Twitter, Facebook та інших соціальних мережах мали пригнічувати сторону опонента та вселяти відчуття страху перед самопроголошеним халіфатом та неспроможністю демократії упоратися із новітніми викликами (Wilson, 2017)

Можливості соціальних мереж пропонують потенційним новобранцям екстремістських організацій відносно безпечну точку входу для пошуку однодумців і створюють соціальне середовище, в якому унормовані радикальні погляди. Таким чином, соціальні мережі сприяють радикалізації, роблять її менш табуйованою. ІДІЛ адаптував звичайні методи вербування до цифрового інформаційного середовища, що дозволило проводити більш цілеспрямовані

інформаційні кампанії, формував емоційно-резонансні повідомлення та персоналізований досвід роботи з потенційними новобранцями (Rollins, 2011).

Принципи ЄС щодо протидії дезінформації включають вірність свободі слова. Дії європейських держав зосереджені на прозорості, викритті дезінформації та заохоченні платформ соціальних мереж допомагати державі шляхом виявлення та розвінчання таких повідомлень, а не пристосуванні до зловживань цими платформами чи застосуванні жорстких заборон. Задекларований підхід ЄС узгоджується з основними демократичними засадами, але разом із тим існує твердження, що посилення європейського законодавства та регуляторних механізмів у мережі може призводити до розмивання цих принципів відкритості та свободи слова.

Активність іноземних урядів та ведення ними власної державної пропаганди та політичних диверсій, що дозволяє впливати на стабільність в середині європейських країн, доводить необхідність такого регулювання. Проте складним завданням лишається проведення тої межі, за якою демократичний контроль, спрямований на безпеку громадян, не перетворюється в засіб контролю чи спостереження за ними. Так само нерегульованими лишаються питання глобального міжнародного права у цифровій сфері. Соціальні мережі змінюють та розмивають традиційну заборону, яка існує в гуманітарному праві, – заборону здійснювати акти агресії проти цивільного населення. Більшість кампаній з дезінформації або кібератаки в першу чергу здійснюються проти цивільних користувачів соціальних мереж. Авторитарні режими активно користуються цим у мирний час, проводячи свої атаки на банківські системи, системи критичної інфраструктури, урядові портали та здійснюють інформаційний тиск на європейських громадян (Гончар та ін., 2017).

Відбувається поступове розмивання явища агресії, відтак значним викликом лишаються питання, пов’язані із спільною безпекою ЄС та НАТО, адже дедалі важче визначити, де пролягає межа між миром та війною і за якими критеріями має бути застосована 5-та стаття НАТО або інші оборонні заходи. Адже кібератаки можуть розцінюватися як пряма атака на країну-члена альянсу.

Сприяє цій ситуації складність визначення, який саме актор стоїть за атаками, адже безліч неурядових об'єднань хакерів ведуть свою діяльність, викрадаючи дані громадян, доступи до їхніх рахунків, персональну інформацію, листування або комерційну таємницю. Ця активність може мати як комерційну мету, так і здійснюватися на замовлення інших урядів із розвідувальною метою. Встановлення причетності до інформаційних та кібератак є ще одним із викликів, перед якими постали демократичні системи, адже справедливе притягнення до відповідальності є основою права в європейських державах. Відсутність наслідків для сторони, що атакує, підриває довіру до можливості протидії та стримування нових таких атак.

Підвищення рівня проникнення цифрових послуг та соціальних мереж має потенційний зиск для демократичних країн, адже це може суттєво обмежувати корупційні ризики – коли значна частка державних послуг відбувається через цифрові інструменти; і тут показовим є досвід Естонії та України. Відсутність необхідності контакту із чиновниками та бюрократичними бар'єрами дозволяє громадянам отримувати необхідні послуги швидше та прозоріше, не покладатися на людський фактор (Polyakova, 2016). Схожу ситуацію маємо із найважливішим демократичним інститутом – інститутом виборів. Перенесення виборчого процесу в мережу може дозволити проводити вибори, залучаючи ширше коло громадян, відповідно, вибори можуть бути більш доступними та інклюзивними. Інша сторона питання такої цифровізації держави, це – безпека даних громадян-виборців. Адже для функціонування вищезазначених підходів держава має збирати дані про своїх громадян у реєстри, обмінюватися цими даними між базами міністерств та відомств. Цей момент створює ризик того, що ці реєстри можуть бути надзвичайно цінним джерелом інформації та об'єктом підвищеного інтересу для інших держав. Ба більше, можливість впливати на результати цифрових виборів чи референдумів або компрометувати їхні результати може спричиняти системну політичну кризу в демократичних суспільствах.

Разом із технічним прогресом цифровізація буде продовжуватись, доповнюючись новітніми 5G мережами та штучним інтелектом. Методи

дезінформації продовжуватимуть розвиватися. Інновації в галузі штучного інтелекту дозволяють створювати «дипфейки» та інші продукти «синтетичного медіа» — маніпулятивні відео та аудіо з можливістю створювати контент, надзвичайно близький до реального, як-от неіснуючі, але реальні виступи політичних діячів. Оскільки ці інструменти стануть дешевшими та доступнішими, вони стануть ідеальною зброєю для інформаційної війни. Такі технології можуть спричинити наступний великий стрибок у дезінформації. Загалом, методи дезінформації переходять від використання простих ботів, які коментують дописи чи поширюють неправдиву інформацію, до більш витонченого маніпулювання групами незгодних, екстремістськими та іншими організаціям тощо. Таким чином, може бути дедалі важче відокремити дезінформацію іноземного походження від звичайного обміну думок між громадянами у соціальних мережах.

Авторитарні держави та їхні лідери дедалі ефективніше використовуються технології на свою користь, інвестують в технологічні засоби впливу на європейські демократії – це суттєво впливатиме на демократичні європейські суспільства у найближчі десятиліття (Гончар та ін., 2017). Спроможність оцінювати ці виклики та адаптуватися до них будуть визначати стійкість демократичних урядів та їхніх суспільств. Європейським урядам найближчим часом належить визначити усі можливі потенційні небезпеки, породжені соціальними мережами, їхнім впливом на суспільно-політичні питання та сформувати моделі, що дозволить ефективно протистояти авторитарним режимам у боротьбі за європейські демократичні принципи.

У підсумку сучасні інформаційні технології та особливо соціальні мережі розвиваються в умовах глобального протистояння демократичних та авторитарних систем. Це протистояння відбувається у багатьох вимірах, а соціальні мережі стали майданчиком, на якому відбувається активне просування наративів, що можуть шкодити сучасним європейським демократичним принципам. Швидкість поширення наративів та повідомлень в мережі обґрунтовує необхідність адаптивних рішень від влади європейських держав:

процес інформування громадян, засоби розвінчування дезінформації, захист даних громадян мають бути у фокусі тих політик, які мають випрацьовувати демократії, щоб залишатися стабільними. Досвід минулого десятиліття та агресії авторитаризму з допомогою соціальних мереж яскраво демонструє, що відсутність своєчасних рішень та протидій призводить до того, що опоненти сучасних європейських демократій організовують інформаційний простір відповідно до власних інтересів та поточних політичних завдань. Ця ситуація спричиняє кризу довіри до європейських урядів, може негативно впливати на безпеку, дозволяє автократам втручатися у внутрішні справи європейських держав, зривати виборчі процеси, розповсюджувати ворожнечу та спекулювати на слабкостях демократичного устрою.

Соціальні мережі довгий час уважалися інструментом, що сприяє демократії – дозволяє зміцнювати її через відкритість дискусій, робить процес громадянського контролю доступнішим, організовує громадян для акцій протесту тощо. Проте із часом авторитарні системи, вступивши у відкритий конфлікт із демократичним світом, почали активно використовувати соціальні мережі у власних інтересах. В умовах, коли пропаганда часів XX-го століття вже не є ефективною, соціальні мережі є інструментом, через який інформаційний вплив та маніпуляції здійснюються більш витончено, сегментовано та точково. Рекламні інструменти соціальних мереж дозволяють налаштовувати необхідні повідомлення на окремі цільові аудиторії, розколюючи європейські суспільства за найбільш контраверсійними темами.

Цифровізація та перехід до «цифрової демократії» в цих умовах також може бути суттєвим викликом для стійкості європейських урядів та країн. Адже цифрові сервіси та реєстри можуть зберігати значну кількість даних про власних громадян, а процес виборів може бути «відкоригованим» або зірваним. Вочевидь, авторитарні системи, що озброїлися демократичною риторикою, будуть і надалі здійснювати вплив на європейські суспільства, переслідуючи мету їхнього занепаду або уведення в стан гострої кризи.

2.2 Моральний вимір впливу соціальних медіа у ситуаціях соціального напруження та політичних криз.

Технологічний розвиток людства та науковий прогрес супроводжують зміну історичних епох та політичних систем безперервно. Інколи швидкість цих винаходів та технологій стає революційною передумовою до переходу людських спільнот на новий рівень організації або формування проривних філософських чи моральних концепцій; часом недосконалі технології «не встигають» за способом організації суспільства та провокують його «відставання». Так чи інакше, технологічні інновації та проривні ідеї – це вода, яка дозволяє обертатися млинові історії.

Свого часу цьому питанню було присвячено знакову розвідку Джареда Даймонда «Зброя, мікроби і харч», в якій автор розглядав витоки нерівності між народами. Головним завданням цієї роботи став пошук відповіді на амбітне питання – де криються причини, які обумовили винайдення письма, рільництва, вогнепальної зброї певними суспільствами та як вони використали їх для завоювання інших. Одне з найважливіших питань дослідження Даймонда стосувалося пошуку відповіді на питання – чому Китай, який до середини XV ст. можна було вважати технологічним світовим лідером, втратив свою першість та врешті поступився відстаючій у технологіях Європі (Даймонд, 1997).

Рішення цього питання лежить, на думку Даймонда, у декількох площинах. Першою є географія – наявність сполучення через великі ріки та відсутність значних природних перепон в середині Китаю обґрунтувала можливість швидкої централізації держави. Другою причиною він називає відмінний спосіб політичної організації та політичних рішень у Європі та Китаї. Китайська ініціатива «флотилії скарбів», що здійснювала морські походи до африканського узбережжя і мала потенціал до колонізації навколишніх регіонів на початку XV ст., різко обірвалася в певний момент. Ця подія була наслідком значної

централізації китайської держави, наявності авторитарного типу влади та деспотичного способу ухвалювати політичні рішення. В певний момент одним безапеляційним рішенням морські походи були заборонені, а флот – знищений. Європа ж, завдяки своїй політичній різноманітності протягом століть, породила феномен Христофора Колумба, який лише з п’ятої спроби знайшов фінанси для своєї заокеанської експедиції, презентуючи свою амбітну ідею різним європейським правителям (Даймонд, 1997).

В цілому, подібний процес відбувався із іншими технічними винаходами – від паперу до гармат; відсутність єдиного центру в Європі створювала більше можливостей експериментувати із інноваціями в одній частині континенту і згодом поширювати їх на інші суспільства. Цей історичний приклад підводить нас до гіпотези, що тогочасна Європа через особливості свого політичного та географічного облаштування вже була схожою на велику, але ще фізичну мережу. Система магдебурзьких міст, італійських міст-держав, університетів, династій, цехових спільнот, військових союзів, монастирів, графств, герцогств, масонських лож була значною частиною історії Європи протягом багатьох століть. Ці мережі безпосередньо впливали на спосіб організації суспільства, політичний устрій, законодавство, культуру, мораль та етику. І хоча до винайдення телеграфу, радіо, цифрових мереж та глобального інтернету людство перебувало у достатньо фрагментованому стані, мережеві спільноти прямо чи опосередковано здійснювали свій вплив.

Мережі, як їх визначає Джошуа Рамо, – це набори поєднаних між собою вузлів, які можуть бути утворені з фінансових ринків, людей, будь-яких елементів, що придатні до поєднання. Форма мережевої організації може визначатися мовою, валютою чи географією або сотнями інших означень. Владою, за такого підходу, можна вважати спроможність додавати нові групи елементів до цієї сукупності мереж (Рамо, 2018). Приклад Христофора Колумба показовий, адже монтування колоніальної системи, започатковане королем та королевою Іспанії, – це значною мірою про реалізацію влади шляхом додавання нових елементів (заокеанських колоній, нових торгових шляхів) до мережі, що

існувала раніше. Вочевидь, ці «старі» мережі значно відрізнялися від нашого сучасного уявлення про те, якою має бути мережа. Швидкість обміну товарами та технологіями, інформацією чи політичними ідеями в середні віки та ранньомодерний час в таких мережах була низькою, зважаючи на обмеження історичної доби: відсутність стандартизованої освітньої системи, швидких засобів зв'язку та механічного транспорту. В таких умовах «сповільнених» мереж трансформації у спільнотах відбуваються протягом тривалого часу (Рамо, 2018).

Для того щоб змінилися підходи до політики, виникли нові політичні ідеї або змінилися базові уявлення про співвідношення політики та моралі, потрібно значно більше часу, ніж у XX чи XXI столітті. Поняття моралі та її співвідношення із політичною сферою рука об руку розгорталося протягом європейської історії, формуючи тяглість та окремі філософські школи. Роздуми про мораль, як і довгий список інших європейських «винаходів», сягають глибиною часів античності та Греції. Греко-римський світ породив значну кількість концептів, термінів та підходів до моралі та чеснот. Між античністю з її комплексом уявлень про світ, підходів до організації суспільства та поняттям «полісу» можна з упевненістю ставити знак рівності.

Поліс – це невелика та компактна спільнота, що існує в модусі самодостатності та автономного існування. Платон, наприклад, визначав, що оптимальним числом родин у полісі є 5040 (Себайн & Торсон, 1997). Грецький світ, за своєю суттю, є надзвичайно камерним; в такому світі кожен повноправний суб'єкт спільноти повсякчас має відтворювати моделі поведінки, закріплені в цій спільноті, а найвищою формою покарання стає вигнання. В такій спільності певні типи поведінки толеруються та охороняються, а деструктивні та такі, що порушують баланс в середині спільноти, вважаються надзвичайно тяжкими. Демонстративною тут є історія про смерть Сократа. Відтак кожен громадянин оцінюється за допомогою специфічних чеснот та якостей, наприклад, індивідуалізм та навіть індивідуалістичні форми економічної діяльності засуджуються греками і мають власний термін – «гібріс». Гібріс, в грецьких уявленнях, призводить до надміру, зарозумілості, а саме бажання відділитися від

інших представників спільноти означає загрозу для цілого полісу. Полісна людина, захищаючи свій простір, породжує цілий спектр морально-етичних категорій, які мають працювати на збереження цього полісу. Цей грецький підхід зумовив не лише специфічний культурний «прорив» Давньої Греції з її класицистичними зразками архітектури та мистецтва, але й дав поштовх мислителям та філософам шукати відповіді на питання моралі та етики. Потреба випрацювати власні явлення про мораль і її взаємозв'язок із політичною сферою є зрозумілою. Адже в грецькому полісі брати участь в політиці – було основним завданням кожного повноправного громадянина (Чумаченко, 2003).

Мораль відображає певний набір цінностей, які є важливими для суспільства; її основним завданням є регулювання та корекція поведінки кожного індивіда у соціумі. Мораль має пояснювати, що в рамках спільноти вважається «добром», а що «злом». Цей базовий рівень дозволяє толерувати певні «потрібні» форми поведінки для того чи іншого суспільства. Разом із тим, категорія моралі органічно конфліктує з іншими проявами діяльності людини, де «моральний» спосіб поведінки є, скоріше, обмеженням. До прикладу, політика, яка функціонує на принципах змагальності та конкуренції, складно поєднується із вимогами, які до людини ставить феномен моралі.

Ми бачимо, як грецька полісна політична система породила комплекс ідей, пов'язаних із тим, як співвідноситься політика та мораль. Окрім впливових сюжетів Геродота про греко-перські війни та протистояння «армії вільних громадян» проти «армії рабів», де чітко прокладена межа між світом цивілізованим та варварським, або платонівської філософії про способи облаштування держави, маємо і роздуми Аристотеля про політику та її співвідношення із мораллю. Аристотель демонструє цей тип полісного мислення, адже для нього участь в політиці і діяльність на користь свого полісу та спільноти – це органічний вияв суб'єктності кожного громадянина. Аристотель стоїть на засадах того, що політика має бути, в першу чергу, етичною, а публічне життя кожної вільної людини є її найважливішою місією. Участь у політиці, за його уявленнями, має бути спрямованою на досягнення загального блага спільноти, а

отже толеруються рішення, які відповідають грецьким уявленням про «arete», яке уособлює в собі досконаліть, гідність, чесноту та доблесть. У цій давньогрецькій полісній мережі постійна включеність у публічне життя і самопожертва на благо полісу – це спосіб демонстрації власної моральної якості. Очевидним у цьому контексті є специфічне ставлення греків до тиранії, деспотизму, демагогії, індивідуалізму – ці явища загрожують самій полісній ідеї, вони дестабілізують та кидають виклик основам, що закладені у грецьку моральну систему координат. Завершення полісного періоду європейської історії та подальші модифікації уявлень про політику та мораль відбувалися разом із руйнуванням старих політичних систем та появою нових, приходом нових релігійних учень та технологічного прогресу.

Християнська мораль передбачала домінантність церкви у всіх проявах людського буття, в першу чергу, в способах організації держави і влади та поглядах на природу людину. Святий Августин та Тома Аквінський відстоювали ідею того, що влада є божественною за своєю суттю та походить від Бога, через це вона має бути підпорядкованою церкві. Августин утверджував концепцію того, що людина є первісно-гріховною, вона має спиратись на певний абсолют і так виправляти свою ураженість. Християнське вчення породило не один політичний конфлікт, в основі якого лежала суперечка про розподіл владних повноважень, зокрема відома боротьба «папацезаризму» проти «цезарепапізму» – один із наслідків значного посилення церкви у Середньовіччі (Буено де Мескіта, 2025). Процес переходу від античних ідеалів полісного життя до середньовічних християнських королівств відбувався досить тривалий час. Погляди на мораль та природу людини модифікувалися поступово. Еразм Роттердамський допускав, що людина є ураженою первісним гріхом, вона може самостійно відновитися, покладаючись на свої найкращі якості. Християнство залишалося важливим інструментом регуляції поведінки в середині спільнот та способів легітимації влади протягом століть; його становище похитнулося лише разом із надзвичайним стрибком у технічному та філософському розвитку людства.

Античні та середньовічні суспільства меншою мірою залежали від технологічних інновацій та наукових проривів, які би суттєво вплинули на фундаментальні уявлення про мораль, політику, владу тощо. Значні трансформації в середині європейських спільнот розпочалися разом з винаходом Йоганом Гутенбергом у XV столітті друкарського верстата. Ймовірно, вперше в історії технологія, що пришвидшує потік інформації, породить мислителів та ідеї, які досить радикально вплинуть на підходи до управління, питань моралі, легітимності влади та способів організації суспільства.

Маршал Мак-Люен обстоював тезу, згідно якої поява технології книгодрукування запустила трансформацію усіх сфер життя людини. Мак-Люен доводить, що інформація впливає на те, в який спосіб індивід сприймає навколишній світ, вона формує його переконання та уявлення. Разом із пришвидшенням інформаційного потоку хвилеподібним чином починають проростати ідеї свободи, науки, капіталізму. Передова технологія друкарства закладає фундамент для появи націй та націоналізму у майбутньому, адже саме друк обумовив процес втрати церквою монополії на знання та поступового відходу від традиційного способу переписування книг при монастирях (Мак-Люен, 2015).

В цих умовах модернізація перетворює політику та природу влади та відповідно погляди на їх поєднання з мораллю. За своєю суттю, політика і мораль мають схоже завдання – організовувати людські спільноти, робити життя в них гармонійним та безпечним. Попри це, ці дві категорії мають потенціал до конфлікту, адже мораль – це набір уявлень, що притаманні індивіду. Мораль регулює поведінку людини на рівні персональних щоденних форм поведінки та пропонує певний ідеал, якого варто намагатися досягти. Політика ж є сферою публічного, де співіснують та конкурують інтереси різних представників суспільства, кожен із яких на своєму індивідуальному рівні може мати відмінний набір уявлень про мораль та чесноти.

Цю конфліктність відчував Ніколо Макіавеллі, який у своєму трактаті «Державець» пропонує у царині політики керуватися доцільністю та інтересами.

Для Макіавеллі використання насилля до підданих – цілком прийнятний інструмент політика, однак він розділяє «добре» та «погане» використання насильства. Якщо воно вчиняється одноразово, в інтересах підданих та для спільного блага – таке насильство є виправданим та мудрим; натомість постійне його повторення – це прямий шлях до втрати влади. Макіавеллі допускає, що державець може вчиняти негідні вчинки, але має зберігати позитивний образ для підданих, адже їхня ненависть чи постійних страх є шкідливими та небезпечними для правителя. В цілому, підхід Макіавеллі передбачає, що політика не має підпорядковуватися моралі і ставити перед собою завдання, досягнення яких є важливішими за моральні приписи (Макіавеллі, 2007).

Ніколо Макіавеллі – представник епохи, яку породив друкарський верстат. Бачимо, що технологічний прогрес запустив процеси переосмислення політики та принципів, якими мають керуватися політичні актори та яким має бути їх етичний «кодекс». Доба Макіавеллі – це також початок формування розлогих мереж на європейському континенті. Його «Державець» демонструє помітні зміни у ставленні до політики та моралі, які контрастують з полісним світоглядом Аристотеля. Ці два підходи до співвідношення політики та моралі давні – вони склалися у традицію, разом із тим, поява нових технологій призвела до появи нових викликів та моральних дилем, в яких технологічні інновації впливають на політичні інституції, владу та громадян.

Джошуа Рамо говорить, що модернізація нерозривно пов’язана зі зростанням кількості мереж у суспільствах. На його думку, пришвидшення швидкості обміну інформації в середині мереж «революціонізує саму сутність влади» та політики: *«Такі фундаментальні переходи з однієї фази в іншу, де "більше" означає "інше"...»* (Рамо, 2018, с. 41). Якщо мережі часів Макіавеллі ще залишалися «повільними», то подальший науковий прогрес та індустріалізація постійно пришвидшували інформаційний потік. Сучасні соціальні мережі стають ключовими інструментами для формування нових мереж впливу, які можуть об’єднувати людей навколо спільних ідей та цінностей, незалежно від географічних кордонів. Соціальні мережі дозволяють створювати нові форми

політичної мобілізації, що можуть обходити традиційні структури влади. Це особливо помітно в контексті розрізнених акцій непокори, де соціальні медіа відіграли вирішальну роль у координації дій протестувальників та поширенні їхніх ідей. З політологічної точки зору, цей феномен викликає питання щодо легітимності нових форм влади, що виникають у мережевому суспільстві. Як саме соціальні мережі впливають на легітимність політичних лідерів і чи можуть вони стати основою для нових форм політичної організації? Це питання стає особливо актуальним у контексті зростання популярності популістських лідерів, які активно використовують соціальні медіа для мобілізації власних прихильників.

Сучасні соціальні мережі та інтернет-платформи не в останню чергу вплинули на формування «стисненого» маклюенівського світу. Вагомий внесок соціальних мереж в позитивні політичні перетворення першої чверті XXI століття відтіняє дискусію про вплив соціальних мереж на суспільства та політику, їхні взаємозв'язки з мораллю та чеснотами. Мануель Кастельс під час своїх лекцій у Гарварді стверджував, що: *«Ми є свідками народження нової форми соціального руху. Інформаційні технології живили масивні, надзвичайно рухливі соціальні хвилі. Ці рухи за якусь мить пройшли еволюцію від невидимих до нездоланних»* (Castells, 2012). Розвиток і поширення соціальних мереж породили не одну моральну дилему, які зазвичай не розглядаються науковцями та дослідниками цієї теми. Найбільш вагомим лишається питання: наскільки політичні та філософські системи встигають за цифровим прогресом, яким чином вони відповідають на виклики, які породжують новітні та інноваційні засоби передачі інформації?

Еразм Роттердамський, Миколай Коперник, Мартін Лютер та Ніколо Макіавеллі означили перехід від епохи усної словесності до друкованого слова. Керовані духом критицизму, постановки нових запитань та відкидання старих догм, ці мислителі впливали на політичний та моральний горизонт власної епохи. Джошуа Рамо у своїй роботі «Сьоме чуття» пропонує розглядати сучасну добу як епоху, яку майбутні історики зможуть назвати «Епохою великого підключення»,

порівнюючи її з добою Просвітництва та іншими революційними відтинками історії людства (Рамо, 2018).

Вирішальний вплив соціальних мереж на процеси демократизації та протистояння авторитарним режимам нині не викликає суперечок. Разом із тим, що більше соціальні мережі стають невід'ємною чистиною побуту, відбувається наростання критичних зауваг та застережень, які стосуються цієї технології. Ба більше, об'єктом критики та скептичних спостережень стають засновники цих мереж, люди, які символізують перехід до мережевого суспільства. Перед тим як розглянути моральний вимір соціальних мереж у ситуаціях соціального напруження та політичних криз, варто розглянути комплекс тих питань, які стосуються архітекторів цих мережевих систем, їхніх поглядів на суспільство, мораль та політику.

Один із прикладів – послідовна критика мережі Facebook у публічному просторі. Цікавий фокус продемонстрований, зокрема, на сторінках американського видання The Atlantic. Де, у своїх дискусійних статтях, авторка Едріенн Лафранс пропонує розглядати цю соціальну мережу як найбільшу «авторитарну систему на Землі» (LaFrance, 2021). Едріенн Лафранс аналізує глобальний вплив Facebook як платформи, що трансформувалась з соціальної мережі в потужного наднаціонального суб'єкта. За її спостереженням, засновник Facebook Марк Цукерберг виступає не стільки у ролі підприємця, а швидше є лідером цифрової держави, яка складається з 2,9 мільярдів активних користувачів. Ця цифра перевершує сукупне населення Китаю та Індії. Для Лафранс Facebook – це значно більше, ніж комунікаційний майданчик, це платформа, яка поступово наближається до здобуття власної суб'єктності, наприклад, через запровадження власної цифрової валюти.

У статтях Лафранс наскрізним наративом є небезпека соціальних мереж, яка зумовлена специфічними, на її думку, моральними якостями засновника цієї мережі. Вочевидь, такий спосіб пояснювати природу Facebook через особливості моральних якостей її засновника – досить нетиповий спосіб аналізувати вплив соціальних мереж на суспільство. Авторка в першу чергу звертає увагу на той

тип управлінських та політичних рішень, які властиві менеджменту Facebook, насамперед її засновнику. Очевидним є той факт, що соціальні мережі вже досить довгий час відіграють значно більшу роль, ніж просто засіб комунікації між друзями, рідними чи однокласниками. Фейсбук, зокрема, перетворився на політичний інструмент, засіб консолідації та мобілізації суспільства для певних політичних перетворень чи революцій. Однак Едрієн Лафранс критикує Марка Цукерберга за своєрідну форму «макіавеллізму», де мета виправдовує засоби, адже, на її думку, керівництво мережі сповідує декларовані демократичні цінності, але водночас зберігає одноосібний контроль за ключовими рішеннями у компанії та концентрує владу у своїх руках (LaFrance, 2020). Лафранс відстоює позицію, відповідно до якої Facebook став значущою загрозою для демократичних цінностей та свобод, адже платформа слугує джерелом поширення кампаній з дезінформації, а її алгоритми підіграють емоційним маніпуляціям та негативно впливають на суспільство (LaFrance, 2024).

Лафранс пропонує термін «техноавторитаризм», який нерозривно пов’язує соціальну мережу з переконаннями та моральними орієнтирами її засновника. Авторка описує цей феномен у контексті специфічного середовища бізнес-еліт у Кремнієвій долині. Такі компанії, як YouTube, X та насамперед Meta, на її думку, уособлюють нову форму авторитарної технократії, де технологічний прогрес виправдовує нехтування демократичними нормами, приватністю та етичними принципами. Основна критика зосереджена на тому, що одержимість масштабуванням і досягненням глобального домінування ставить прибуток і зростання компаній вище за етичні міркування та відповідальність перед суспільством (LaFrance, 2020).

У її статтях підкреслюються антидемократичні переконання цих нових технократів, які, попри декларовану прихильність до цінностей Просвітництва – розум, прогрес і свободу – насправді ведуть антидемократичний і неліберальний курс. Багато з них декларують абсолютну підтримку свободи слова, проте виявляють неприязнь до критики та незручних висловлювань. Їхні погляди часто є нестандартними: вони вважають, що будь-який технічний розвиток завжди

позитивний, що слід створювати нові технології лише через те, що це можливо, що безперервний інформаційний потік є найважливішим незалежно від його якості. «Їхня головна мета — безмежна влада», говорить Лафранс. Створювані ними системи, що перебудовують комунікацію, соціальні мережі та впроваджують штучний інтелект у повсякденне життя, нав'язують ці переконання суспільству, не консультуючись із громадськістю і не інформуючи про це (LaFrance, 2024).

У статті «Народження техноавторитаризму» проведені паралелі між ідеологією Кремнієвої долини та рухами початку 20-го століття, такими як футуризм і технократія, що прагнули замінити традиційні демократичні структури керуванням технічної еліти. Авторка підкреслює лицемірство технологічної еліти, яка, декларуючи свободу слова та інновації, насправді придушує інакодумство та ігнорує соціальні наслідки своїх дій.

У цьому контексті цікавим є спільне для багатьох дослідників і авторів бачення раннього етапу розвитку всесвітньої мережі в 90-х роках минулого століття. *«Усесвітня мережа в середині дев'яностих була прекрасна. Індустрія поринула в ідеалізм та утопічні мрії*», – пише Роджер Макнамі (Макнамі, 2021, с. 55). Він демонструє поширене оптимістичне уявлення про те, що ця технологія робитиме світ демократичнішим, вільнішим. Технологічний оптимізм того періоду, на думку Макнамі, призвів до однієї з фундаментальних суперечностей, які були закладені у всесвітню мережу від самого її створення – неможливість ідентифікації користувача та віра у те, що усі користувачі мають бути анонімними (Макнамі, 2021).

Схожі спостереження висловлювала у своїх статтях і Едріен Лафранс, яка зізнавалася, що вбачала в перших соціальних мережах потенціал до продуктивних змін. Ідеалізм «першопрохідців» інтернету відзначають також Ерік Шмідт та Джаред Коен з компанії Google. Можна констатувати, що надмірна ідеалізація мережевих технологій кінця минулого століття породила хвилю розчарування, зокрема серед людей, які докладалися або були залученими спостерігачами у процесі становлення інтернету та соціальних мереж. Одним з

таких авторів є згаданий вище Роджер Макнамі, який був інвестором у Facebook та близьким радником засновника платформи – Марка Цукерберга. Макнамі стверджує, що технологічні платформи були створені з ідеалістичною метою – «об'єднати світ». Однак за революцією соціальних мереж, яку очолював Facebook, є непомітна «катастрофа», яка стосується демократії, економіки, виборчих процесів, захисту персональної інформації. Макнамі слушно зауважує, що поява нової технології нерідко нагадує магію, а найвдаліші технологічні рішення активно умонтовуються в повсякдення і трансформують способи організації людських спільнот (Макнамі, 2021, с. 23)..

Досвід користування такими технологіями, серед яких можна назвати смартфони, інтернет чи соціальні мережі, веде до неодмінних змін в людині. *«Технології, починаючи з телебачення, змінюють спосіб нашої взаємодії зі світом, замінюють активно громадянську позицію пасивним споживанням контенту й ідей, а розмови – комунікацією в цифровому середовищі»*, – говорить Макнамі (Макнамі, 2021, с. 23). На його думку, громадяни поступово перетворюються на споживачів та поступово втрачають суб'єктність. Вочевидь, вельми критичний погляд автора на вплив соціальних мереж нерозривно пов'язаний із його переконанням про те, що перемога в Сполучених Штатах лібертаріанських ідей, з пріоритетом на індивідуальне, а не колективне благо, в останній чверті XX-го століття, породила кризу етики та моралі.

На думку Макнамі, лібертаріанська мораль дозволяє «не соромитися своїх амбіцій чи жадоби»; він йде далі, висуваючи тезу про те, що така філософія дозволяє уникати відповідальності за власні управлінські чи політичні рішення. Щоб урівноважити такий спосіб пояснювати мораль засновників компаній-техногігантів, варто відзначити, що насправді він є частиною традиційної дискусії про те, чи спричиняє вільний ринок і накопичення багатства моральному занепаду, чи навпаки культивує цінності та сприяє формуванню сталого суспільства. Разом із тим, емпіричні дослідження не підтверджують ідею того, що ринкова економіка призводить до розмивання моральних норм. Автори такого дослідження – Джастін Каллейс, Колін Харріс, Бен Борчард у 2022-му році

встановили, що суспільства із розвиненою ринковою економікою мають вищий рівень довіри та несприйняття аморальної поведінки (Callais et al., 2022).

З Роджером Макнамі можна погодитись в тому, що соціальні мережі і алгоритми їхньої роботи можуть репрезентувати морально-етичну систему координат своїх засновників; вони є органічним продуктом того, що Джошуа Рамо називає добою «мережевої влади» – влади, яка будується через вплив на різноманітні мережеві структури. Погляди та цінності сучасної технократичної еліти можна прослідкувати на прикладі «Маніфесту технооптиміста», який був опублікований у 2023-му році на ресурсах великого інвестиційного фонду Andreessen Horowitz, який активно інвестує в соціальні мережі та інтернет-платформи. Так, до прикладу, фонд відомий своїми інвестиціями у X (Twitter) та Facebook. Своїми фінансовими діями він формує «цифровий ландшафт» в середині глобальної мережі. Текст маніфесту належить співзасновнику фонду – Марку Андреессену (Andreessen, 2023). Деякі з тверджень, наведених у цьому маніфесті, дозволяють проаналізувати погляди людей, які є впливовими і дотичними до рішень та вектору, за яким розвиваються інноваційні мережі та стартапи у сфері соцмереж та глобальних комунікацій. Розглянемо декілька тез з цього документу:

- «Ми віримо, що технології – це важіль впливу на світ – спосіб робити більше з меншими витратами».
- «Ми віримо, що немає жодної матеріальної проблеми, створеної природою чи технологією, яку не можна було б вирішити за допомогою нових технологій».
- «Ми вважаємо, що ринки не вимагають від людей ідеальних чи навіть добрих намірів – і це добре…».
- «Девід Фрідман зазначає, що люди роблять щось для інших лише з трьох причин – любові, грошей чи сили. Любов не має масштабу, тому економіка може працювати лише на грошах чи силі. Силовий експеримент було проведено та визнано необхідним. Давайте триматися грошей».

- «Ми вважаємо, що основний моральний захист ринків полягає в тому, що вони відволікають людей, які інакше створювали б армії та створювали релігії, до мирних продуктивних занять».

Твердження, що наведені у маніфесті, є досить радикальними; запропонований спосіб взаємодії з технологіями та інноваціями ставить їх на чолі усього прогресу людства. В маніфесті демонструється абсолютне захоплення безмежним горизонтом до експериментування із технологіями, яке, на думку Андреессена, не має штучно регулюватись. Необхідність обмежень та обачливого застосування технологій – елемент, якого ми не побачимо у цьому есе. Фактично, в розумінні автора, технологія є позитивною апріорі, вона позбавлена моральних дилем і викликів, а спроби обмежень та регулювання – шкодять та призводять до людських втрат та страждань.

Не менш цікавою для дослідження особливостей моралі новітньої «мережевої еліти» є згадка про віру технооптимістів у давньогрецьку «eudaimonia», яку варто досягати через «arete» (згадане раніше у контексті полісної моралі). Звертаючись до досвіду греків, Андреессен говорить: «Ми віримо у процвітання через досконалість», – разом із тим він трансформує це явище, підлаштовуючи його до світогляду сучасної цифрової людини. Адже в цій інтерпретації залишається лише одна зі складових «arete» – досконалість, довершеність (Andreessen, 2023). Натомість гідність, чеснотність та доблесть лишаються поза увагою. В маніфесті можна зустріти і інші посилання на грецьку традицію та світосприйняття, щоправда ідеї запропоновані у ньому, за суттю, є ближчими до ідей, які пропонував Ніколо Макіавеллі. Індивід зі своїми моральними, політичними та персональними якостями у світі технократів розчиняється у щільній павутині мереж, по суті, позбавлений необхідності етичної регуляції. В той же час сила та агресивність – проголошені необхідною чеснотою «нового цифрового світу», якщо говорити термінологією Шмідта та Коена.

У словах цього маніфесту можна відшукати своєрідний виклик державним інституціям та політичним системам. Твердження про те, що «національна сила ліберальних демократій витікає з економічної сили, культурної сили та військової

сили. Економічна, культурна та військова сила випливає з технологічної сили», – це недвозначна амбіція вже сформованих технократичних еліт впливати на процеси як в середині власної держави, так і на питання глобальної політики. Вочевидь, що соціальні мережі, різноманітні месенджери чи відео-хостинги вже мають значний вплив на політику та мораль, однак у запропонованій вище ідеї відсутнє бачення та конструктивні пропозиції до того, в який спосіб технології можуть сприяти демократії у світі чи вирішувати глобальні загрози і виклики, а не доповнювати їх або створювати нові.

В контексті цього маніфесту варто згадати напрацювання Гаетано Моски, який відомий своїми дослідженнями елітаризму. Він стверджував, що суспільство завжди управляється меншістю, яка встановлює правила і норми для більшості. У контексті соціальних мереж ця теорія набуває нового значення. Сьогодні еліти не обов'язково належать до політичного класу чи традиційної інтелігенції; нові цифрові еліти формують нові моральні стандарти і визначають суспільний порядок денний. Саме ці нові еліти мають значний вплив на формування нових соціальних норм через соціальні мережі. Вони встановлюють стандарти поведінки, які можуть або відповідати традиційним моральним принципам, або кардинально від них відрізнятися, що призводить до зміни суспільного морального клімату.

Девід Прістленд у своїй роботі «Купець, воїн, мудрець: нова історія влади» вкладає європейський історичний процес у рамку конкуренції основних груп еліт, які він означує індійською категорією «каст». Першою кастою Прістленд називає касту купців – мотивовану ринком і діловими якостями, другою кастою він називає касту солдатів, а третьою – касту мудреців або клірикiв. Для Прістленда тісна взаємодія, поєднання чи конкуренція між цими елітними групами є «локомотивом історії»; у своєму баченні він ідейно продовжує напрацювання Моски з його концепцією «циркуляції еліт». На думку Прістленда, домінування однієї з каст викликає кризу, після якої владу отримує інша каста; ці зміни приносять із собою також і визначні перетворення в суспільствах (Priestland, 2012).

Джошуа Рамо звертається до робіт Прістленда, аргументуючи, що можна відстежити появу нової елітної «касти», яка контролює розлогі сітки мереж. Для усталених політичних та етичних систем поява цієї когорти нової еліти – значний виклик, через їхню спроможність створювати та розробляти нові цифрові системи та мережі, в яких вони є єдиними творцями законів та правил, ба більше, етичних принципів. Глибоке проникнення технології в повсякденне життя західних (але не виключно) суспільств обумовлює значні можливості нової «касти» утримувати владу. Джошуа Рамо говорить про те, що ці еліти визначатимуть майбутнє та наступні перетворення в нових мережевих системах. Він порівнює нову технократичну еліту з мореплавцями часів становлення європейських імперій – Христофором Колумбом чи Васко да Гамою, які здійснювали свої відкриття, обмінюючи їх на знання, статки, статус та славу. Разом із тим, залишається відкритим питання, наскільки добре західне суспільство, що є надзвичайно включеним у систему нових мереж, розуміє, якими якостями володіють нові еліти, які створюють мережі, підключають до них все більшу кількість користувачів та встановлюють розуміння поняття «зло» та «добро» в середині цих мереж.

Однією з ключових теорій, яка може пояснювати процеси трансформації морального виміру у середині соціальних мереж, – це теорія гегемонії Антоніо Грамші. Грамші передбачає, що культурні і моральні норми формуються і підтримуються домінуючими соціальними групами, які володіють владою контролювати суспільний дискурс. У цифрову епоху соціальні мережі також можуть бути інструментом для досягнення гегемонії, де корпорації, політичні лідери та впливові особи мають можливість формувати моральні норми через контроль над контентом і алгоритмами. За Грамші, гегемонія — це не лише контроль над державними інститутами, але й панування певних ідей та цінностей, які стають домінуючими у суспільстві (Грамші, 2017). Соціальні мережі відтак стають платформою та інструментом для встановлення нових гегемонічних порядків. Наприклад, впливові бренди чи політичні діячі використовують свої платформи для просування певних моральних цінностей,

які потім поширюються через мережі і стають частиною соціальних норм. Це підсилює динаміку, коли нові норми з'являються і швидко поширюються, витісняючи традиційні моральні стандарти.

У цифрову еру кожна точка зору може знайти свою аудиторію, незалежно від того, наскільки вона відповідає загальноприйнятим етичним нормам. Це створює середовище, де всі точки зору можуть бути представлені як рівноцінні, навіть якщо вони суперечать базовим принципам моралі. Наприклад, через соціальні мережі поширюються різноманітні конспірологічні теорії, які ставлять під сумнів наукові факти і моральні принципи, на яких будується суспільство. Пітер Померанцев, говорить, що це може призводити до того, що традиційні моральні орієнтири втрачають свою значущість, а суспільство стає більш поляризованим (Померанцев, 2015). У політичному контексті це може призвести до підриву довіри до інститутів влади, адже різні групи починають керуватися різними моральними нормами, що ускладнює досягнення суспільного консенсусу. За таких умов розрізнені групи у суспільстві намагаються встановити свої цінності як загальноприйняті. Це може бути особливо помітно на прикладі кампаній, які використовують соціальні мережі для мобілізації масової підтримки. Наприклад, рухи на кшталт #MeToo або #BlackLivesMatter є прикладом того, як певні групи намагаються змінити домінуючі моральні стандарти через цифровий активізм.

Дослідження впливу морального виміру соціальних мереж на людину тільки розпочинається і становить доволі обмежене коло наукових праць, частину з яких було згадано вище. Разом із тим, можна з упевненістю говорити, що кількість запитань і моральних дилем, які породжують соціальні мережі у різних контекстах, поступово наростає. Одними із таких найперших питань першого десятиліття XXI століття були питання про те, як соціальні мережі впливають на взаємодію індивіда із суспільством та на його поведінку. Так звана «епідемія самотності», породження соціальними мережами, викликала серйозне занепокоєння у науковому середовищі. Ці пересторогі зрештою отримали розголос, до прикладу, в статті Стівена Марша із назвою «Facebook робить нас

самотніми?», де проаналізований новий тип соціального страху — страх самотності та ізоляції, породжений соціальними мережами (Marche, 2012).

Основна думка статті зосереджена на парадоксі, що виник із технологічним розвитком: з одного боку, технологічний прогрес забезпечив безпрецедентний доступ до засобів комунікації через соціальні мережі. З іншого боку, ці технології насправді створюють умови для поверхневих взаємодій, що підриває соціальну солідарність і знижує якість суспільних відносин. Як наслідок, виникає нова форма самотності — «самотність у натовпі», коли індивід може мати сотні «друзів» у соціальних мережах, але разом із тим традиційні соціальні зв'язки порушуються і посилюється ризик соціальної атомізації (Marche, 2012).

Подальше проникнення соціальних мереж у життя людини породило наступний перелік питань – про етичність використання користувацьких даних алгоритмами соціальних мереж. Особливо гостро це питання постало в один із найважливіших моментів розвитку Facebook – цим моментом стала поява новинної стрічки у соціальній мережі. Ця зміна, за своєю суттю, перетворила мережу, призначену для «об'єднання людей», в платформу, яка шляхом постійних експериментів та покращень алгоритмів все більше схожа на новинний ресурс, який конкурує з традиційними медіа.

Стрічка новин – це центральний стрижень в архітектурі багатьох сучасних соціальних мереж. Спосіб організації цієї стрічки, частота її оновлень, принципи, які закладені у підходи до контенту, який бачить користувач, беззаперечно впливає на спосіб взаємодії з мережею і також впливає на його світосприйняття. Досвід компанії Facebook показує, що експерименти із емоціями користувачів породжують новітні моральні дилеми. Так, наприклад, відомим став ряд експериментів, які дослідники проводили, використовуючи стрічки близько 690 000 користувачів мережі. Метою експерименту було встановити взаємозалежність між тим, який тип контенту – позитивний, негативний чи нейтральний – отримує користувач та який контент після тривалої взаємодії він поширює вже самостійно. Результат експерименту показав ефект «емоційного зараження» і підтвердив, що налаштування стрічки впливають на реакцію

користувачів: негативні повідомлення, наприклад, отримують більшу активність та залучають користувача до більшого написання слів, а зменшення позитивного контенту у стрічці викликає зростання негативно забарвлених слів в дописах користувача. В дослідженні зазначається, що щоденна кількість контенту в мережі значно переважає можливості одного користувача для її перегляду, відтак в мережі передбачений набір алгоритмів для призначення рейтингу одній одиниці контенту. Відповідно до цього ранжування відбувається пріоритезація – які повідомлення потрапляють у стрічку, а які залишаються поза нею (Kramer et al., 2014).

Проте сам алгоритм фільтрації та деталізовані принципи формування стрічки – тема, яку представники соціальних мереж оминають від моменту їх появи. Компанії Meta (Facebook, Instagram) та ByteDance (TikTok) майже не надають даних для незалежних дослідників. Вочевидь, що сам експеримент здійснювався відповідно до Політики використання даних Facebook, яку формально підтверджують усі користувачі при реєстрації, і в цілому не порушував законодавства. Проте його таємне проведення піднімає ряд етичних питань про наслідки подібних експериментів над емоціями людей, що користуються мережею. Експеримент над стрічкою користувачів Facebook виходить далеко за межі тих перших пересторог щодо соцмереж, які стосувалися впливу на окремі явища соціальної поведінки: самотність чи самовпевненість, повертає до питання про етичність впливу на емоції користувачів.

Експеримент довів значний приріст активності, які бачили емоційно насичені повідомлення; ця специфіка може мати різносторонній вплив на публічні обговорення та дискусії в мережі. Наприклад, публічний осуд є однією з нових форм соціального контролю, яка набула значного поширення завдяки соціальним мережам. Коли певна особа або група порушує суспільно визнані моральні норми, користувачі соціальних мереж швидко мобілізуються, щоб висловити своє обурення і засудити ці дії. Це може мати позитивний ефект, змушуючи членів спільноти дотримуватися соціальних норм і бути відповідальними за свої вчинки. Схожий механізм вже описував Мішель Фуко у

свої книзі «Наглядати і карати», описуючи паноптикум – в'язницю, де кожен індивід перебуває під наглядом, не маючи змоги розпізнати, чи спостерігають за ним у кожний конкретний момент часу. В такий спосіб здійснюється саморегуляція та нормалізація поведінки у суспільстві (Фуко, 2020). Завдяки цій якості соціальні мережі можуть відігравати ключову роль у викритті корупції та порушеннях прав людини та інших форм аморальної поведінки. Публічне обговорення цих питань у соціальних мережах дає громадянському суспільству додаткові можливості впливати на політичні процеси, змушуючи уряди реагувати на критику і вживати відповідних заходів.

Разом із тим, алгоритми соціальних мереж здатні провокувати деструктивний вплив на соціум, адже у соціальних мережах такі кампанії з публічного осуду мають потенціал набирати неконтрольованих масштабів, що призводить до стигматизації та дискредитації не лише окремих індивідів, але й цілих груп, іноді без належних доказів їхньої провини. Це створює моральну дилему: з одного боку, соціальні мережі забезпечують механізм соціальної відповідальності, з іншого — сприяють нестабільності, коли відсутність чітких критеріїв для засудження може призвести до несправедливих наслідків.

Юрген Габермас у своїй теорії публічної сфери наголошував на важливості відкритого та раціонального обговорення суспільно важливих питань (Habermas, 1993). Соціальні мережі можна розглядати як нову форму публічної сфери, де кожен має можливість брати участь у формуванні суспільних норм. Проте, соціальні мережі часто перетворюються на простір для емоційних, а не раціональних дискусій, що може мати деструктивний вплив на суспільні моральні норми, розмиваючи їх шляхом формування множинних інтерпретацій відносно тієї чи іншої події. Принципи, закладені в алгоритми фільтрації та добору відображуваного в мережі контенту, із постійним збільшенням кількості користувачів в інтернеті та соціальних мережах впливають на великі соціальні системи та політичні процеси, що відбуваються в них. Ювал Ной Харарі у своїй статті «Чому технології сприяють тиранії» розвиває цю дискусію та аналізує вплив новітніх технологій, таких як штучний інтелект та соціальні мережі, на

політичні системи та демократичні цінності. Він стверджує, що соціальні мережі, завдяки контролю над масивними обсягами даних, стають інструментами маніпуляції та пропаганди. Ці платформи, на його думку, дозволяють централізувати владу і сприяти поширенню авторитаризму, формуючи упередження та поляризацію серед населення. Соціальні мережі, будучи частиною більш широкої екосистеми технологічного контролю, можуть підривати здатність людей до незалежного мислення та самоврядування, що веде до зростання нерівності та політичного відчуження (Harari, 2018).

На думку Харарі, сучасна демократична модель може опинитися під загрозою через алгоритми, що керують поведінкою користувачів у соціальних мережах, формуючи їхні політичні вподобання. Автономія особистості в умовах технологічного прогресу стає дедалі більш ілюзорною, коли люди все більше залежать від рішень, прийнятих на основі алгоритмічного аналізу їхніх даних. У цьому контексті соціальні медіа виступають як посередники, які маніпулюють публічним дискурсом, зміщуючи акценти з об'єктивної правди на емоційно заряджений контент. Це створює умови для глибокої політичної поляризації та поширення дезінформації, що особливо небезпечно в авторитарних системах, де ці інструменти можуть використовуватись для придушення інакомислення та зміцнення режиму.

Крім того, Харарі розглядає глобальну боротьбу за домінування в сфері технологій, де соціальні мережі стають ареною для міждержавних конфліктів та інформаційних війн, які позбавлені будь-яких правил або моральних обмежень. Алгоритмічний контроль дозволяє не тільки комерційним структурам, але й урядам ефективніше маніпулювати громадською думкою, посилюючи політичну нерівність. В умовах, коли алгоритми керують вибором контенту та формують сприйняття реальності мільйонів людей, постає питання про майбутнє демократичних свобод та права на самовизначення. Таким чином, Харарі підкреслює, що соціальні мережі, поряд із іншими технологіями, можуть стати інструментом глобального технологічного контролю, який позбавлений моральних обмежень і дилем, у випадку якщо не будуть розроблені етичні та

регуляторні механізми для захисту фундаментальних прав. Він закликає до критичного підходу до управління технологіями, щоб уникнути перетворення їх на засіб пригнічення, а не звільнення, у нову епоху цифрового контролю (Harari, 2018).

Сучасні політичні кампанії, що розгортаються у соціальних мережах, часто базуються на маніпуляціях, емоційних закликах та спрощених рішеннях складних проблем. Це веде до поляризації і радикалізації суспільства та спотворення публічних обговорень, коли замість раціональних аргументів превалюють популістські твердження. Цей процес також впливає на моральні норми, сприяючи їхній еволюції у напрямку більшої нетерпимості до інших думок і підсилюючи конфліктність у суспільстві.

«Моральна паніка» є ще одним важливим концептом, який варто розглянути в контексті впливу соціальних мереж на сферу моралі. Цей термін, який став популярним завдяки роботам Стенлі Коена, описує процес, коли певні соціальні проблеми або явища роздмухуються до масштабів, що викликають надмірне суспільне занепокоєння і паніку (Cohen, 2017). Соціальні медіа стали новим простором для формування моральної паніки, оскільки вони дозволяють інформації поширюватися з неймовірною швидкістю і в глобальних масштабах. Це особливо помітно в умовах криз, таких як пандемія COVID-19, коли соціальні мережі стали головним джерелом інформації для багатьох людей. Однак разом з правдивою інформацією, вони також сприяли поширенню фейкових новин і конспірологічних теорій, що підсилювало моральну паніку та створювало атмосферу недовіри. Соціальні мережі є дієвим інструментом маніпуляції громадською думкою, коли моральна паніка використовується для досягнення політичних або економічних цілей.

Теорія соціального конструювання реальності Бергера і Лукмана наголошує, що соціальні реалії, включно з моральними нормами, є продуктом колективної взаємодії та інтерпретації (Berger & Luckmann, 1966) . У цифровому середовищі ця взаємодія прискорюється і поширюється на глобальному рівні. Соціальні мережі створюють умови для впливу на колективну свідомість і ведуть

до швидкого оновлення соціальних норм. Цей підхід дозволяє глибше зрозуміти, чому і як моральні норми, що колись були вкорінені в традиціях і звичаях, тепер піддаються постійним змінам під впливом соціальних мереж. Ці зміни часто є відповіддю на глобальні події, такі як політичні кризи, природні катастрофи або пандемії, які підсилюють важливість певних норм і роблять їх домінуючими у суспільстві.

Відповідно до цієї теорії, соціальна реальність конструюється через мову, комунікацію та спільні уявлення про світ. У сучасному контексті соціальні мережі стали головним інструментом, через який ці процеси відбуваються, адже значна частка комунікації відбувається саме з допомогою мереж. Соціальні мережі дозволяють користувачам активно брати участь у конструюванні соціальної реальності, формуючи та поширюючи нові соціальні норми та моральні стандарти. Поведінкові норми, які колись вважалися стабільними, тепер постійно піддаються перегляду та переформатуванню під впливом цифрових кампаній або масових онлайн-дебатів. Це підтверджується такими кейсами, як масові кампанії «відміни», акції проти кібербулінгу, що швидко стають трендом і змушують соціальні платформи переглядати свої політики. Завдяки цьому платформи, такі як Twitter, Facebook чи Instagram, стають полем битви за визначення того, що є «морально правильним» або «неправильним».

Таким чином, мережі можна розглядати як структуру, що безпосередньо впливає на контекст і порядок денний моральних питань. Контроль над тим, які питання висвітлюються, як вони інтерпретуються та поширюються, надає платформам соціальних медіа значну владу над формуванням моральних норм. Наприклад, платформи, що належать великим корпораціям, можуть просувати певні ідеї або блокувати інші, тим самим впливаючи на суспільну моральну свідомість. Це також стосується підйому або падіння рухів, що базуються на поняттях моралі, таких як #MeToo чи екологічних кампаній, де контроль над порядком денним стає ключовим чинником їхнього успіху або провалу.

Політичні та соціальні процеси все більше підкоряються логіці медіа, що веде до зміни традиційних уявлень про вплив соціальних мереж на моральний

вимір. Соціальні мережі, які стали основними каналами комунікації для багатьох людей, тепер також виконують функцію формування та трансформації моральних стандартів (Strömbäck & Esser, 2017). Ця медіатизація створює нові виклики для традиційних інститутів моралі, таких як релігія чи сім'я, які раніше виконували роль головних арбітрів моральності. Наприклад, моральні питання, які колись обговорювалися в контексті церковних громад або сімейних дискусій, тепер стають публічними і масовими завдяки соціальним мережам. Це змінює не лише процес формування моральних норм, але й саму природу цих норм, роблячи їх більш відкритими для впливу зовнішніх факторів, таких як популярні тренди чи політичні інтереси. В таких умовах соціальні мережі сприяють тому, щоб політика набувала певних форм шоу, де головне — це ефектність та емоційність, не обтяжена обмеженнями моралі чи цінностей. Моральні норми у такому середовищі стають нестабільними і піддаються постійним змінам, що може призводити до нестабільності в середині суспільства.

Розвиток технологій має величезний вплив на політичні процеси, соціальні системи та моральні норми протягом історії. Спроби осмислити вплив технологій на людські спільноти відбувалися здавна, особливо вона прискорилась у ХХ-му столітті, коли технології досягли суттєвого рівня розвитку. Від спроб Джареда Даймонда відповісти на питання, чому західна цивілізація стала успішною, до питання – як мережеві технології впливають на появу нової еліти та перерозподіл влади, питання про значення технологічних інновацій завжди цікавило дослідників. Маршал Мак-Люен у своїх роботах описував, як винахід технології друкарства змінив політичні, моральні, економічні та суспільні інститути у Європі та світі. Він попереджав про те, що люди, найглибше занурені у революційні перетворення, не можуть збагнути усю їх суть і відчути справжню глибину змін – ця проблематика є актуальною і для революції у комунікації, яку спричинили соцмережі. Цей спосіб пояснювати сучасне суспільство через трансформаційну технологію, яка змінює старі форми сприйняття і мислення, добре описує ті зміни, які фундаментально впливають на людину з появою Інтернету та соціальних мереж.

Ці технології пришвидшують обмін інформацією, що змінює природу політичної влади, призводить до появи нових форм соціальної організації та трансформує суспільні відносини. Однак ці зміни не є однозначно позитивними: вони супроводжуються значними моральними дилемами та потенційними загрозами для демократичних політичних систем. Сьогодні соціальні мережі перетворилися на потужний інструмент для формування суспільної свідомості та моральних норм, а також стали важливим фактором політичної мобілізації. Вони створюють нові можливості для демократичних перетворень. Водночас соціальні мережі стають засобом маніпуляції громадською думкою, поширення дезінформації та поляризації суспільства, чим охоче користуються авторитарні режими.

Традиційні способи погляду на політику як справу, що має обмежуватися мораллю, можемо відслідкувати від часів Аристотеля. Інший погляд на політику представлений Ніколо Макіавеллі, з його тезою про те, що цілі та інтереси політики не мають обмежуватися питаннями моралі та етики. Джошуа Рамо стверджував, що усі подальші трансформації, які з собою несе мережева цифрова доба, будуть так чи інакше політичними. І моральні дилеми в середині соціальних мереж не позбавлені тієї ж проблематики – чи мають соціальні мережі обмежуватися мораллю або їх подальший розвиток не має бути штучно обмеженим, про що говорять «техноптимісти».

Етичні питання, пов'язані з використанням даних користувачів та алгоритмів, які визначають їхній досвід у мережі, стають все більш актуальними. Маніпуляції з емоціями користувачів, експерименти над їхнім світосприйняттям та можливості централізованого контролю над інформаційними потоками викликають серйозні занепокоєння. Це може призвести до підриву демократичних інститутів та встановлення нових форм авторитаризму, про які говорять Ювал Ной Харрарі, Адрієн Лафранс та Роджер Макнамі. Для цих авторів притаманний погляд на соціальні мережі та нові комунікаційні технології як потенційну небезпеку, що підриває сталість у суспільстві, руйнує старі соціальні зв’язки і змінює звичні етичні та моральні принципи. Вони описують

соціальні мережі у світлі «макіавелівських» підходів, звертаючи увагу на небезпеки в залежності принципів роботи соціальних мереж від моральних якостей засновників та архітекторів цих мереж.

Технологічний прогрес не тільки змінює способи комунікації та політичної мобілізації, але й впливає на моральні стандарти, що регулюють поведінку в суспільстві. Соціальні мережі, з їхньою здатністю до швидкого поширення інформації та мобілізації великих груп людей, стають новою ареною для боротьби за гегемонію, де нові еліти встановлюють свої моральні норми, витісняючи традиційні. Моральний вимір впливу соціальних мереж у ситуаціях політичних та соціальних збурень залишається важливим для розуміння сучасних політичних процесів.

Взаємодія між етичними принципами та політичною комунікацією значно ускладнюється через швидке поширення інформації в онлайн-просторі, що часто супроводжується дезінформацією, маніпуляцією та підбуренням до насильства. Соціальні мережі не лише служать майданчиком для висловлення думок, а й можуть стати інструментом для маніпуляції масовою свідомістю, сприяючи політичній нестабільності та поглибленню соціальних конфліктів. У такому контексті моральний вимір впливу соціальних мереж на політику залишається невід'ємною частиною дискурсу щодо відповідальності політичних акторів і необхідності забезпечення етичних норм та обмежень у цифровому просторі.

Соціальні мережі стали новим полем боротьби за владу, де моральні стандарти формуються та змінюються під впливом цифрових еліт, віральності контенту та емоційних обговорень. Соціальні мережі можуть сприяти сталості громадянського суспільства і поширенню нових соціально відповідальних норм, але також можуть стати інструментом маніпуляції, що підриває довіру до традиційних політичних інститутів і призводить до «моральної паніки», про яку говорив у своїх роботах Стенлі Коен.

Цей процес призводить до формування нових моральних дилем, які постають перед користувачами та суспільством у цілому. У цьому контексті виникає питання моральної відповідальності як самих користувачів, які

опиняються у «інформаційних бульбашках» і взаємодіють із контентом, який відповідає їхнім власним переконанням, так і власників платформ, які повинні гарантувати достовірність інформації та запобігати її зловживанню.

Висновки до розділу 2

Аналіз політичного та морального вимірів впливу соціальних мереж дозволяє констатувати, що сучасна європейська демократія опинилася в стані глибокої кризи, спричиненої невідповідністю традиційних інститутів швидкості цифрових трансформацій. Соціальні мережі, які раніше вважалися «технологіями визволення», сьогодні дедалі частіше виступають інструментами ерозії демократичних принципів. Це проявляється у виникненні гібридних режимів, які вдало поєднують ринкову економіку та цифрову риторику з жорстким контролем над суспільною думкою.

«Керована демократія» використовує демократичні підходи та процедури, а також алгоритми соціальних платформ для створення ілюзії плюралізму, де реальна політична конкуренція замінюється сегментованим маніпулюванням емоціями цільових аудиторій. Моральна криза цифрової доби полягає у домінуванні логіки «техноптимізму», яка відкидає етичні обмеження заради безмежного масштабування та прибутку. Трансформація публічної сфери (за Ю. Габермасом) у простір емоційно заряджених «інфодемій» та «моральних панік» руйнує можливість раціонального суспільного консенсусу. Алгоритмічне ранжування контенту, засноване на емоційному зараженні, не лише підриває довіру до об'єктивної правди, а й веде до централізації влади у руках нової технократичної еліти.

Ці актори, володіючи більшим обсягом даних про громадян, ніж національні уряди, фактично встановлюють нові моральні норми в обхід демократичного контролю. У підсумку, стійкість європейських суспільств у ситуаціях соціального напруження прямо залежить від здатності відродити

етичну суб’єктність індивіда. Захист демократії сьогодні потребує глибокого переосмислення відповідальності архітекторів цифрових систем.

Перед демократичним світом постає виклик випрацювання нової «цифрової етики», яка б урівноважувала владу алгоритмів перед ризиком остаточного переходу до «технологічної тиранії», де ілюзія «підключеності» приховуватиме тотальне відчуження особистості від реальних важелів впливу на політику.

Розділ 3. СОЦІАЛЬНІ МЕРЕЖІ ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКОВОЇ ПОЛІТИКИ

Проблема інтеграції соціальних мереж у систему національної та колективної безпеки Європейського Союзу є стратегічним пріоритетом сучасної оборонної політики. Зміст цього розділу передбачає аналіз еволюції підходів ЄС до цифрового середовища: від початкового фокусу на кібербезпеці до визнання соцмереж ключовим фактором гібридних загроз та інструментом інформаційної війни. Важливим аспектом дослідження є розкриття феномену «веапонізації» (weaponization) соціальних мереж та типізація «цифрової зброї» за характером її впливу на інфраструктуру, психіку, алгоритми та соціальні зв'язки суспільства. У межах розділу досліджуються особливості національних безпекових стратегій країн-членів ЄС — від жорсткого юридичного регулювання контенту до формування моделі «суспільного щита. Особлива увага приділяється адаптації концепції «стовпів підтримки» Джина Шарпа та досвіду Едварда Лукаса для обґрунтування моделі «цифрової громадянської оборони», здатної забезпечити стійкість демократичних систем в умовах системного протистояння з авторитарними режимами.

3.1 Роль соціальних мереж та цифрового середовища у рамках безпекової політики ЄС

Ніл Фергюсон стверджує, що найбільшим викликом для сучасної демократії є втрата спільної публічної сфери. В епоху, коли ефірне телебачення тотально домінувало в інформаційній сфері, більшість громадян дивилися однакові вечірні новини та політичні програми, що створювало спільний контекст для національного діалогу. Сьогодні, завдяки персоналізованим стрічкам новин у Facebook та інших мережах, кожен користувач отримує «індивідуально підігнану версію реальності» (Фергюсон, 2018). Алгоритми конструюють інформаційні бульбашки, де користувачі бачать лише те, що підтверджує їх переконання. Це робить практично неможливим ведення

змістовної розмови між людьми з різними політичними поглядами, оскільки вони оперують різними наборами фактів і живуть у паралельних інформаційних всесвітах.

Розуміння сучасного медіасередовища є стратегічно важливим для оцінки будь-яких політичних процесів, зокрема в Європейському Союзі. Дані Євробарометра свідчать, що громадяни ЄС нині живуть в епоху гібридної інформаційної системи, що хоч і частково, але підважує твердження Фергюсона про передову роль соціальних мереж в інформаційному полі. Всупереч поширеним уявленням про повне витіснення «старих» медіа «новими», реальність є складнішою. Традиційні та цифрові джерела інформації не стільки конкурують, скільки співіснують, формуючи комплексні та багатошарові звички медіаспоживання серед громадян ЄС. Як саме соціальні мережі впливають на демократичні процеси в країнах Європейського Союзу і як громадяни європейських країн взаємодіють з інформацією можна прослідкувати на даних комплексного дослідження «Social Media Survey 2025», проведеного Євробарометром на замовлення Європейського Парламенту в червні 2025-го року (European Commission, 2025).

Аналіз показує, що традиційні медіа (телебачення, радіо, преса) все ще зберігають міцні позиції: 66% європейців звертаються до них щодня. Водночас цифрові джерела (соціальні мережі, новинні портали, блоги) щоденно використовують 59% громадян. Це свідчить про паралельне існування двох потужних інформаційних потоків, які доповнюють один одного. Ієрархія джерел, до яких громадяни звертаються за інформацією про соціально-політичні події, підтверджує цю гібридну модель, де телебачення (71%) зберігає беззаперечне лідерство, однак розрив між іншими традиційними медіа, такими як радіо (43%) та преса (41%), і цифровими та особистими джерелами — соцмережами, пошуковими системами та особистими контактами (по 40%) — практично зник. Динаміка за останній рік є особливо показовою. Хоча телебачення продовжує посилювати свої позиції (42% респондентів відзначили його зростаючу важливість), саме соціальні мережі демонструють найпотужніший висхідний

тренд: 25% громадян вважають, що їхня роль як джерела новин зросла. Це значно перевищує показники для друкованої преси (19%), радіо (18%) та пошукових систем (18%), і свідчить про поступовий, але невпинний зсув у медіаландшафті.

Розуміння моделей поведінки користувачів на цих платформах є ключем до оцінки їхнього реального впливу як на громадянську активність, так і на процеси політичної поляризації. Дані Євробарометра дозволяють детально проаналізувати, як саме європейці споживають політичний контент і долучаються до дискусій онлайн. Передусім, увага користувачів сконцентрована на кількох домінуючих платформах. Основними майданчиками для отримання новин є:

• Facebook (58%)

• YouTube (57%)

• Instagram (46%)

Така концентрація означає, що алгоритми трьох американських компаній мають надзвичайний вплив на те, яку саме політичну інформацію бачать мільйони європейців, що ставить серйозні питання щодо інформаційного суверенітету ЄС.

Дослідження дозволяє побачити подвійний характер споживання політичного контенту. З одного боку, 76% користувачів зізнаються, що натрапляють на таку інформацію випадково під час перегляду стрічки. З іншого боку, 66% стверджують, що шукають її на соціальних платформах практивно. Цей феномен «випадкового інформування» є надзвичайно важливим: пасивна модель споживання робить громадян вкрай вразливими до алгоритмічно підібраного контенту, який може пріоритезувати залучення (гнів, емоції) над фактичною точністю, створюючи таким чином сприятливі умови як для поляризації, так і для дезінформаційних кампаній.

Аналіз рівня та якості громадянської активності в мережі демонструє чітке домінування пасивних форм взаємодії над активними. Це можна представити у вигляді ієрархії залучення:

• Пасивне споживання. Найпоширенішими діями є читання або перегляд контенту (38%) та проставлення лайків чи інших реакцій (36%).
• Активна, але обмежена взаємодія. Значно менша кількість користувачів вдається до коментування (23%) або поширення чужого контенту (19%).
• Створення оригінального контенту. Лише 11% користувачів створюють та публікують власні дописи зі своїми думками та поглядами.

Ці дані свідчать, що для переважної більшості європейців соціальні мережі є радше простором для спостереження за політикою, аніж для активної участі в ній. Така модель поверхневого залучення, керована простими реакціями, створює ідеальне підґрунтя для швидкого поширення дезінформації та маніпулятивного контенту.

Дезінформацію слід розглядати не просто як «фейкові новини», а як системну загрозу, що підриває довіру до демократичних інститутів, посилює суспільну фрагментацію та руйнує саму основу для раціонального політичного діалогу. Ефективність дезінформаційних кампаній прямо пов'язана із загальним рівнем довіри в суспільстві: чим нижча довіра до урядів, експертів та медіа, тим простіше поширюються маніпуляції. Додатково, близько 35% громадян ЄС вважають, що стикалися з дезінформацією «дуже часто» або «часто» лише протягом останнього тижня. Це вказує на те, що маніпулятивний контент у свідомості європейців став невід'ємною частиною їх щоденного інформаційного досвіду. Поширення дезінформації створює значні ризики для демократичного дискурсу в Європейському Союзі, адже сама архітектура платформ, оптимізована для залучення, а не для правдивості, робить європейський інформаційний простір вразливим до маніпуляцій — як внутрішніх, так і зовнішніх.

Водночас аналіз готовності громадян протидіяти цій загрозі дає змішану картину. З одного боку, 61% респондентів почуваються впевненими у своїй здатності розпізнати дезінформацію. З іншого боку, стратегії верифікації, які вони використовують, часто є обмеженими та не завжди надійними. Серед таких інформаційних «фільтрів» бачимо:

1. Перехресна перевірка з іншими джерелами (49%). Це найбільш ефективний метод, але він вимагає від громадянина додаткових зусиль, часу та високого рівня медіаграмотності.
2. Перевірка автора допису (40%). Ця стратегія свідчить про покладання на репутацію, що в умовах інформаційних бульбашок не верифікує факти, а лише підсилює вже існуючі переконання, незалежно від їхньої правдивості. Це класичний прояв упередження підтвердження.
3. Перевірка коментарів (29%). Це один із найменш надійних методів, оскільки коментарі можуть бути легко сфабриковані ботами або організованими групами, що створює хибне враження суспільного консенсу.

Особливе занепокоєння викликає той факт, що 10% громадян ЄС не роблять абсолютно нічого для перевірки сумнівної інформації, що робить їх найбільш вразливою ціллю для маніпуляцій. Проблема дезінформації нерозривно пов'язана із глибинною кризою довіри до інституційних джерел інформації. Дані Євробарометра чітко ілюструють, кому саме довіряють європейці, коли йдеться про суспільно-політичні питання.

Джерело	Рівень довіри (найбільше довіряють)	Коментар
Друзі та родина	45%	Свідчить про розпад довіри до інституційних «вертикальних» джерел та відкат до «горизонтальної» довіри в межах особистих мереж, які є особливо вразливими до неперевіреної інформації та емоційних маніпуляцій.

Вчені	45%	Показує високу довіру до експертного знання, яке, однак, не завжди легко транслювати в поляризований публічний дискурс.
Журналісти	13%	Вказує на глибоку кризу довіри до професійних медіа, які мали б бути головним запобіжником проти дезінформації.
Публічні інституції	13%	Підкреслює значну відстороненість громадян від держави та її комунікацій.
Політики	5%	Сигналізує про майже повну втрату довіри до політичного класу, що робить демократичні процеси вразливими.
Інфлюенсери	4%	Показує, що нові цифрові лідери думок, попри свою популярність, не сприймаються як надійне джерело серйозної політичної інформації.

Примітка. Дані адаптовано з Social Media Survey 2025, European Commission, 2025 (https://europa.eu/eurobarometer/surveys/detail/3592)

Низький рівень довіри до інститутів, медіа та політиків створює ідеальний вакуум, який заповнюється дезінформацією, теоріями змови та емоційними маніпуляціями. Цей ефект, однак, є неоднаковим у різних країнах Європейського Союзу.

Вплив соціальних мереж на демократію не є універсальним для всього Європейського Союзу. Він значною мірою залежить від національного політичного, культурного та медійного контексту кожної окремої країни. Аналіз

цих відмінностей дозволяє уникнути надмірних узагальнень та побачити мозаїку різноманітних сценаріїв, що розгортаються в цифровому просторі ЄС.

Існують країни з традиційно високим рівнем політичної залученості, як-от Греція (61% громадян «часто» обговорюють політику) та Кіпр (59%). На протилежному полюсі знаходяться країни, де політичні дискусії є значно менш поширеними, наприклад, Латвія (лише 24%). Вибір основного джерела інформації також суттєво різниться. Хоча в більшості країн ЄС телебачення залишається домінуючим, існує виразна група країн, де ситуація кардинально інша. На Кіпрі, Мальті, в Греції, Латвії та Угорщині саме соціальні мережі є основним джерелом новин для громадян. Цей зсув може бути пов'язаний з низкою факторів, зокрема з історичною недовірою до державних чи олігархічних традиційних медіа, високим рівнем поляризації медіапростору або специфічними демографічними моделями використання інтернету. Це має глибокі наслідки для політичного дискурсу в цих країнах, роблячи його більш залежним від алгоритмічних стрічок.

Національний контекст також визначає тематичні пріоритети громадян, які вони відстежують у медіа. Дані Євробарометра показують, що соціальні мережі, ймовірно, не стільки створюють нові теми, скільки посилюють увагу до тих питань, які вже є центральними в національному порядку денному.

• Міграція та притулок: Ця тема викликає найвищу зацікавленість у країнах, що є або основними напрямками міграції, або де це питання є ключовим у внутрішній політиці, зокрема в Німеччині (64%) та Нідерландах (58%).

• Оборона та безпека ЄС: Цілком очікувано, ця тема є найбільш актуальною в країнах східного флангу ЄС, які безпосередньо межують із РФ: в Литві (53%), Фінляндії (53%) та Польщі (51%).

Таким чином, єдиної «європейської» моделі впливу соціальних мереж на політику не існує. Натомість ми бачимо мозаїку національних сценаріїв, де глобальні цифрові тренди переломлюються крізь призму місцевих реалій. Це вимагає розробки диференційованого підходу як до регулювання цифрового

простору, так і до протидії загрозам як на рівні всього Союзу, так і специфічним загрозам у кожній країні-члені ЄС.

Аналіз даних Євробарометра підтверджує тезу про двоїсту природу впливу соціальних мереж на демократичні процеси в Європейському Союзі. З одного боку, вони беззаперечно розширили можливості для доступу до інформації та стали невід'ємною частиною медіаландшафту. З іншого боку, вони не лише не вирішили старих проблем, а й поглибили існуючі, зокрема низьку довіру до інститутів, суспільну фрагментацію та вразливість до дезінформації.

Для розуміння глобального впливу соціальних мереж на демократичні процеси вкрай важливо проаналізувати, як їх сприймають звичайні громадяни в різних культурних та політичних контекстах не лише в ЄС. Масштабне дослідження Pew Research Center, проведене у 19 розвинених країнах, дає змогу побачити глобальну картину цих настроїв, яка виявляється напрочуд неоднозначною.

Всупереч поширеній тривожній риториці, у більшості досліджених країн переважає позитивна оцінка ролі соціальних мереж. Медіанний показник у 57% респондентів вважають, що ці платформи є «скоріше позитивними» для демократії в їхній країні, тоді як 35% дотримуються протилежної думки. Найбільш оптимістично налаштовані громадяни Сінгапуру, Польщі та Швеції, де понад 65% респондентів бачать позитивний вплив. Такий позитивний образ соціальних мереж у суспільній уяві конкретної країни потребує детального вивчення та окремих розвідок. Можна припустити, що це може бути наслідком політичної культури з одного боку, так і вдалих урядових стратегій (тут варто відзначити успіхи Швеції) по підсиленню спроможності громадян опиратися деструктивним впливам в соціальних мереж та свідомій відмові громадян взаємодіяти з токсичною інформацію.

На цьому тлі Сполучені Штати виглядають головним винятком. Американське суспільство демонструє найвищий рівень скептицизму та негативного сприйняття. Згідно з даними Pew Research Center. 64% дорослих американців вважають, що соціальні мережі мають поганий вплив на

американську демократію, і лише 34% вбачають у них позитивний ефект (Pew Research Center, 2025). Цей разючий контраст між США та більшістю інших розвинених країн є ключовим індикатором того, що вплив соціальних мереж не є універсальним і значною мірою залежить від внутрішніх політичних та соціальних умов. Що саме зумовлює таку різницю в оцінках? Які конкретні переваги та недоліки бачать громадяни, що формує їхню загальну думку? Розглянемо спочатку ті аспекти соціальних мереж, які громадяни по всьому світу вважають корисними для демократії.

Попри численні ризики, громадяни в багатьох країнах продовжують бачити значну цінність у соціальних мережах як у політичному інструменті. Це можна пояснити тим, що ці платформи дають відчуття впливу у той час, коли традиційні політичні інститути здаються віддаленими або ж закритими. Дані Pew Research Center свідчать, що медіана 65% респондентів у 19 країнах вважають, що політична система не дозволяє таким людям, як вони, мати вплив на політику. Саме на цьому тлі соціальні мережі сприймаються як альтернативний канал для участі та вираження своєї позиції.

Дані Pew дозволяють виділити декілька ключових переваг, які громадяни пов'язують із соціальними мережами:

• Підвищення інформованості: Медіана 73% респондентів вважає, що люди стали більш поінформованими про поточні події у своїй країні, й ідентична медіана 73% стверджує те саме про події в інших країнах.

• Мобілізація уваги: Переважна більшість (медіана 77%) бачить у соціальних мережах ефективний спосіб привернення суспільної уваги до важливих проблем.

• Вплив на владу та політику: Значна частина громадян (медіана 64%) вважає соціальні мережі дієвим інструментом для того, щоб змусити посадовців звернути увагу на певні питання. Також 61% (медіана) вважають, що ці платформи можуть впливати на політичні рішення.

Ці ефекти розширення можливостей є проявом процесу «діалогізації», як його визначають Ліллквіст та група дослідників. Ця концепція описує тенденцію, що сприяє поліфонії (наявності багатьох незалежних голосів) та респонсивності

(взаємодії та реагуванню). Соціальні мережі, з цієї точки зору, створюють простір, де громадяни можуть кидати виклик усталеним владним структурам та домінуючим наративам, вносячи власні теми до публічного порядку. Таким чином, соціальні мережі сприймаються як цінний ресурс саме там, де традиційні демократичні механізми здаються неефективними. Вони дають громадянам інструменти, щоб їхній голос був почутий (Lillqvist et al., 2016).

Позитивне сприйняття соціальних мереж як інструменту розширення можливостей суттєво нівелюється їхніми негативними наслідками, які є універсальною проблемою. Навіть у країнах з позитивною загальною оцінкою переважна більшість громадян визнає руйнівний потенціал онлайн-платформ. Два ключові явища, що викликають найбільше занепокоєння, – це дезінформація та політична поляризація. Дезінформація – поширення неправдивої інформації та чуток – сприймається як одна з головних загроз. Дані Pew свідчать, що медіана у 84% респондентів вважає, що інтернет і соціальні мережі зробили людей більш вразливими до маніпуляцій. Це відчуття вразливості підриває довіру до інформації та інститутів, що є критичним для функціонування демократії (Pew Research Center, 2022).

Політична поляризація є іншим руйнівним наслідком. Медіана 65% респондентів погоджується, що соціальні мережі зробили людей більш розділеними у своїх політичних поглядах. Крім того, медіана 44% вважає, що люди стали менш цивілізованими у політичних дискусіях, що свідчить про зростання токсичності.

Ці негативні явища можна пояснити через концепцію «монологізації» — протилежності діалогізації. За своєю суттю цей феномент описує процес, коли дискурс в соціальних мережах слугує інтересам маніпулятора на шкоду інтересам аудиторії (Lillqvist et al., 2016). Потужні політичні актори, подібно до корпорацій, прагнуть встановити контроль над дискурсом: вони уникають гострих тем, поширюють вигідні наративи та використовують риторичні прийоми для нейтралізації критики. Дизайн платформ, що алгоритмічно надає перевагу емоційному та конфліктному контенту, сприяє цьому. Замість

справжньої взаємодії виникає «псевдосоціальність» (Thurlow, 2013), що створює лише ілюзію спілкування, а насправді слугує політичним чи комерційним цілям. Результатом стає не діалог, а «набір одночасних монологів», що поглиблює ідеологічні розколи в середині суспільства

Саме баланс між силами «діалогізації», що дає громадянам голос, та «монологізації», що дозволяє маніпулювати цим голосом, визначає загальне сприйняття соціальних мереж. І приклад США яскраво демонструє, що відбувається, коли негативні ефекти починають домінувати. Сполучені Штати є критично важливим прикладом для розуміння того, як негативні аспекти соціальних мереж можуть повністю переважити їхні потенційні переваги в очах суспільства. Дані Pew Research Center чітко показують, що американці набагато песимістичніше оцінюють вплив цих платформ на демократію, ніж громадяни інших демократичних країн.

Показник	**США**	**Медіана по 19 країнах**
Вважають соцмережі шкідливими	64%	35%
Вважають, що соцмережі посилюють розкол	79%	65%
Вважають, що люди стали менш цивілізованими	69%	44%

Примітка. Дані адаптовано з *Social Media Seen as Mostly Good for Democracy Across Many Nations, But U.S. is a Major Outlier*, Pew Research Center, 2022 (https://www.pewresearch.org/global/2022/12/06/social-media-seen-as-mostly-good-for-democracy-across-many-nations-but-u-s-is-a-major-outlier/).

Аналіз цих даних дозволяє зробити висновок, що в американському контексті маніпулятивні та поляризаційні сили («монологізація») сприймаються

як значно потужніші за можливості для громадянської участі («діалогізація»). Якщо в інших країнах громадяни ще бачать баланс між перевагами та недоліками, то в США переважна більшість відчуває домінування негативних ефектів, які отруюють політичний клімат.

Важливим фактором є надзвичайно високий рівень політичної поляризації в самій країні. Дані Pew свідчать, що республіканці (74%) ставляться до соціальних мереж значно негативніше, ніж демократи (57%). Це вказує на те, що глибокий суспільний розкол є одночасно і причиною, і наслідком негативного сприйняття цих платформ. Соціальні мережі не просто відображають існуючі конфлікти, а й активно їх посилюють. Ця внутрішня корозія громадянського дискурсу є не лише внутрішньою проблемою; вона створює системні вразливості, на які активно націлюються авторитарні суперники на світовій арені.

Внутрішньодержавні проблеми, посилені соціальними мережами, не існують у вакуумі. Вони є частиною ширшого глобального ідеологічного конфлікту, який Майкл Макфол описує як новий глобальний безлад — протистояння між демократичними та авторитарними режимами (McFaul, 2025). У цій боротьбі соціальні мережі перетворилися з інструменту комунікації на потужну зброю. Авторитарні режими, зокрема Росія та Китай, експортують свою внутрішню модель інформаційного контролю у глобальний цифровий простір. Вони активно використовують «монологізуючі» функції соціальних мереж — дезінформацію, маніпулятивні кампанії та пропаганду — для підриву демократичних суспільств зсередини. Посилюючи існуючу поляризацію, розпалюючи соціальні конфлікти та поширюючи недовіру до урядів і виборів, вони цілеспрямовано використовують відкритість демократичних систем проти них самих.

Це ставить перед демократичними країнами надзвичайно складну дилему. Як протидіяти зовнішнім інформаційним загрозам та які стратегії випрацьовувати? Іншу регуляторна дилема, в якій демократії змушені балансувати на небезпечній межі, описана Юджином Волохом. ЇЇ він позначає

термінами «урядовий тиск» та «урядовий примус» — діями, що ризикують підірвати ту саму свободу слова, яку вони прагнуть захистити. Еволюція засобів масової комунікації пройшла шлях від жорсткої медіа-олігархії середини XX століття до сучасної централізації на базі великих технологічних компаній. У 1960-х роках свобода преси фактично належала лише власникам друкарських верстатів. Поява інтернету на початку 2000-х років створила короткочасну ілюзію повної демократизації мовлення (за Волохом - епоха «дешевого мовлення»), коли кожен індивід отримав технічну можливість поширювати інформацію мільйонними тиражами (Volokh, 2024).

Проте сучасний ландшафт виявив системну вразливість: замість володіння власними засобами поширення, користувачі фактично «позичають» інфраструктуру у великих платформ, таких як Facebook, X (Twitter) або YouTube. Така концентрація зробила ці платформи надзвичайно потужними політичними акторами, здатними впливати на результати виборів, що одночасно перетворило їх на пріоритетні цілі для державного тиску. Владі значно легше спрямувати зусилля на контроль над кількома глобальними посередниками, ніж намагатися модерувати мільйони незалежних вузлів мережі.

Яскравим проявом запропонованої Волохом гіпотези є дискусія навколо законопроєкту EU’s «Chat Control», який пропонує сканувати приватні чат користувачів в ЄС. В пояснювальній записці до цього закону, йдеться про нагальну потребу захистити права дітей, котрі стають жертвами різних форм насильства, зокрема сексуального, в мережі (Direction des Affaires Juridiques, 2022). Цей проєкт, активно лобійований урядом Франції, був підданий критиці Європейським центром свободи преси та ЗМІ. У заяві центру : *«передбачений ним механізм дозволить владі зобов'язати постачальників послуг обміну повідомленнями, електронної пошти та хостингу сканувати приватні повідомлення, незалежно від наявності конкретних підозр. Це фактично відкриє шлях для масового спостереження за особистими розмовами та послабить технічний захист, що забезпечує конфіденційність»* (ECPMF, 2025).

Окрім того, 470 дослідників з 34-х європейських країн підримали цю позицію відкритим листом, про необхідність відхилити цей законопроєкт, як такий, що створює загрозу свободі слова, приватності та може призвести до цензури.

Боротьба за контроль над цифровим публічним простором є невід'ємною частиною глобальної конкуренції між різними політичними системами, і успіх демократій у цьому протистоянні залежатиме від їхньої здатності знайти баланс між захистом та збереженням основоположних свобод.

Глобальне дослідження громадської думки показує, що саме відмінності в цьому балансі пояснюють, чому в одних країнах переважає позитивна оцінка, а в інших, зокрема в США, — вкрай негативна. Там, де громадяни відчувають, що інструменти для підвищення інформованості та громадської мобілізації переважують ризики, соціальні мережі сприймаються як чинник, що позитивно впливає на демократичну функціональність. Натомість там, де домінують дезінформація та поляризація, вони перетворюються на загрозу. Американський виняток є свідченням того, що високий рівень внутрішнього політичного конфлікту, помножений на архітектуру платформ, може призвести до майже повного затьмарення їхніх позитивних аспектів. Американський приклад, дозволяє змоделювати, що може відбуватися з інформаційним полем в Європейському Союзу у майбутньому, у випадку відсутності ефективних та зважених політик щодо соціальних мереж, — наростання внутрішніх суперечностей та конфліктів загострюватиме деструктивний вплив соціальних мереж на європейські суспільства, підсилюючи руйнівні тренди в політичному вимірі.

Цей внутрішній виклик ускладнюється зовнішнім, геополітичним виміром, де авторитарні режими використовують вразливості цифрового простору для дестабілізації демократій. Отже, головним завданням для сучасних ліберальних демократій є розробка стійких механізмів — правових, освітніх та технологічних — які б дозволили максимізувати переваги цифрових платформ для

громадянського суспільства, одночасно мінімізуючи їхні руйнівні ризики для політичної стабільності, безпеки та суспільної злагоди.

На початку 2010-х роль соціальних мереж у питаннях безпеки ще не була в центрі уваги ЄС. Основні зусилля зосереджувалися на кібербезпеці та захисті даних користувачів. Однак поширення екстремістських матеріалів в інтернеті та пропаганди з боку іноземних акторів поступово змінювало ландшафт взаємодії між ЄС та компаніями-власницями соціальних мереж. Особливо активно це переформатування стало помітним під час російської агресії в Україні 2014 року, коли соцмережі стали каналом кремлівської дезінформації, та на тлі координованих інформаційних атак та активності терористичних угруповань, які вербували прихильників через онлайн-платформи.

У березні 2015 року політичні лідери ЄС вперше офіційно вказали на необхідність протидіяти ворожим інформаційним кампаніям. Європейська Рада на саміті 19–20 березня 2015 року наголосила на потребі «кинути виклик триваючим дезінформаційним кампаніям Росії» (European Parliamentary Research Service, 2018). Це рішення заклало основу для створення в структурах ЄС спеціальної команди з протидії пропаганді. В тому ж році, у квітні, Європейська Комісія ухвалила «Європейський порядок денний з безпеки 2015–2020», де серед пріоритетів боротьби з тероризмом було згадано й інтернет. Зокрема, Комісія анонсувала запуск платформи співпраці з ІТ-компаніями для протидії терористичній пропаганді в інтернеті та соціальних мережах. Ця ініціатива привела до створення в липні 2015 року Європейської групи інтернет-реферування при Європолі, завданням якої стало виявлення і видалення екстремістського контенту онлайн, а також до ініціювання Форуму ЄС з питань інтернету – майданчика для діалогу між правоохоронцями та великими інтернет-платформами щодо протидії загрозливому контенту (Europol, 2015). Хоча цей документ стосувався передусім ксенофобії та ненависті в мережі, він став важливим прецедентом до практики саморегуляції платформ. Facebook, Twitter, Google та інші компанії добровільно взяли на себе зобов’язання швидше виявляти й блокувати матеріали екстремістського характеру. Ці кроки ще не були

закріплені на законодавчому рівні, проте започаткували модель неформальних домовленостей між владою та соцмережами задля безпеки європейських громадян. Успішні результати його імплементації підтвердили доцільність добровільних зобов'язань і підготували ґрунт для застосування аналогічного підходу вже в питаннях кампаній з дезінформації.

В цілому, 2015 рік став переломним у усвідомленні ЄС соціальних мереж як фактора безпеки. Теракти в Європі (зокрема, напад на редакцію Charlie Hebdo) продемонстрували, як радикальні ідеології поширюються через онлайн-платформи. Паралельно ЄС реагував на інформаційну війну, що розгорнулася на сході Європи. У квітні 2015 року, виконуючи доручення Європейської Ради, Верховний представник ЄС із закордонних справ підготував план дій із стратегічних комунікацій, спрямований на протидію зовнішній дезінформації, передусім з боку Кремля. Уже у вересні 2015 року в структурі Європейської служби зовнішніх дій була створена спеціальна цільова група East StratCom, націлена на виявлення та спростування фейкових повідомлень, а також на проактивне інформування про політику ЄС (European External Action Service [EEAS], 2015). Фактично ця ініціатива стала першою спробою інституційно відповісти на проблему дезінформації. Команда East StratCom започаткувала сайт EUvsDisinfo для публікації прикладів проросійської дезінформації. Попри те, що ця інституція мала обмежені ресурси і носила радше аналітичний та комунікаційний характер, її впровадження відображало усвідомлення: соціальні мережі і онлайн-медіа поступово перетворюються на поле битви за громадську думку та безпеку демократичних суспільств в Європі.

У 2016 році тема впливу соціальних медіа на безпеку набрала ще більшої ваги, значною мірою через зовнішні події. Референдум щодо Brexit у Великій Британії та вибори президента США продемонстрували, як масштабне поширення неправдивих новин та цілеспрямовані кампанії у соцмережах можуть вплинути на результати голосувань в демократичних системах. Розслідування виявили, що частина цього інформаційного впливу координувалася з-за кордону, зокрема російськими тролями та бот-мережами. Вочевидь, для Європейського

Союзу можливість іноземних акторів впливати на думку громадян та виборців створювала комплексну загрозу, найперше підриваючи демократичний процес, який є важливим фундаментом усього європейського об'єднання. Разом із тим, ЄС ще не мав достатніх інструментів, процедур та важелів впливу на цифрове середовище та платформи соціальних мереж.

Восени 2016 року в середині Європейського парламенту було відкрито засвідчено про «ворожу пропаганду» проти ЄС. У листопаді ЄП ухвалив резолюцію щодо стратегічних комунікацій, засудивши дезінформаційний тиск з боку Росії та екстремістських угруповань. Депутати назвали ці явища «наростаючою проблемою», яка призводить до спотворення правди, поширює страх і може розколювати Євросоюз. Парламент закликав посилити спроможності East StratCom Task Force, аби ефективніше викривати неправдиву або вигадану інформацію. Ця резолюція, хоч і декларативна, відобразила політичний консенсус: дезінформація розглядається як загроза європейській безпеці, на яку треба відповісти не контрпропагандою, а правдою, підвищенням обізнаності громадян та зміцненням медіаграмотності (European Parliament [EP], 2016).

Відтак, перші кроки ЄС в напрямку випрацювання безпекових політик щодо соціальних мереж були достатньо м'якими та переважно апелювали до здатності компаній самостійно регулювати небезпечний контент. 2017 рік також суттєво вплинув на вимір європейської цифрової безпеки. Під час виборів президента Франції навесні 2017 відбулася спроба інформаційного втручання – так званий витік «Macron Leaks», коли за кілька днів до голосування на президентських виборах в мережу потрапив масив електронних листів штабу Еммануеля Макрона, перемішаний з неправдивою інформацією, яка стосувалася, наприклад, «офшорних рахунків» Макрона. Хоча французька влада і медіа оперативно попередили суспільство про ймовірну дезінформацію, цей випадок підтвердив реальність загрози (Mohan, 2017).

Німеччина, готуючись до виборів восени 2017, навіть ухвалила національний закон, який зобов'язував соцмережі швидко видаляти

протиправний контент, аби запобігти можливому розпалюванню ненависті та фейкам. Таким чином, зростання випадків загроз, що походять з соціальних мереж та цифрових платформ, поступово обумовлювало необхідність Союзу реагувати активніше та координувати протидію спільними зусиллями держав-членів ЄС. До прикладу, у червні 2017 року Європарламент у резолюції щодо онлайн-платформ закликав Єврокомісію проаналізувати правові межі у протидії «фейковим новинам» та розглянути можливість законодавчих дій для обмеження поширення фальшивого контенту. Президент Європейської Комісії Жан-Клод Юнкер спеціально доручив комісару Марії Габріель дослідити виклики, які створюють онлайн-платформи для демократії, і запропонувати відповідні рішення. Отже, на зламі 2017–2018 років тема маніпуляцій у соціальних мережах вже була однією з важливих тем у безпековому вимірі Євросоюзу (Juncker, 2017).

2018 рік став поворотним у генезі політики ЄС щодо соціальних мереж як безпекового чинника. Першим кроком стало широке залучення експертного середовища та громадськості до вироблення необхідних рішень. У січні 2018 року Єврокомісія створила групу високого рівня із питань фейкових новин та онлайн-дезінформації (HLEG), до якої увійшли представники академічного середовища, медіа, інтернет-компаній та громадянського суспільства. Паралельно було проведено публічні консультації зі зацікавленими сторонами по усьому ЄС. Результатом став звіт HLEG із рекомендаціями, який ліг в основу подальших дій Комісії. 26 квітня 2018 року Єврокомісія оприлюднила документ з назвою «Протидія онлайн-дезінформації: європейський підхід». У цьому стратегічному документі вперше на рівні ЄС було комплексно окреслено проблему дезінформації як загрозу демократичному ладу та безпеці. Комісія визначила низку заходів, направлених на протидію, зокрема:

- **Саморегуляція платформ:** було запропоновано розробити Кодекс практик щодо дезінформації – добровільний набір зобов’язань для соціальних мереж та онлайн-платформ, покликаний забезпечити прозорість алгоритмів (особливо відносно відбору новинного контенту),

видалення фейкових акаунтів, маркування ботів, обмеження реклами на фейкових сайтах тощо.

- **Підтримка «фактчекерів» та достовірних ЗМІ:** передбачалося створити незалежну європейську мережу організацій, що перевіряють факти, та вжити заходів для підвищення якості журналістики.
- **Медіаграмотність:** рекомендувалися просвітницькі кампанії для громадян, щоб ті могли краще розпізнавати неправдиву інформацію (European Commission, 2018).

Підсумовуючи, варто відзначити, що попри поступове наростання небезпек, викликаних соціальними мережами, домінантним лишався принцип: платформи соціальних мереж мають самостійно контролювати інформаційний потік. Причини зволікання в середині ЄС у встановленні прозорих правил та обмежень для соціальних мереж можливо лише припускати. Ймовірно, застосування обмежень в мережі могли бути сприйняті європейськими громадянами як обмеження фундаментальних принципів, на яких заснований ЄС, особливо чутливим постало би питання свободи слова та свободи вираження. Проте в травні 2018 року відомими стали масштабні факти маніпуляцій з користувачами соціальних мереж з допомогою Cambridge Analytica – з'ясувалося, що дані мільйонів користувачів Facebook були незаконно використані для націлювання політичної реклами, що впливало на виборчий процес.

Втручання в електоральні процеси призвело до посилення контролю за приватністю – було застосовано новий регламент GDPR, а на політичному рівні значно зросла підтримка ідеї, що саморегуляції від платформ може бути недостатньо. Також Європарламент викликав Марка Цукерберга на слухання, де євродепутати вимагали пояснень щодо втручання у вибори та неналежного захисту даних користувачів (Rankin, 2018). Цей випадок став демонстрацією того, що ЄС очікує від соцмереж відповідальності за безпекові наслідки впливу їхніх сервісів на європейські суспільства, і якщо добровільні заходи не спрацюють, ЄС може застосувати законодавче втручання, обмеження та регуляцію.

Варто відзначити, що активізація питань безпеки даних та загроз, що походять від соціальних мереж, найінтенсивніше розпочиналися в ЄС здебільшого у контексті виборів. Європейські політики того ж року, готуючись до майбутніх виборів у Європарламент, закликали європейські інституції до захисту демократичного процесу та боротьби з проявами дезінформації. Відповідаючи на цей заклик, Єврокомісія спільно з Верховним представником ЄС у зовнішніх справах вже у грудні підготували всеосяжний План дій проти дезінформації (European Commission 2018). План передбачав швидке впровадження запропонованих кроків, для того щоб забезпечити прозорість та легітимність наступних виборів. Цей План передбачав скоординовану реакцію на рівні ЄС і держав-членів у чотирьох ключових напрямках:

- **Покращення виявлення загроз:** збільшення фінансування і штату груп стратегічних комунікацій (зокрема East StratCom) та створення в структурі ЄС спільної Гібридної аналітичної групи для обміну даними про інформаційні атаки.
- **Координація реагування:** заснування системи швидкого оповіщення між інституціями ЄС і країнами-членами для негайного обміну інформацією про дезінформаційні кампанії та гібридні загрози.
- **Залучення онлайн-платформ та індустрії:** імплементація Кодексу практик. Провідні платформи (Facebook, Google, Twitter та ін.) підписали цей Кодекс, взявши на себе зобов’язання щодо прозорості реклами, закриття фейкових акаунтів, співпраці з фактчекерами тощо.
- **Просвіта та підвищення стійкості суспільства:** проведення кампаній з медіаграмотності, підтримка національних команд незалежних фактчекерів у державах ЄС для викриття фейків на платформах.

Таким чином, в ЄС поступово почала формуватися комплексна стратегія протидії загрозам, що походять із соціальних мереж. Від переважно добровільних і розрізнених заходів ЄС перейшов до більш скоординованого підходу, визнавши соцмережі критично важливим полем забезпечення інформаційної та виборчої безпеки.

Основним викликом 2019 року були вибори до Європарламенту, що відбулися у травні. ЄС прагнув не допустити повторення сценаріїв зовнішнього втручання, тому заходи, накреслені в Плані дій, втілювалися прискореними темпами. На початку 2019-го запрацювала Система швидкого оповіщення – канал обміну інформацією між брюссельськими інституціями та столицями держав-членів для повідомлень про дезінформаційні атаки в реальному часі. У тісній координації діяли також оперативні штаби з кібербезпеки та охорони виборчого процесу, адже кібератаки на виборчу інфраструктуру часто йдуть поряд з кампаніями у соцмережах. Онлайн-платформи під тиском ЄС звітували про виконання взятих зобов'язань (MediaSapiens, 2019).

У передвиборчі місяці Facebook, Twitter, Google та інші компанії регулярно подавали Єврокомісії звіти про заходи: вони видаляли мільйони фейкових акаунтів, впроваджували інструменти прозорості для політичної реклами, помічали ботів спеціальними мітками тощо. Була запущена база даних політичної реклами (наприклад, у Facebook), де користувачі могли побачити, хто фінансує ту чи іншу агітацію. Також платформи розширили співпрацю з фактчекерами в різних країнах ЄС, щоб спростовані фейкові новини ставали менш видимими.

В результаті вибори в Європарламент 2019 відбулися без масштабних інцидентів втручання. Незалежні дослідження та звіти EUvsDisinfo зафіксували спроби поширення фейків проросійського походження (зокрема, піднімалися теми міграції, скепсису щодо ЄС), але скоординованої кампанії, здатної суттєво вплинути на результати виборів, не спостерігалося. Єврокомісія заявила, що спільні зусилля з технологічними компаніями дали змогу уникнути серйозної дестабілізації виборів, хоча загроза нікуди не зникла і потрібні нові довгострокові рішення.

Згодом Європейська Комісія на чолі з Урсулою фон дер Ляєн у своїх програмних заявах обіцяла створити Європейський план дій для демократії, а також переглянути правила функціонування цифрових платформ (що вилилося у підготовку Акту про цифрові послуги) (European Commission, 2020a). Це

означало, що напрацювання Європейського Союзу у безпековому секторі будуть поглиблюватись – через нові політики, які зроблять соцмережі відповідальнішими перед законом.

2020 року ЄС перейшов від переважно добровільних підходів до розробки нормативних механізмів регулювання діяльності соціальних мереж. На порядку денному залишалися питання дезінформації та інформаційного втручання, але додався новий масштабний виклик – інфодемія, пов'язана з COVID-19 (European Commission, 2020). Пандемія коронавірусу супроводжувалася вибухом неправдивої інформації в соцмережах щодо вірусу, лікування, вакцин тощо, що становило пряму загрозу громадському здоров'ю. ЄС розцінив цілеспрямоване поширення фейків про COVID-19 як питання, дотичне безпосередньо до безпеки європейських громадян, і заявив про участь іноземних гравців у цих кампаніях. Єврокомісія та Європейська служба зовнішніх дій опублікували спільну доповідь щодо дезінформації про пандемію, закликавши онлайн-платформи посилити модерацію шкідливого контенту та регулярно звітувати про вжиті заходи. Вперше компаніям довелося щомісяця надавати ЄС детальні дані про видалені фейки, кількість перенаправлень до достовірних джерел тощо. Ця ініціатива продемонструвала, що ЄС може вимагати прозорості й фактично виконувати роль наглядового органу навіть без формального закону, коли ситуація є надзвичайною і становить значну загрозу для безпеки усього ЄС.

Наприкінці 2020 року Єврокомісія представила два стратегічно важливі документи, які заклали основу довгострокової політики: Європейський план дій для демократії (EDAP) і пакет законодавчих пропозицій щодо цифрових послуг. Європейський план дій для демократії передбачав заходи для зміцнення стійкості демократії, в тому числі боротьбу з дезінформацією та інформаційним втручанням (European Commision, 2020). План анонсував підготовку законодавства про прозорість політичної реклами онлайн та посилення Кодексу практик щодо дезінформації – перетворення його з добровільного інструмента на щось на кшталт співрегулювання (коли під наглядом регулятора виконання кодексу стає обов'язковим для найбільших платформ). Цей документ також

наголосив на необхідності зберегти баланс: боротися з інформаційними загрозами, одночасно захищаючи свободу слова. Тут важливою є генеза поступової трансформації відповідальності соціальних мереж – від саморегуляції та добровільності до подальшого визнання факту, що ЄС має здійснювати певний контроль над соціальними мережами, визначаючи межі, в яких свобода не тотожна безконтрольності та анархії.

Найважливішою законодавчою ініціативою став проєкт Акту про цифрові послуги (DSA), який Комісія внесла у грудні 2020 року. Проєкт DSA – це масштабна реформа правил для онлайн-платформ, що покликана «запобігати незаконній та шкідливій діяльності онлайн і стримувати поширення дезінформації». З точки зору безпеки, DSA мав ввести для великих соцмереж (із аудиторією понад 45 млн користувачів в ЄС) обов'язки регулярно оцінювати системні ризики від їхніх сервісів – у тому числі ризики для громадської безпеки, демократичного дискурсу та здоров'я громадян, пов'язані з дезінформацією чи маніпуляціями. Платформи мають впроваджувати заходи для зменшення цих ризиків, під загрозою санкцій з боку ЄС. Крім того, DSA мав би зобов'язати всі онлайн-платформи оперативно видаляти незаконний контент після отримання повідомлення, а також підвищити прозорість алгоритмів і реклами. Попри те, що цей акт ще вимагав узгодження з Європарламентом і Радою, ця ініціатива означала, що ЄС готовий закріпити відповідальність соцмереж на рівні закону, виходячи із уроків попередніх криз (European Commission, 2020).

Варто зауважити, що у січні 2021 відбулася подія у США, яка також вплинула на європейські дебати – штурм Капітолію прихильниками теорій змови, організований значною мірою через соціальні платформи. Після цих подій великі компанії заблокували акаунти Дональда Трампа за підбурювання до насильства. Європейські лідери, з одного боку, схвалили протидію онлайн-екстремізму, а з іншого – висловили занепокоєння тим, що такі рішення приймаються приватними компаніями без чіткої правової основи. Цей випадок підкреслив, що соцмережі стали настільки впливовими, що їхня політика модерації має

стратегічне значення для суспільної безпеки, тож Союз повинен встановити демократичний контроль над цим процесом.

У 2021–2022 роках Євросоюз завершив розробку ключових регуляторних заходів щодо онлайн-платформ, одночасно зіткнувшись з новими викликами – передусім, повномасштабною війною в Україні, де соціальні мережі стали фронтом інформаційного протиборства. У квітні 2021 після тривалих переговорів було ухвалено Регламент (ЄС) 2021/784 про протидію поширенню терористичного контенту онлайн. Він набув чинності з червня 2022 року, запровадивши для інтернет-платформ обов'язкові правила: якщо уповноважений національний орган виявляє на платформі контент, що містить терористичну пропаганду або заклики до насильства, платформа має видалити його протягом 1-ї години з моменту отримання припису. Також компанії повинні були запровадити проактивні заходи проти такого контенту (наприклад, фільтри, позначення підозрілої активності), у зворотному випадку пропонувалося застосовувати штрафні санкції (Regulation 2021/784, 2021). Цей регламент став першим обов'язковим законом ЄС, адресованим безпосередньо діяльності соцмереж у сфері контенту, та зафіксував можливість покарання для тих платформ, які уникають приписів Європейського Союзу. В той же час Єврокомісія працювала над удосконаленням вже наявних кодексів. У червні 2022 року було презентовано оновлений Кодекс практик з дезінформації, підписаний ширшим колом учасників (до попередніх платформ долучилися нові, як-от TikTok, Twitch, Microsoft та ін.)

Оновлений кодекс містив 44 зобов'язання і 128 конкретних заходів, серед яких – декларування політики проти маніпулятивних поведінкових практик, обмеження фінансових стимулів для розповсюджувачів фейків (йшлося насамперед про прибутки від реклами), покращення співпраці з незалежними журналістами у всіх країнах ЄС та створення прозорої бібліотеки політичної реклами (Pingen, 2022). Важливим стало те, що невиконання найбільшими платформами своїх обіцянок за кодексом може тягти за собою конкретні санкції у вигляді грошових стягнень. Таким чином, саморегуляція еволюціонувала у

форму спільного регулювання, в якій індустрія сама пропонує стандарти, але ЄС наполягає на їх обов'язковому дотриманні в інтересах суспільства та забезпечення його безпеки.

Детальна розробка нових планів європейської цифрової безпеки додатково активізувалася через нові геополітичні кризи. 24 лютого 2022 року Росія розпочала повномасштабну агресію проти України, що супроводжувалася небаченою хвилею дезінформації та пропаганди, в тому числі в соцмережах. Європейський Союз оперативно відреагував не лише економічними санкціями, а й інформаційними обмеженнями. Вже на початку березня 2022 ЄС ухвалив безпрецедентне рішення заборонити мовлення російських державних каналів RT (Russia Today) і Sputnik на території Союзу. Це означало, що операторам зв'язку та онлайн-платформам в ЄС наказано припинити будь-яку трансляцію чи поширення контенту, пов'язаного з RT і Sputnik (Reuters, 2022).

Вперше регуляторний акт ЄС прямо зобов'язав соціальні мережі та відеоплатформи блокувати сторінки і пости цих пропагандистських ресурсів. У заяві щодо цього рішення. Великі IT-компанії одразу виконали цю вимогу: Meta (Facebook), Google (YouTube), TikTok, Twitter та інші оголосили про блокування акаунтів RT і Sputnik у всіх країнах ЄС. Цей крок виразно показав, наскільки серйозним безпековим фактором стали соціальні мережі: в умовах війни ЄС вперше вдався до інформаційних санкцій, фактично відкривши новий фронт – боротьбу з ворожою пропагандою в цифровому просторі.

Протягом війни 2022 року та надалі ЄС активно підтримує ініціативи з протидії дезінформації про війну, координує роботу зі стратегічних комунікацій з НАТО і країнами G7, а також фінансує дослідницькі центри, що займаються відстеженням фейків. Водночас тема російських фейків щодо енергетичної кризи, санкцій, міграції постійно лишається на порядку денному робочих груп ЄС з гібридних загроз. В цілому, можна стверджувати, що безпекова політика ЄС щодо соцмереж перейшла від реагування на окремі кризи до статусу постійної діяльності, інтегрованої в оборонні і зовнішньополітичні стратегії Союзу.

Глобальний характер загроз, які походять з соціальних мереж, та конфлікт між демократичними та авторитарними системами відобразився на викликах, які постали перед Європейською унією. Соціальні мережі неодноразово протягом останнього десятиріччя були джерелом нестабільності для Європейського Союзу: хвилі дезінформації, втручання у вибори (показова ситуація з президентськими виборами в Румунії і раптовим успіхом кандидата-аутсайдера Келіна Джорджеску), інформаційні атаки на європейські уряди та окремі політичні сили, витоки конфіденційної інформації та персональних даних громадян, маніпуляції суспільною думкою та відкрите застосування соціальних мереж як зброї під час широкомасштабної війни в Європі обумовили появу деталізованих та системних рішень та перегляд вже існуючих стратегічних документів (Гончар, 2025).

Так, вже протягом 2021-го року тривали переговори між державами-членами та Європарламентом щодо Акту про цифрові послуги, проєкт якого був згаданий раніше. В результаті у 2022 році документ був остаточно ухвалений. Digital Services Act офіційно набув статусу регламенту ЄС влітку 2022, а його основні вимоги почали застосовуватися з серпня 2023 року. DSA закріпив на законодавчому рівні багато положень, що раніше були добровільними: наприклад, вимоги прозорості реклами і алгоритмів, процедури швидкого видалення протизаконного контенту, обов’язковий аналіз ризиків дезінформації та надання даних дослідникам. Фактично, боротьба з дезінформацією стала юридичним обов’язком великих соцмереж у рамках підтримання *«безпечного, передбачуваного онлайн-середовища»* для користувачів (European Commission, 2024). Європейська комісія отримала повноваження наглядати за виконанням DSA і навіть проводити аудити алгоритмів. Це безпрецедентний крок, який демонструє еволюцію підходу: від апелювання до «доброї волі» платформ ЄС перейшов до прямих регуляторних вимог, мотивованих необхідністю захисту суспільної безпеки і демократичних систем у Європі.

З політичної перспективи цей документ відображає складний баланс між наднаціональними (європейськими) стандартами та національними інтересами

держав-членів. Він демонструє, що цифровий простір стає ареною, де вирішуються питання не лише безпеки громадян, але й стратегічної безпеки держав, захисту суверенітету, боротьби з дезінформацією та захисту прав людини. Звіти, присвячені впровадженню DSA, демонструють складності на шляху до оформлення спільних європейських правил в цифровому середовищі. У звіті за 2025 рік продемонстровано, що в деяких державах-членах ЄС, таких як Бельгія, Фінляндія та Франція, для забезпечення виконання DSA було створено множинність державних органів, залучених до регулювання, що призводить до неефективності їх роботи. В деяких країнах, наприклад у Фінляндії, три окремі органи поділяють повноваження у сфері контролю за виконанням DSA, що потребує високого ступеня взаємодії між ними (Library of Congress, 2025). Узагальнюючи, можна вивести загальні перешкоди до впровадження принципів, на яких заснований DSA:

- **Неготовність національного законодавства.** Деякі держави-члени ЄС ще не повністю впровадили необхідні національні акти в підтримку DSA. Наприклад, Нідерланди лише перебувають на етапі обговорення свого законопроєкту, що створює невизначеність щодо ефективності застосування регламенту на території країни.
- **Розбіжності між країнами ЄС у визначенні санкцій та їх розмірів за порушення DSA.** Наприклад, максимальні штрафні санкції варіюються в межах до 6% річного глобального обороту компаній (Австрія, Франція, Швеція) до фіксованих адміністративних штрафів (Німеччина – до 300,000 євро, Болгарія – 25,000 євро).
- **Збереження можливості фрагментації** у виробленні спільних європейських політик та реакції на цифрові загрози (Digital Services Act Implementation in Selected EU Member States, 2025).

Для того щоб оцінити увесь комплекс заходів, які здійснюються в середині ЄС для випрацювання засад, на яких соціальні мережі складають важливу частину безпекового сектору, важливо звернути увагу на тенденції в середині самих держав-учасниць Союзу. Попри спробу упровадити узагальнену рамку

європейської безпекової політики, на рівні національних урядів можна віднайти суттві відмінності та особливості у функціонуванні безпекових політик щодо соціальних мереж. У відповідь на зростання рівня цифрових загроз держави ЄС пройшли свій шлях до визначення соціальних платформ як загрози (а подекуди й інструменту) для нацбезпеки, ухваливши низку власних законів і стратегій. Діяльність національних урядів демонструє, що єдиного підходу до питань безпеки у європейському мережевому просторі наразі не існує. Показовий приклад – Федеративна республіка Німеччина.

Німецький підхід відзначається жорстким примусом до виконання існуючих законів у цифровому середовищі. Девізом німецької політики стало гасло: «що незаконно офлайн – незаконно онлайн». Політика Німеччини була однією з перших в ЄС, що на законодавчому рівні містила реакцію на виклики, спричинені соцмережами. Ще у 2015 році Міністерство юстиції ФРН створило робочу групу для аналізу контенту в соцмережах. Причиною були випадки стрімкого поширення онлайн-ненависті та проросійської дезінформації і як наслідок – стихійних акцій протесту, цей випадок детально проілюстрований в звіті «The Lisa Case: STRATCOM Lessons for European states» («інцидент Лізи», під час якого російські медіа роздмухали сфальшовану історію про зґвалтування дівчинки в Берліні) (Janda, 2016). Добровільні зусилля самих платформ виявилися недостатніми: наприклад, моніторинг 2017 р. показав, що Facebook видаляв лише ~39% протиправного контенту, Twitter – 1%, тоді як YouTube – 90%. Це переконало уряд, що потрібне юридичне зобов'язання компаній видаляти небезпечний контент. Міністр юстиції Гайко Маас прямо заявив: «Необхідно посилити тиск на соцмережі» (Європейська правда, 2017).

Окремим законом 2020 р. влада зобов'язала соцмережі передавати особливо небезпечні повідомлення прямо до правоохоронців. Йдеться про контент, що містить погрози, підтримку та схвалення злочинів, матеріали екстремістських організацій тощо – такі публікації мають надсилатися платформою в Федеральне відомство кримінальної поліції з особистими даними автора. Це зробило Німеччину піонером регулювання соцмереж серед

демократій, і нині вона має одну з найсуворіших моделей контролю платформ у світі.

Про серйозність уряду до питань безпеки в соціальних мережах свідчить розробка комплексу законів, котрі значно обмежують технологічні компанії. Згаданий раніше закон NetzDG (Закон про забезпечення правового порядку в соціальних мережах) був ухвалений в 2017-му році. Уведенням в дію цього закону Бундестаг став одним з перших у світі законодавчих органів, який розпочав практику жорсткого регулювання цього сектору. Закон зобов'язав великі соціальні платформи (понад 2 млн користувачів) швидко видаляти незаконний контент – «очевидно протиправний» за 24 години, інший – до 7 днів після перевірки (Tworek, 2019).

Під заборону потрапив широкий спектр матеріалів, визначених у Кримінальному кодексі ФРН, серед яких розпалювання ненависті, нацистська пропаганда, заклики до насильства, терористичний контент, наклеп тощо. Платформи були зобов'язані запровадити прозорі процедури розгляду скарг, інформувати користувачів про рішення щодо їхніх скарг та зберігати вилучений контент як можливий доказ. Також закон поставив вимогу представництва технологічної компанії, що володіє мережею, в Німеччині. Це, в свою чергу, призводило до необхідності взаємодії між державою та компанією і додатково контролювалося звітами про модерацію контенту, котрі мають публікуватися регулярно. Закон також встановлював значну відповідальність, передбачаючи фінансові стягнення з компаній (Опришко, 2021).

Згодом закон був додатково посилений: платформи зобов'язані покращити прозорість звітів (розкривати, зокрема, використання алгоритмів автоматичного виявлення забороненого контенту та на яких даних вони навчаються), запровадити для користувачів механізм оскарження видалення/невидалення контенту, а також підпорядкуватися розширеному нагляду Федерального відомства юстиції. Окрім того, німецький уряд вийшов за межі соціальних мереж і додатково включив до сфери дії NetzDG також відеоплатформи (YouTube).

Законопроєкт NetzDG спричинив палкі дискусії у Бундестазі та німецькому суспільстві. Урядові партії (ХДС/ХСС та СДПН) підтримали ініціативу, наголошуючи, що «інтернет формує культуру дебатів і загальний суспільний клімат», а хвиля ненависті та фейків онлайн може радикалізувати громадян. Німецькі урядовці аргументували необхідність жорсткого регулювання тим, що держава мусить захистити громадян від ворожнечі і наклепів у мережі, які підривають єдність та безпеку, особливо після наростання дезінформації навколо кризи біженців 2015–2016 рр. та інформаційних втручань Кремля. Опоненти з різних політичних таборів критикували NetzDG за спроби запровадження «цензури», а правозахисники, журналістські об'єднання і навіть ООН висловили занепокоєння, що закон спричинить невмотивоване видалення контенту і придушення свободи слова (Kaye, 2017). Значні зауваження викликало і те, що закон напряму не розкривав суті понять «фейкові новини» чи «мова ненависті», а натомість відсилав до списку з 23 злочинів, зазначених в Кримінальному кодексі. Серед цих норм, зокрема, вміщені положення «про наклеп на президента, державу та її символи» (Human Rights Watch, 2018).

Від опозиційних сил в Бундестазі лунали застереження, що уряд фактично перекладає на приватні корпорації функцію цензора, і ті будуть готові видаляти будь-який контент, аби уникнути штрафів – це називали ризиком надмірного блокування інформації. Загалом дискусії в Німеччині відображали непростий пошук балансу між захистом демократії від інформаційних атак та збереженням фундаментальних свобод і основоположних принципів ЄС. Метою німецьких ініціатив передусім можна вважати забезпечення верховенства закону навіть у цифровому просторі та захист суспільства від шкідливого контенту. NetzDG прямо спрямований на регулювання соцмереж – примусити їх оперативно реагувати на протиправний контент, тим самим нейтралізуючи загрози на ранніх стадіях.

Таким чином, німецькі закони можна розглядати як превентивний засіб проти дезінформації, так і каральний/стримуючий інструмент. В цілому, логіка німецьких ініціатив була радше реактивною – вони з'явилися у відповідь на

конкретні виклики соціального напруження, котрі пов’язані із соціальними мережами.

Інший підхід до безпеки та соціальних мереж продемонструвала Франція, де тема соцмереж і нацбезпеки актуалізувалася у контексті виборчого процесу. Під час президентських виборів штаб Емануеля Макрона зазнав інформаційних атак та витоку даних, тому вже в січні 2018-го Макрон назвав фальшиві новини в соцмережах «загрозою для ліберальних демократій» і прямо звинуватив російські державні канали у спробах втрутитися в французькі вибори через мережі. Він оголосив, що Франція підготує спеціальний закон проти дезінформації під час виборів. Таким чином, для Франції шлях до регулювання соцмереж визначив чинник захисту виборчої демократії від зовнішніх інформаційних маніпуляцій (Reuters, 2018).

Влітку 2018 року у Франції було ухвалено так званий «закон проти маніпуляції інформацією», що вводить заходи тільки на період виборчих кампаній (Young, 2018). Протягом трьох місяців до виборів великі онлайн-платформи повинні дотримуватися підвищених стандартів прозорості – розкривати, хто оплачує політичну рекламу/контент, скільки за цю рекламу було сплачено, і як використовується персоналізація даних користувачів для просування політичної реклами. Таким чином, наголос, в першу чергу, робиться на прозорості алгоритмів та реклами, аби користувачі та влада бачили джерела інформаційного впливу. Крім того, закон давав право кандидатам або уряду звернутися до суду для блокування поширення завідомо фейкової інформації під час виборів. Суддя мав розглянути звернення за прискореною процедурою (протягом 48 годин) і мав можливість постановити видалити контент, закрити акаунт чи навіть заблокувати доступ до сайту, якщо будуть докази, що такий контент є вигаданим і спрямованим на підрив голосування.

Окремо було розширено повноваження аудіовізуального регулятора CSA, якому дозволили призупиняти трансляцію іноземних державних ЗМІ на території Франції під час виборів, якщо ті навмисно поширюють дезінформацію. Практично це положення націлене на пропагандистські канали на кшталт Russia

Today. Разом із цим, французький уряд провадив спроби розробити законодавчу базу, яка дозволила би ефективно протидіяти інформації, що може загрожувати національній безпеці. У 2020 р. парламент ухвалив окремий закон Avia (за ім'ям депутатки-ініціаторки Летісії Авіа), який вимагав від онлайн-платформ видаляти «очевидно протиправні» публікації протягом 24-х годин, а терористичну пропаганду – за 1-ну годину після повідомлення. Однак Конституційна рада Франції визнала більшість положень запропонованого закону неконституційними, заявивши, що такі суворі вимоги непропорційно обмежують свободу слова в країні (Conseil Constitutionnel, 2020). Цей закон, вочевидь, був навіть жорсткішим за німецький NetzDG у плані строків видалення інформації.

Фактично французький суд заблокував основні норми, залишивши лише зобов'язання платформ розташовувати відповідні інтерфейси для скарг і надсилати звіти, але без жорстких часових обмежень щодо видалення. Таке обмежене застосування механізмів контролю показало межі французького національного регулювання соціальних мереж перед усталеною традицією дотримання свободи слова та преси. Пізніше Франція почала більше покладатися на доступні загальноєвропейські інструменти: активно підтримала Регламент ЄС про терористичний контент онлайн, який встановив ті ж вимоги видалення за 1 годину по всьому ЄС, але вже на основі єдиного європейського закону.

Інший аспект – підготовка спеціальних інституцій, котрі здатні протидіяти загрозам, що виникають в соцмережах. У 2021 році Франція створила спеціальне агентство Viginum (під егідою Національного секретаріату оборони і безпеки, SGDSN), завдання якого – виявляти і нейтралізувати іноземні цифрові впливи у французькому інформаційному просторі, передусім у соцмережах (VIGINUM, 2025). Viginum здійснює моніторинг соцмереж на предмет координованих інформаційних кампаній, публічно викриває їх і інформує уряд. Це скоріше оперативний, а не законодавчий крок, але він демонструє, що уряд Франції розглядає маніпуляції у соцмережах як питання національної безпеки, яким повинні займатися спецслужби та урядові органи.

Відповідно, французьке регулювання соцмереж фокусується на:

1. **Захисті виборів від дезінформації** (прозорість політичної реклами, судове блокування фейків).
2. **Боротьбі з мовою ворожнечі і тероризмом онлайн** (спроби зобов'язати швидке видалення, зараз більше через норми ЄС).
3. **Протидії іноземному інформаційному впливу** (моніторинг і можливість обмежувати пропагандистів) (VIGINUM, 2025).

Франція вирізняється тим, що виокремила дезінформацію в окрему категорію загроз саме в контексті виборів. Якщо німецький NetzDG універсальний, то французький «закон про фейкові новини» діє тільки під час передвиборчої кампанії, коли держава особливо пильнує за інформаційним полем. При цьому Франція зробила ставку на судову владу як арбітра справедливості, адже саме суд за запитом кандидата чи прокуратури вирішує, чи інформація є фейком, і чи необхідно здійснювати її блокування чи обмеження. Ця модель покликана уникнути звинувачень у цензурі з боку уряду – весь процес відбувається через незалежний судовий розгляд, а не з ініціативи політичної влади, котра може бути ангажована у своїх рішеннях.

Водночас французька влада прямо вказала на джерело загрози – іноземні державні медіа – і надала регулятору можливість зупинки їх діяльності. Це специфічний крок, якого інші країни ЄС у своїх безпекових політиках уникали. Фактично було визнано, що певні закордонні інформаційні канали є інструментами ворожих впливів, отже їх можна обмежити, керуючись потребами національної безпеки. Французький уряд, вочевидь, прагнув стати «взірцем» і задати високий стандарт боротьби з небезпечним контентом, навіть якщо це потребувало перейти поширені європейські рамки (VIGINUM, 2025).

Така проактивна позиція Франції свідчить не лише про занепокоєність питаннями загроз, що надходять від соціальних мереж, але і про певну конкуренцію безпекових підходів в середині Європейського Союзу. З заяв французьких політиків стає зрозумілим, що французьке національне законодавство могло розглядатися ними як фактична основа для загальноєвропейської організації безпеки в соціальних мережах (Kayali, 2020).

Таким чином, лідерство в питанні боротьби з інформаційними загрозами та регулюванням соцмереж є також елементом престижу конкретної держави – воно дозволяє поширювати власні «моделі» на весь Європейський Союз, впливаючи на рішення, політики та стратегії усього об'єднання. Окрім того, для Франції проблематика соцмереж – це питання внутрішньої єдності та громадського порядку, наприклад, масові протести «жовтих жилетів», наприклад, координувалися з допомогою соціальних мереж (Нуарьєль, 2018) і водночас елемент геополітичного протистояння (захист демократії від гібридних атак Кремля, просування французького наративу за кордоном).

Під час обговорення «анти-фейкового» закону ліві і праві депутати об'єдналися в критиці, називаючи його «поспішним і неефективним», а декотрі – навіть небезпечним прецедентом цензури. Лідер лівопопулістів Меланшон відстоював тезу, що заборони Russia Today і Sputnik є політично вмотивованими (Mélenchon, 2018). Попри критику, урядова партія «Вперед, Республіко!», маючи більшість, провела закон через Національну асамблею. Сенат же спершу відкинув ці ініціативи, навіть відмовившись розглядати їх по суті у липні 2018, мотивуючи це сумнівами в ефективності та ризиками для свободи слова. Врешті, після доопрацювання, закон набув чинності перед європейськими виборами 2019 року. Навколо «закону Авіа» тривали гострі дебати (Bryant, 2019). Його підтримав уряд як необхідний засіб проти онлайн-ненависті. Однак опоненти – від правих до Лівої партії – визначали цей закон як надмірний. Технологічні компанії і правозахисні організації тиснули, аргументуючи, що такий закон суперечить директивам ЄС і ставить непропорційні вимоги. Зрештою, свою крапку поставила Конституційна рада, яка майже одностайно підтримала аргументи про непропорційність обмежень свободи вираження. Судді зазначили, що вимога видаляти контент без рішення суду за 1 день фактично перекладає на приватні компанії функцію цензурування публічної сфери, що неприпустимо в демократичному суспільстві (Conseil Constitutionnel, 2020).

Отже, французькі політичні дискусії точилися навколо дилеми – як протидіяти дезінформації в мережі, не давши владі надмірних цензурних повноважень.

Метою кроків французьких законодавців та політиків було захистити національний інформаційний суверенітет і демократичний процес. Це законодавство тісно пов'язане із захистом демократії від зовнішніх атак та штучних криз. Одночасно закон слугує для забезпечення внутрішньої гігієни інформаційного поля – аби вибори відбувалися в умовах чесних дебатів, без засилля фабрикованих скандалів. Мета законів щодо шкідливого контенту – захист громадян від проявів екстремізму онлайн і убезпечення суспільства від наслідків радикалізації (терактів, насильства на ґрунті ненависті тощо). Франція також прагнула просувати власні цінності та стати флагманом регулювання інтернету на засадах демократичної відповідальності, можливо зміцнити свій вплив у формуванні європейської безпекової політики в цифровому просторі.

Франція, попри всю риторику про загрози, активно використовує соцмережі у своїх інтересах (Ministry for Europe and Foreign Affairs, 2018). Урядові структури давно присутні в соцмережах, адже ще з 2009 року МЗС Франції стало провідною інституцією у соцмережах серед держустанов держави. Сьогодні французьке МЗС веде акаунти в Twitter кількома мовами (англійською, іспанською, арабською, німецькою, російською), щоб доносити позицію Франції різним аудиторіям. Вони прямо називають Twitter «безцінним інструментом комунікації під час кризи». Це означає, що держава бачить в соцмережах канал для оперативного зв'язку з населенням і світом, наприклад, під час надзвичайних ситуацій. Так само уряд активно веде Facebook-сторінки для діалогу з населенням, роз'яснення політики, спростування чуток (показовим був період пандемії COVID-19, коли офіційні сторінки МОЗ Франції постійно публікували оновлення і розвінчували міфи про вакцини). Отже, Франція розглядає соцмережі не лише як щось, що треба регулювати чи обмежувати, а й як потужний інструмент цифрової державної комунікації. Більше того, вона свідомо використовує соцмережі в інформаційній політиці на зовнішній арені, в якій багатомовні акаунти – це елемент публічної дипломатії, формування контрнаративів (зокрема, франкомовний і англомовний контент проти російських тез, робота з аудиторією Африки, де Франція конкурує з Китаєм/Росією в

інформаційному просторі). Таким чином, французький досвід показує двоєдину стратегію – оборонну (фільтрувати загрози в соцмережах) і наступальну (використовувати соцмережі для просування своїх цінностей і інтересів).

Особливий шлях у формуванні власної безпекової стратегії в соціальних мережах пройшли країни Балтії. Соціальні мережі опинилися на передовій російської інформаційної війни вже в 2007 році, коли Естонія зазнала масованої кібератаки і пропагандистської кампанії в інтернеті з боку Росії (під час «війни пам'ятників»), що було одним з перших прикладів гібридної атаки в Європі (Європейська правда, 2022). Після цього, а особливо після подій 2014 року в Україні, естонський уряд усвідомив, що дезінформація – це реальна загроза нацбезпеці, частина ширшої гібридної агресії. Проте шлях у зебезпеченні безпечерно середовища в мережі та соцмедіа Естонії відрізнявся від західноєвропейського. Країна пішла шляхом стратегічної підготовки та суспільної просвіти. Естонська конституція дуже високо цінує свободу слова, тому уряд уникав давати юридичні визначення «фейків» чи вводити цензурні норми. Як зазначено в дослідженні «Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016–2020», Естонія «не має легального визначення дезінформації чи фейкових новин, але має робоче (оперативне) визначення, узгоджене з підходом ЄС», – це «хибна або оманлива інформація, створена і поширена навмисно задля політичної, економічної або особистої вигоди» (McBrien, 2020).

Відсутність законодавчих новацій естонська влада компенсувала організаційними: наприклад, до 2016–2017 роках при уряді Естонії сформували невелику групу стратегічних комунікацій, яка аналізувала інформаційне середовище (включно з соцмережами) і розробляла методи протидії ворожим кампаніям. Особливість естонської виборчої системи обумовила, що їхні електронні вибори і прозора демократія можуть стати мішенню для атак з боку іноземних акторів. Тому Естонія визначила, що соцмережі, по своїй суті, можуть перетворюватись на «поле бою», але заборони та обмеження не призведуть до бажаних результатів з точки зору національної безпеки країни. Характерно, що

жодного окремого «закону про соцмережі» Естонія не приймала. Формально там діють загальні європейські та національні норми, які можуть бути застосовані й до онлайн-діяльності. Наприклад, якщо хтось у соцмережах закликає до насильства чи заворушень, його можуть притягнути за статтями про хуліганство або про загрозу громадському порядку – такі положення є у законах усіх балтійських країн (McBrien, 2020).

Основний наголос естонського підходу – на медіаграмотності власних громадян та міжвідомчій координації. Естонія вклала зусилля у просвіту населення, залучивши школи, бібліотеки, громадські організації. Ця країна однією з перших розробила національну програму медіаграмотності (ще у 2013 році та оновлену 2019-го). Медіаосвіта впроваджена на всіх етапах освіти – від дитячого садка до старшої школи. Влада виходить з того, що «медіаграмотність – ключова для побудови стійкого суспільства», і усвідомила це досить рано. Таким чином, громадяни складають перший рівень безпекового контуру, по суті, самостійно ухвалюючи рішення про рівень небезпеки, яку становить та чи інша інформація (Baltic Engagement Centre for Combatting Information Disorders, 2024).

Додатково ці заходи були підсилені через координацію між безпековими відомствами. Наприклад, Державна виборча комісія співпрацює з Службою інформаційної безпеки та зовнішньополітичним відомством, щоб відстежувати, які наративи з’являються в соцмережах під час виборів, і швидко реагувати (спростуваннями, роз’ясненнями, якщо треба – зверненнями до Facebook/Google про видалення відверто неправомірного контенту). Естонські посадовці активно взаємодіють з платформами; відомо, що перед виборами 2019 року Facebook видалив кілька фейкових акаунтів, котрі поширювали неправдиві новини про е-вибори, після сигналів від естонських спецслужб. Тобто замість ухвалення закону, що примушує Facebook до дій, Естонія використала міжнародний тиск і співпрацю для досягнення результату (McBrien, 2020).

Звіт «The Regulation of Fact-Checking and Disinformation in the Baltic States», демонструє, що у країнах Балтії спостерігається комплексний підхід до протидії дезінформації, який поєднує законодавчі, технічні та соціальні заходи. Литва на

законодавчому рівні криміналізувала умисне поширення дезінформації, хоча практика застосування відповідних норм залишається обмеженою. Латвія у 2024 році внесла зміни до кримінального кодексу, передбачивши покарання за використання технологій діпфейку для втручання у виборчий процес. При цьому в усіх трьох державах відсутні прямі аналоги німецького NetzDG, і регулювання платформ здійснюється через механізми обмеження доступу до контенту, що становить загрозу національній безпеці або громадському порядку. На практиці ці інструменти застосовувалися для блокування російських пропагандистських сайтів та телеканалів, помічених у систематичних кампаніях дезінформації (Baltic Engagement Centre for Combatting Information Disorders, 2024).

Безпекова політика Естонії і регіону загалом поєднує правові, технічні та соціальні компоненти, усвідомлюючи, що дезінформація є не лише юридичною проблемою, а й елементом гібридної чи психологічної війни. Підхід Естонії багато в чому проактивний, адже країна прагне підвищити стійкість суспільства до зовнішніх інформаційних впливів, перш ніж вони стануть критичними. У цьому контексті Естонія була однією з ініціаторок створення Європейського Центру передового досвіду з протидії гібридним загрозам у Гельсінкі, де основну увагу приділено інформаційним операціям. Політики запропоновані Естонією щодо безпеки громадян в соціальнх мережах є досить стриманими і відзначаються поміркованістю, так, на відміну від Литви, уряд не запроваджує великої кількості спеціальних законів, що відображає внутрішню політичну культуру з високою повагою до свободи слова та прагнення уникнути інструментів цензури (Estonian Human Rights Centre, 2026). Практично це також пов’язано з демографічним фактором, адже російськомовна меншина становить близько 25% населення, і надмірні заборони могли б активізувати російські наративи про утиски російської мови та додатково підживлювати деструктивні рухи в середині країни (Kremez, 2023).

Литва обрала більш «силовий» підхід, сигналізуючи як громадянам, так і зовнішнім акторам, що дезінформаційна активність буде кваліфікуватися як злочин проти держави. Балтійські країни виявили готовність радикально

обмежувати доступ до ресурсів, які вважаються джерелами інформаційної загрози. Наприклад, з 2022 році Латвія заблокувала доступ до 400 сайтів, які поширювали російську пропаганду, а також обмежели доступ до соціальних мереж і платформ, контрольованих Росією, посилаючись на їхнє використання у гібридних атаках і на підставі режиму надзвичайного стану, запровадженого після початку війни РФ проти України (ДетекторМедіа, 2025). Такий підхід відображає специфіку регіону, який безпосередньо межує з РФ, соцмережі афілійовані з Росією можуть становити настільки серйозну загрозу, що їх легше відключити повністю, ніж фільтрувати окремий контент. У Західній Європі подібна практика майже не зустрічається, за винятком спеціалізованих випадків.

У цілому, у балтійських державах існує консолідоване розуміння інформаційної загрози з боку Росії. Основні політичні сили не дискутують про саму необхідність боротьби з дезінформацією, а суперечки здебільшого стосуються методів її протидії — від «м'яких» заходів просвіти та спростування до жорстких правових і технічних інструментів блокування. В Естонії опозиція іноді критикує уряд за недостатню рішучість або навпаки, за потенційні ризики свободі слова. Політики в цих країнах часто акцентують, що боротьба з фейками – це частина їхніх зобов'язань перед ЄС і НАТО на «східному фланзі».

Балтійські країни дуже прямо формулюють мету своїх заходів, направлених на цифрове середовище – захистити інформаційний простір від російської дезінформації та пропаганди, яка розглядається ними як складова гібридної війни Кремля. Це захист від зовнішніх атак – настільки, що входять до стратегій національної безпеки цих країн. На відміну від західних країн, де іноді звучить ідея «суверенітету над даними» чи «цифрового протекціонізму» (щоб підтримати власні платформи), балтійці керуються чисто оборонними міркуваннями, вони не мають своїх великих платформ соціальних мереж, і захищають свій інформаціний простір від іноземних (зокрема російських) платформ, котрі можуть нашкодили їхній безпеці. У 2019 році, коли проводилися одночасно парламентські вибори в Естонії і Європарламент, естонські фахівці вже відстежували соцмережі в режимі реального часу та одразу реагували на

підозрілий контент. Підсумовуючи, варто відзначити, що загалом балтійці діють у руслі концепції «суспільний щит», де суспільство має бути заздалегідь підготовлене, щоб коли інформаційна атака все ж станеться, її ефект був мінімальний.

Для Естонії, Латвії, Литви соцмережі – це не тільки загроза, а й необхідний інструмент комунікації з громадянами і світом. Ці держави доволі успішно використовують соціальні платформи, щоб транслювати свої наративи. Наприклад, у Twitter та Facebook активно присутні профілі естонського уряду англійською та російською мовами, які доносять позицію щодо історичних питань, пояснюють політику НАТО і ЄС, спростовують дезінформацію (Естонія часто відповідає на фейки російського МЗС через твіти англомовного акаунту МЗС Естонії). Литва проводить «мем»-дипломатію – її МЗС і Міністерства оборони відомі підблікаціями, що висміюють російську пропаганду (NATO StratCom COE, 2021). Відтак, балтійські країни намагаються оволодіти мовою соціальних мереж і «воювати» на території противника. Вони також координуються з союзниками: зокрема, за підтримки НАТО створено Центр стратегічних комунікацій у Ризі, який аналізує тенденції в соцмережах у регіоні і ділиться інформацією з урядами. Отже, балтійський підхід передбачає, що соцмережі – своєрідне поле зіткнення, де потрібно не лише оборонятися, але й атакувати, захищаючи демократію та національну безпеку своїх країн.

Підсумовуючи, варто відзначити, що увага Європейського Союзу до соціальних мереж як важливого елементу у сфері національної безпеки почала виразно проявлятися на початку 2010-х років, суттєво під впливом зростаючої ролі цифрових платформ у політичному та безпековому вимірі. У 2013 році була опублікована Стратегія кібербезпеки ЄС під назвою «Стратегія кібербезпеки Європейського Союзу: відкритий, безпечний та захищений кіберпростір». Це був один із перших офіційних документів, у якому європейські інституції визнали соціальні мережі та інші онлайн-платформи потенційними джерелами загроз, що потребують комплексної відповіді. У документі підкреслювалися загрози

кібернетичних атак, дезінформації та маніпуляції громадською думкою через цифрові медіа, що стало основою для наступних дій та рішень.

У зв'язку з війною Україні та посиленням інформаційної війни з боку зовнішніх акторів, особливо Росії, у 2014–2015 роках Європейська Рада у березні 2015 року ухвалила висновки щодо необхідності стратегічних комунікацій для протидії кампаніям дезінформації. Це призвело до створення у 2015 році Оперативної групи стратегічних комунікацій (East StratCom Task Force) у рамках Європейської служби зовнішніх дій (EEAS). Група була створена спеціально для протидії кампаніям дезінформації, особливо через соціальні мережі, з метою дестабілізації ЄС та країн-членів.

Значення соціальних мереж стало ще більш чітким із прийняттям у квітні 2016 року «Спільної рамки протидії гібридним загрозам» Європейською комісією та Високим представником. Документ визначив соціальні медіа як ключовий канал поширення гібридних загроз, таких як дезінформація, політичне втручання та радикалізація. Це стало важливим етапом інтеграції соціальних мереж у загальну стратегію безпеки ЄС.

У грудні 2016 року Європейський парламент додатково закріпив цей підхід, ухваливши резолюцію про стратегічні комунікації ЄС щодо протидії пропаганді третіх країн. Резолюція закликала до активної співпраці з платформами соціальних медіа з метою посилення прозорості, боротьби з дезінформацією та зміцнення стійкості ЄС перед гібридними загрозами.

Подальша інституціоналізація відбулася з ухваленням у грудні 2018 року Європейською комісією «Плану дій проти дезінформації». Цей план передбачав системний підхід, включаючи співпрацю з онлайн-платформами, фактчекерами та громадськими організаціями. Він запровадив важливі механізми, такі як Система швидкого оповіщення ЄС (Rapid Alert System), для оперативного обміну інформацією між інституціями ЄС та країнами-членами у відповідь на скоординовані кампанії дезінформації.

На рівні ЄС проблематика соцмереж і нацбезпеки також отримала розвиток, особливо після 2018 року. Багато національних ініціатив (як-от

німецький NetzDG чи французькі закони) стали прототипами для нових європейських правил. У 2022 році ЄС ухвалив Акт про цифрові послуги (DSA) – комплексний регламент, що встановлює єдині вимоги до онлайн-платформ у всіх країнах. DSA, серед іншого, зобов'язує великі соцмережі швидко видаляти незаконний контент по запиту національних органів, розкривати алгоритми рекомендацій та модерації для аудиту, проводити регулярну оцінку ризиків (зокрема ризиків поширення дезінформації або виборчих маніпуляцій), надавати дослідникам доступ до даних. Це частково уніфікує підходи і піднімає мінімальний рівень реакції навіть в тих країнах, які раніше не мали національних законів. Скажімо, Іспанія чи Нідерланди не приймали власних «антифейкових» законів, покладаючись на саморегуляцію та загальні норми. Європейський Союз також ініціював Кодекс практик щодо дезінформації – добровільну угоду з технологічними компаніями (2018, оновлено 2022), де соцмережі зобов'язуються маркувати ботів, закривати фейкові акаунти, співпрацювати з фактчекерами тощо. Хоч кодекс і не обов'язковий, його підтримали ключові платформи, і він став своєрідним європейським стандартом.

Національні уряди активно брали участь у формуванні цих європейських політик. Наприклад, Франція лобіювала положення про термінове зняття терористичного контенту, спираючись на свій досвід (в результаті це закріплено в регламенті і діє по всьому ЄС). Німеччина наполягала на включенні соцмереж до сфери DSA і збереженні можливості національних штрафів. Польща і деякі інші – на гарантіях свободи слова (щоб була процедура оскарження модерації контенту, що теж ввійшло в DSA). Проте національні особливості все одно лишаються – скажімо, французький регулятор Arcom (на базі CSA) отримав додаткові повноваження моніторити виконання DSA у Франції, і той же Viginum тісно співпрацює з Arcom, щоб відстежувати іноземні впливи в соцмережах. В Естонії координатором DSA буде міністерство економіки, яке може долучати свій Центр стратегкомунікацій. Тобто структури, створені під час національних ініціатив, тепер використовуються для впровадження загальноєвропейської політики.

Протягом останнього десятиліття ставлення Європейського Союзу до соціальних мереж пройшло еволюцію від майже повної відсутності уваги до визнання їх одним з ключових факторів безпеки. Генеза цієї політики відображає уроки низки криз: терористичних атак, хвиль зовнішньої дезінформації, втручання у вибори, зловживань даними користувачів, пандемії COVID-19, а також війни в Україні. Кожна з цих подій спонукала до нових кроків – від створення робочих груп і добровільних кодексів до ухвалення законів та запровадження санкцій та обмежень для соціальних мереж.

Нині в арсеналі ЄС – ціла низка інструментів, які охоплюють як неформальні механізми співпраці з платформами, так і обов'язкові норми. Офіційні документи ЄС (комунікації, плани дій, регламенти) чітко визначили, що соціальні мережі мають бути частиною безпекового контуру: від них вимагається швидкого реагування на протизаконний та шкідливий контент, прозорості та підзвітності. Політичні дебати в Європарламенті і між державами-членами збалансували ці вимоги з потребою зберегти свободу слова і інтернет як відкритий простір – тому ЄС обрав модель, де платформи залучені до вирішення проблем (через кодекси поведінки, спільні заходи), але під наглядом суспільства і влади.

Соціальні мережі поступово стали не лише середовищем комунікації, а й ареною, де вирішується питання національної та регіональної безпеки. Їхній вплив на громадську думку, вибори, соціальну стабільність і навіть результати воєн тепер неможливо ігнорувати. ЄС, реагуючи на цей факт, вибудував у 2015–2022 роках політику, що включає елементи кібербезпеки, інформаційної протидії та правового регулювання. Цей досвід Євросоюзу став прикладом для інших демократій світу, в який спосіб можливо «опанувати» глобальні соціальні платформи, вписавши їх у рамки верховенства права та колективної безпеки.

Більшість європейських урядів ЄС усвідомили, що неможливо просто «відключити» соцмережі – натомість треба включати їх в контур європейської безпеки. Паралельно з обмежувальними заходами йде процес інтеграції соцмереж у державне управління: від спілкування чиновників з громадянами (е-

government через Facebook Messenger, наприклад, у Естонії) до цілих цифрових кампаній.

3.2. «Веапонізація соціальних мереж: застосування цифрового середовища у військових операціях та оборонних доктринах ЄС»

Для подальшого заглиблення в проблематику соціальних мереж слід увести поняття «веапонізація» («weaponization»), котре описує процес, коли явища чи інструменти, які первинно не були військовими, цілеспрямовано використовуються як зброя у політичному або воєнному протистоянні. Це поняття увійшло в академічний лексикон на тлі змін у характері сучасних конфліктів після закінчення Холодної війни. І все частіше входить у вжиток в західних дослідженнях, присвячених політиці та міжнародним відносинам. Як зазначає дослідник Марк Ґалеотті, фактично «будь-що може бути використане як зброя в сучасну добу» (Galeotti, 2022). Традиційні збройні зіткнення, разом із тим, стали надто дорогими та ризикованими, натомість держави все частіше вдаються до «війни всіх проти всіх» у постійному конкурентному середовищі, де військова сила заміщується шпигунством, саботажем, кібернападами, економічним тиском та інформаційними операціями. Це твердження дослідника є валідним лише частково, адже світ з моменту широкомасштабного російського вторгнення в Україну перебуває у доволі турбулентному становищі, коли «правила гри», встановлені в післявоєнний період, поступово демонтуються. У цьому контексті термін «веапонізація» став застосовуватися до різних сфер – економічної взаємозалежності, інформації, культури, технологій – щоб описати, як вони перетворюються на інструменти тиску і впливу.

У міжнародних відносинах концепцію «weaponized interdependence» запропонували Генрі Фаррелл і Абрахам Ньюман, показавши, як держави можуть використати асиметричну структуру глобальних економічних та інформаційних мереж для примусу і досягнення стратегічних цілей (Farrell & Newman, 2019). На практиці це означає, що країна, контролюючи ключові вузли або ресурси

(фінансові системи, енергетичні поставки, інтернет-інфраструктуру), здатна «відключити» суперника від життєво важливих потоків або зібрати цінну інформацію, перетворюючи взаємозалежність на зброю. Яскравий приклад – «енергетична зброя» Росії, використання нею поставок газу та нафти як важеля тиску на Європу. Як відзначає Джозеф Най, вторгнення Росії в Україну і проілюстрували небезпеку економічної залежності від авторитарних держав (Nye, 2022).

Цей приклад ілюструє, що глобалізовані зв'язки, які раніше вважалися взаємовигідними, у сучасних умовах можуть свідомо порушуватися задля геополітичного шантажу. Паралельно у сфері міжнародних комунікації та ідеологічного протиборства виникло поняття «гостра сила» (sharp power), запроваджене Крістофером Вокером і Джесікою Людвіг для опису проєкції впливу авторитарних режимів. «Гостра влада» позначає методи, за допомогою яких автократії обмежують свободу слова, поширюють дезінформацію та викривлюють інформаційне середовище демократій (Walker & Ludwig, 2017). На відміну від «м'якої сили» (soft power) Джозефа Ная, що базується на привабливості і переконанні, «гостра сила» є репресивно-маніпулятивною за своєю суттю та прагне підірвати цілісність незалежних інститутів, цензурувати небажані повідомлення і сіяти сум'яття.

Авторитарні держави на кшталт Росії та Китаю активно застосовують такі підходи, використовуючи асиметричні стратегії між відкритими й закритими суспільствами. В цьому випадку вільний простір демократичних країн стає полігоном для маніпуляцій, тоді як власний інформаційний простір автократії віддзеркалюють або «екранують» від зовнішніх ідей та інформаційного проникнення. У термінах Ная це своєрідна «інверсія м'якої сили», коли культура, медіа та освіта чи соцмедіа перетворюються з мостів взаєморозуміння та комунікаційних майданчиків на зброю впливу.

Поняття «веапонізація соціальних мереж» увійшло до вжитку після низки подій 2010-х років: «Арабська весна» продемонструвала роль Facebook і Twitter в мобілізації протестів, ІДІЛ успішно рекрутувала прихильників через YouTube і

Telegram, а російські операції впливу через Facebook та Twitter вплинули на перебіг референдуму щодо Brexit та виборів у США 2016 року. Ці події були докладно проаналізовані науковцями протягом останньої декади. У 2018 р. вийшла книга Пітера Сінґера та Емерсона Брукінґа «LikeWar: The Weaponization of Social Media», де автори переконливо доводять: «майбутні війни відбуватимуться у соціальних мережах». Вони розглядають інтернет як новий театр війни – продовження політики іншими засобами, де «межа між миром і війною розмивається» і боротьба йде за свідомість мас (Singer & Brooking, 2018).

Таким чином, поняття «веапонізація» сформувалося на перетині досліджень влади і безпеки аналізу авторитарного впливу та досвіду новітніх конфліктів. Воно відображає якісну зміну у світовій безпеці: інформація, економіка, технології, взаємозв'язки – усе може стати зброєю у глобальному протистоянні. Зокрема, соціальні мережі із платформ для спілкування перетворилися на стратегічний ресурс, здатний як зміцнити демократію, так і поставити її під удар. Різноплановість явища веапонізації цифрового середовища зумовила появу кількох теоретичних підходів до його аналізу. Базуючись на роботах ключових дослідників активного перетворення мереж та соцмедіа на зброю, можна виокремити кілька форм «цифрової зброї» за характером впливу: інфраструктурна, психологічна та алгоритмічна.

Інфраструктурна «цифрова зброя» – це використання або ураження самої цифрової інфраструктури ворожої держави для досягнення воєнних цілей. Ідеться про кібератаки на критичні мережі, сервери, комунікаційні системи, про використання інтернету як поля бою. Едвард Лукас у книзі «Cyberphobia: Identity, Trust, Security and the Internet» застерігав, що залежність суспільств від мереж створює нові вразливості, де хакерські операції можуть паралізувати економіку чи оборону без жодного пострілу. Приклади не забарилися – атаки російських хакерських груп на електромережі України (2015, 2016), вірус NotPetya (2017), що вразив світову інфраструктуру, або злам супутникової мережі KA-SAT у день вторгнення РФ в Україну 24.02.2022. Цей останній випадок навіть потрапив у поле зору Європейського інституту космічної політики, у звіті «EU space strategy

for security and defence», вказано, що кібератака на «KA-SAT демонструє, що комерційні космічні системи є важливими інструментами для підтримки військових операцій на Землі, а також головними цілями для (кібер)атаки». Космічні засоби також мають вирішальне значення у відповіді України на російське вторгнення: військова та цивільна реакція України на вторгнення Росії значною мірою залежить від Starlink (EPRS, 2023).

Марк Ґалеотті, аналізуючи інструменти сучасної російської гібридної стратегії, звертає увагу на використання економічних і напівлегальних мереж як інструментів політичного впливу, що концептуально можна інтерпретувати як форму «економічної ґерили». До неї входять злами банків, маніпуляції валютою тощо – усе це стало можливим завдяки цифровим технологіям. Таким чином, інфраструктурна форма цифрової зброї охоплює дії, спрямовані на руйнування або використання цифрових «артерій» суспільства: електронних реєстрів і мереж зв'язку, хмарних сховищ даних та супутників і цифрової архітектури аеропортів.

Психологічна «цифрова зброя» – це інформаційно-пропагандистські впливи через онлайн-середовище, метою яких є вплинути на свідомість, настрої та поведінку населення, деморалізувати війська чи суспільство противника, дезорієнтувати різні гілки влади та зробити організований спротив складнішим. Цей вимір спирається на класичні теорії психологічної війни, але здобуває нові можливості завдяки соцмережам. Ще у 1970–80-х роках теоретик ненасильницьких дій Джин Шарп показав, що масові комунікації і символічні дії можуть стати потужною зброєю проти диктатур – достатньо згадати його «198 методів ненасильницького спротиву» (Шарп, 1973). Сьогодні ж, у добу Facebook і YouTube, можливості для таких впливів зросли на порядки.

З іншого боку, ті ж режими самі навчилися використовувати психологічні операції онлайн: Росія стала піонером у проведенні координованих дезінформаційних кампаній проти інших держав. Едвард Лукас і Пітер Померанцев у звіті «Winning the Information War: Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe» (2016) проаналізували російські тактики інформаційної війни – від «фабрик тролів» та

бот-мереж, які масово тиражують вигідні Кремлю наративи, до тонших методів, як-от просування конспірології чи розпалювання внутрішніх конфліктів у країнах Заходу. Мета таких операцій – посіяти недовіру і хаос, розколоти суспільство, підірвати вольовий опір без застосування сили (Pomerantsev, & Lucas, 2016).

Алгоритмічна «цифрова зброя» – новітній феномен, пов'язаний з використанням великих даних, штучного інтелекту та алгоритмів соціальних платформ для маніпуляції виборами громадян. Шошанна Зубофф у праці «The Age of Surveillance Capitalism» показує, що сучасні цифрові платформи функціонують як інфраструктури поведінкового контролю, де збір і аналіз даних дозволяють не лише передбачати, але й формувати дії користувачів, створюючи нові асиметрії влади в інформаційному середовищі. Дослідниця описала, як великі технологічні корпорації накопичують безпрецедентний обсяг даних про користувачів і застосовують алгоритмічні системи для передбачення та спрямування поведінки людини. Первинно – з комерційною метою, задля тоншого налаштування рекламних повідомлень у соціальних мережах, проте ті самі механізми вже неодноразово були задіяні і в політичних чи воєнних цілях (Zuboff, 2019). Використання соцмереж під час електоральних циклів продемонструвало принципово новий вид зброї – «бомбардування» свідомості, коли кожен громадянин та потенційний виборець отримує свій специфічний «набір» меседжів, слабко помітних ззовні, але надзвичайно ефективних. Крім того, алгоритми самих соцмереж (наприклад, стрічка новин Facebook або рекомендаційна система YouTube) влаштовані так, що віддають перевагу більш резонансному, емоційному контенту, часто на шкоду правдивості.

Варто відзначити зміни, які соціальні мережі принесли в політичну культуру та комунікації між політиками та виборцями. Політичні партії та впливові політичні фігури, розуміючи увесь потенціал мереж, активніше звертаються напряму до своїх виборців через соцмережі, оминаючи «традиційні» медіа. Яскравий приклад — комунікації кандидатів під час президентських виборів в США в 2024-му році, під час яких платформи соцмереж були полем

безперервних політичних дебатів, маніпуляцій та інформаційного впливу і, найнебезпечніше, були джерелом політичної поляризації в американському суспільстві. Важливим тут є той факт, що відбулося не лише «переміщення» аудиторії від «традиційних» медіумів у цифровий простір, а й поступовий спад довіри до усталених інституцій та медіа (Wike et al., 2024).

Дослідження довіри, проведене Інститутом довіри Едельмана, зафіксувало глобальну тенденцію до зростання страху перед неправдивою інформацією, починаючи з 2021-го року (Edelman Trust Barometer Global Report, 2025). В суспільствах по всьому світу наростає тривога, пов'язана з тим, що представники уряду, бізнесу та ЗМІ усвідомлено транслюють неправдиву інформацію. Для уряду цей параметр виріс на 11 пунктів і зараз складає 69, а для сфери журналістики 70, де також відбулося зростання на 11 пунктів. Також барометр демонструє, що медіа мають низький рейтинг довіри серед інших інституцій, пропускаючи вперед бізнес або некомерційні організації. Серед 28-ми країн, де проводилося опитування, медіа не довіряють в 14-ти. Показово, що в ці чотирнадцять країн потрапили країни, в яких усталена та стійка демократія – Швеція, Німеччина, Ірландія, Японія, Сполучене Королівство, Іспанія, Сполучені Штати тощо. Натомість найбільше довіри до медіа демонструють країни, які в рейтингу Freedom House відзначені в категорії «невільних» або «частково вільних», наприклад, Китай, Індонезія та Індія. 63% опитаних підтримують твердження, що дедалі важче відслідковувати, чи походить повідомлення з перевіреного та «поважного» джерела, чи її автором є хтось, хто прагне маніпулювати суспільною думкою (Гончар, 2025).

Також важливо відзначити, що соціальні мережі цілковито не стали повноцінним замінником традиційних медіа з точки зору довіри, опитування демонструє, що соціальні мережі мають менший «кредит довіри» у порівнянні з першими. Таким чином, розгортаються одночасно декілька глобальних процесів – ЗМІ втрачають довіру, що прямо впливає на їх легітимність в ролі «четвертої влади», а соціальні мережі та специфіка роботи їх алгоритмів не дозволяє їм утвердитись в ролі джерела інформації, котрому можна довіряти, але поруч із

цим вони створюють «бульбашки дезінформації» та консолідують прибічників популістських політичних сил (Гончар, 2025).

Європейська політика демонструє десятки випадків, коли соціальні мережі та інтернет стають інструментом в руках політиків, які вдало користуються моментом невпевненості та страху, відзначених в звіті Едельмана. В Італії популістські політичні сили використали інтернет для мобілізації прихильників «Руху п’яти зірок», який виріс із блогу коміка Беппе Грілло, зробивши ставку на розчарованих громадян. Подібно, в Іспанії лівопопулістська партія Podemos використала Facebook і Twitter для організації масових протестів та розбудови підтримки поза межами традиційних медіа (Gerbaudo, 2018). Під час президентських виборів у Франції у 2017-му році відбувалися координовані атаки через соціальні мережі персонально на президента Макрона. Зовнішнім акторам, які ініціювали ці інформаційні кампанії, на руку зіграв «Macron Leaks», коли за два дні до голосування хакери опублікували в мережі добірку документів штабу Макрона. Цей випадок був спробою прямого втручання та впливу на фінальний результат виборів однієї з ключових країн Європейського Союзу (Mohan, 2017).

В Угорщині партія «Фідес» активно задіює увесь спектр можливостей соціальних мереж для просування власних наративів та консолідації прибічників. Випадок Угорщини цікавий ще й тим, що сама влада виступає в якості джерела дезінформації: здійснюючи атаки на нечисельну опозицію, поширюючи кремлівські тези про російсько-українську війну. Угорський уряд підкріплює настрої недовіри до ЄС, міжнародних організацій та інституцій, підтримуючи стабільність своєї влади (Freedom House, 2025).

Часом соціальні мережі дозволяють аутсайдерам користуватися недосконалістю демократичного суспільства та здобувати значну підтримку в ході виборів. Раптове лідерство Келіна Джорджеску на президентських виборах в Румунії за допомогою TikTok та Telegram – приклад того, як електоральний ландшафт під впливом «алгоритмічної цифрової зброї» цілком перегортається за допомогою технологій (Гончар, 2025).

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 як 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 «нездоланними» навіть без застосування чи опертя на збройну силу, якщо вони володіють відповідними навичками організованого, скоординованого і морально обумовленого легітимного опору. У своїх працях «Від диктатури до демократії», «Making Europe Unconquerable» (1985) та «Civilian-Based Defense» (1990) 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 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 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 століття, в якому заборона 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 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. 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 (Померанцев, 2025).

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 урядам 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 – 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 (Sharp, 1973). 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 (Sharp, 1993).

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. Ця ідея є універсальною і дозволяє однаково пояснювати як динаміку авторитарних, так і демократичних систем (Sharp, 1993).

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 «стовпів» — наприклад, атакуючи довіру до виборчої системи, медіа чи міжнародних структур ЄС, про що йшлося вище. 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.

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. 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 (Гончар, 2025).

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, адже вони працюють через локальних акторів і «здаються» органічними для внутрішнього інформаційного поля. Це має два 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: The Potential of Civilian-Based Deterrence and Defence» 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 (Sharp, 1985).

Описаний досвід Литви, Латвії та Естонії демонструє 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 додаткової 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, згаданої раніше, що «здатність до спротиву має виховуватися задовго до моменту атаки» (Гончар, 2025).

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 в 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 (Sharp, 1993, From Dictatorship to Democracy). 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, що 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 теорії військову силу. Він стверджує, що організована неспівпраця 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.

Окремо слід 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».

Системність теорії Джина Шарпа дозволяє побачити важливу трирівневу структуру захисту. Перший аспект розгортається на рівні індивідів — як культивація навичок неспівпраці з маніпуляцією: медіагігієна, мінімізація участі у ланцюгах поширення токсичного контенту тощо. Більше того, індивідуальна здатність виявляти та свідомо відмовлятися від «співпраці» зі 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, у свою чергу, вимагає розбудови етичних кодексів, що утримують суспільство в балансі, відмовляють у мові ворожнечі між учасниками 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. Ця трирівнева модель дозволяє забезпечити стійкість демократичного суспільства в умовах, коли межа між миром та війною в соціальних мережах дедалі більше розмивається. «Цифрова» громадянська

оборона цілком адаптується до підходів, які запропоновані для громадянської оборони офлайн-формату: підготовка кадрів, симуляції криз, правові рамки прозорості алгоритмів, узгоджені 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, до прикладу, протиставляє одноразові кампанії — реакції лише постфактум — культурі прогнозування і превентивного розгортання громадянської оборони. Вона розглядається не як пасивна оборонна конструкція, але як динамічна та активна система, що здатна діяти на випередження, зберігаючи моральну стійкість та суверенітет навіть у разі тривалої зовнішньої загрози.

Перенесення цієї логіки у цифровий простір Європейського Союзу вимагає, у тому числі, глибокого переосмислення ролі громадянина в захисті євпроейського інформаційного поля, ЄС має не лише створювати захисні механізми, а також визнати факт, що цифровий простір ЄС вже є театром систематичних атак з боку авторитарних держав, а отже, вимагає складнішої системи їх нейтралізації. В цій трирівневій моделі громадянське суспільство та неприбуткові організації виступають активним партнером держави у протидії поширенню шкідливої інформації в соціальних мережах. Важливим наслідком такої постановки питання є переорієнтація з суто оборонної безпекової моделі на проактивну стратегію. Це передбачає не лише нейтралізацію шкідливих впливів, але й цілеспрямоване формування стійкої та суб’єктної цифрової культури в ЄС. Якщо авторитарні режими намагаються розхитати підтримку демократичних інституцій через відповідні «слабкі» місця в дократичному процесі, то випрацювання усвідомленої «неспівраці» європейських громадян із агресором є одним із факторів, котрий може додатково збалансувати комплекс безпекових

заходів, які здебільшого представлений нині у формі законодачого регулювання соцмереж та інтернету.

Разом із тим, лишається нерозкритою 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 (Лукас, 2008). Він доводить, що «гасіння пожеж» демократичними системами лише призводить до їх відставання в геополтичному вимірі. 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, свого роду фортеці, — до суб'єкта, здатного формувати власний порядок денний у цифровому просторі та соціальних мережах.

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 безпрецедентним атакам на своє медіаполе, котре, безумовно, включає і його цифровий вияв. В цій ситуації напрацювання в українських громадян спроможності «неспівпраці» 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.

В пошуках відповіді на це запитання варто звернутися до логіки, яку пропонує Едвард Лукас. У своїх працях «The New Cold War» (2008) та звітах на зразок «Winning the Information War» (2016) він доводить, що західні демократії

зіштовхнулися з новим типом загрози, коли соціальні мережі перетворюються на канали поширення фейків, поляризації суспільств і підриву інституцій. На думку Лукаса, Європейський Союз — одна з ключових цілей таких впливових операцій. Лукас наполягає, що використання інформації для підриву супротивника — не нова практика, але сьогодні її радикально посилили цифрові технології. Кремль з XX-го століття провадить операції впливу, саме тому ігнорувати цей контекст небезпечно.

У звіті «Winning the Information War», підготовленому разом із Пітером Померанцевим, Лукас пише, що «використання Росією інформації як зброї не є новим, але складність і інтенсивність наростає». Новим є масштаб і швидкість, яких надають інтернет і соцмережі. Кремль та інші авторитарні актори «проштовхують конспірологічний дискурс і використовують дезінформацію, щоб забруднювати інформаційний простір, підвищувати поляризацію та підривати демократичні дебати», руйнуючи довіру до інституцій (Lucas & Pomerantsev, 2016). Ця загроза виходить далеко за межі «прифронтових держав» Східної Європи; вона реальна для союзників у Європі загалом і Північній Америці. У рамці Лукаса соціальні мережі — це одне з ключових бойовищ ширшої гібридної війни: через них авторитарні системи доповнюють відкриті пропагандистські майданчики традиційних медіа і наявні приховані операції з інформаційного впливу. Отже, «веапонізація» соціальних мереж — це процес перетворення платформ та соціальних мереж на інструменти геополітичної боротьби.

З теоретичного погляду Лукас вписує сучасну дезінформацію в доктрину гібридної війни, в якій Москва поєднує військові й невійськові засоби, де інформаційні операції доповнюють економічний тиск, кібератаки та навіть застосування сили. Гібридні операції послаблюють внутрішню й міжнародну волю, — зазначається у звітах CEPA, ускладнюючи захист кордонів, критичної інфраструктури й медіа (Bajarunas, 2025). Дезінформація, яку викоирстовує Кремль – це пряме продовження радянської пропаганди, попри певну дискусійність терміна «гібридна війна», він корисний тим, що підкреслює

багатовимірність стратегії РФ. Маніпуляції соцмережами — лише одна з форм досягнення цілей нижче порогу відкритої війни (Bajarunas, 2025). Росія може «досягати результатів, порівнянних із традиційними військовими операціями», не провокуючи прямої військової відповіді. Лукас доходить висновку, що країни Заходу, особливо ЄС, мають оновити свої підходи до цифрового простору та соцмереж в цілому. Лукас відстоює тезу, згідно якої, Захід має відновити знання та навички доби Холодної війни, в умовах Москва радикально кидає виклик євроатлантичній солідарності» і загрожує довгостроковому майбутньому європейського безпекового порядку (Лукас, 2008).

Авторирані режими використовують значний набір прийомів, якими експлуатують соцмережі та цифрову екосистему. Класична техніка — hack-and-leak, коли спецслужби викрадають конфіденційні дані й поширюють їх, аби скомпрометувати демократичних політиків. Приклади — витік листування Демократичної партії США 2016 року чи оприлюднення приватних розмов польських посадовців. Ці прийоми працюють завдяки маніпулюванню західними ЗМІ та соцмережами, котрі стають «каналом» для трансляції компромату й посіву сумнівів. Інша ключова техніка — масове виробництво неправдивого та оманливого контенту — те, що Лукас прямо називає «дезінформацією, яку просувають через Facebook і WhatsApp». Такі історії часто містять відсоток правди, але спотворені до сенсаційних викриттів і теорій змови.

Паралельно Москва вирощує симпатиків і проксі: пропонує «хлібні посади відставним політикам» (так звана «шредеризація», від імені екскансцлера ФРН Герхарда Шредера) або фінансує партії й ГО. Такі актори ретранслюють прокремлівські меседжі в соцмережах і мейнстримних дебатах, підсилюючи основну лінію пропаганди. Кремль при цьому ідеологічно опортуністичний: у одній країні підтримує крайніх правих, у іншій — радикальних лівих — будь-кого, хто стає «вхідною брамою» до розмивання демократичного консенсусу. Соцмережі збільшують вплив таких маргінальних голосів, дозволяючи фейкам проникати глибоко в суспільства.

Звіт «Winning the Information War» подає низку європейських кейсів. У Балтії та Центральній Європі російські наративи сіють страх і недовіру: «страшилки про західні інституції та альянси (Литва), підбурення до заколоту (Україна), загальна дискредитація міжнародної репутації країни (Латвія)». В Естонії та Чехії Кремль інвестує у «локальні» прокремлівські медіа, що маскуються під незалежні, але просувають потрібні меседжі. У Польщі та інших країнах підсилюються ультранаціоналістичні та ксенофобські голоси, ворожі до ЄС (Lucas & Pomerantsev, 2016). Ці приклади підтверджують, шо авторитарна стратегія ведення інформаційної війни підлаштовується під конкретні вразливості — етнічні напруження, історичні образи, соціально-економічні фрустрації. Соцмережі є сполучною тканиною цих зусиль, дозволяючи чуткам і вигадкам перетинати кордони та досягати «домінування наративу» над фактами. Як зауважують Лукас і Померанцев, російські вигадки часто «розважальні й емоційно привабливі» та вбудовані у стратегічні наративи, що резонують із цільовими аудиторіями (Lucas & Pomerantsev, 2016)..

Хоч Росія – головний фокус Лукаса, він підкреслює, що вона не унікальна у своїх спроб дескредитувати демократиний устрій. Інші авторитарні сили, зокрема Китай, опановують соцмережі для пропаганди та впливу. Лукас брав участь у ініціативі CEPA «Infektion Points» (2020) щодо російської та китайської дезінформації під час COVID-19. Під час пандемії Пекін і Москва наповнювали соцмережі фейковими наративами, хоч і з різними цілями: КНР звинувачувала США у походженні вірусу та демонструвала себе як донора допомоги, Росія ж «сіяла розбрат всередині західних країн, щоб підірвати довіру до компетентності європейських урядів». Обидва режими експлуатували слабкості інформаційного простору, щоб контролювати й модифікувати наративні лінії із значними наслідками для геополітики та нацбезпеки (CEPA, 2020).

Лукас закликає до рішучої протидії, прозорості й міжпартійної згоди. Держави мають «розслідувати, що сталося, і покарати винних», а також «укріпити системи, щоб це не повторилося»: від кіберзахисту штабів до суворішого моніторингу іноземного фінансування та онлайн-реклами в

кампаніях. У свідченнях британському парламенту, в 2018-му році, Лукас радив зосередитися на «каналах» втручання в європейські справи , по суті повторюючи ідею Шарпа про важливість захисту «стовпів підтримки», напротивагу тривалим обговоренням про визначення меж між цензурою та справедливими обмеженнями. (House of Commons Digital, Culture, Media and Sport Committee, 2018). Замість оцінювати кожну публікацію, слід розбиратися, як приховані сторінки, боти та компанії поширювали меседжі й купували політичну рекламу. Основний фокус — прозорість платформ і нагляд за соціальними мережами, Facebook, Twitter/X і Google мають розкривати, хто стоїть за оголошеннями на політичну тематику та впливоми інтернет-акторами, як це вже вимагається від традиційних медіа. Відсутність прозорості дозволила російським агентам 2016-го анонімно закуповувати значні обсяги деструктивної та полризуючої реклами в мередах і створювати фальшиві особистості без реальних ризиків викриття. Позаяк ідеться не лише про національні вибори, Лукас вбачає ширший шаблон авторитарного втручання в європейський дискурс — від нідерландського референдуму 2016 року щодо Угоди Україна — ЄС до виборів у Франції та Німеччині, де російські медіа намагалися підсилити радикальних кандидатів. Кожен із цих епізодів — бій у триваючій «війні ідей», де автократії дискредитують демократію. Як зауважувала єврокомісарка Вєра Йоурова, Кремль володіє «багатомільйонною зброєю масової маніпуляції», націленою на вибори в ЄС (Bloomberg, 2023).

Отже, втручання через соцмережі — це напад на суверенітет європейських демократій. На відміну від традиційної війни, яка загрожує території, гібридна агресія б’є по інформаційному простору — спільній реальності й довірі, на яких тримаються не лише вільні вибори, але основоположні європейські принципи. Злами даних кандидатів, фейки про політиків і партії, підсилення екстремістських голосів — усе це має на меті або перекосити результати, або бодай підірвати віру громадян у демократичні процедури. Навіть якщо підсумок голосування не змінюється, підривається довіра — і це вже стратегічний виграш Москви чи Пекіна, котрі вбачають в атомізації населення потужний

управлінський підхід. Для ЄС, побудованого на демократичних цінностях та колективному ухваленні рішень, збереження демократичних процесів є критично важлим, адже зниження легітимності ЄС та його інституцій в очах громадян – це шлях до наростання зневіри, збільшення кількості євроскептиків та подальшого зростання прихильників політичних сил, котрі прагнуть демонтувати це об'єднання. Тому безпеку виборів слід трактувати як складову нацбезпеки. Ініціативи на кшталт East StratCom Task Force, яка викриває фейки, вже працюють над збереженням стійкого інформаційного поля, але захист виборів та демократії у добу «веапонізованих» соцмереж потребує глибшої кооперації урядів, платформ і громадянського суспільства у зміцненні демократії.

Лукас називає кілька структурних вразливостей та викликів, які є важливими для розуміння того, в який спосіб варто розбудовувати систему «цифрової» громадянської оборони. Передусім — онлайн-анонімність і фальшиві ідентичності. На відміну від офлайн-світу, де медіа та політичні рекламодавці підзвітні, великі платформи дозволяють користувачам та іноземним політичним акторам діяти під вигаданими іменами чи без них. Це дає широкий простір для зловживань: можна запустити «незалежне» медіа або сторінку зі схованою власністю, а «фабрика тролів» створить тисячі акаунтів під виглядом місцевих громадян. Купівля політичної реклами нерідко відбувається невідстежуваними платежами (наприклад, передплаченими картками з інших країн). Анонімность ускладнює ідентифікацію таких операцій і зменшує простір для покарання виконавців.

У лекції 2019 року в Оксфорді він стверджував, що домінантні соцмережі «майже неможливо регулювати, і вони відкриті до маніпуляцій» за нинішніх умов; отже, потрібна публічна дискусія про стандарти цифрової ідентифікації. Лукас не закликає до повної заборони анонімності, але вважає, що надійна автентифікація має стати нормою для громадянських взаємодій онлайн. Основний фокус такої пропозиції – дати користувачам можливість підтверджувати особу, а платформам – чітко позначати неперевірені або неавтентичні джерела, подібно до маркування спаму в електронній пошті (Lucas,

2019). Можна відзначити, що Британський уряд у 2024-му році взяв курс на збільшення сервісів, платформ та соцмереж, які вимагають ідентифікації за ID-карткою для верифікації особи (Department for Science, Innovation and Technology [DSIT], 2024).

Друга вразливість – нестача прозорості й підзвітності техногігантів. Під час розслідування в парламенті Великої Британії Лукас зауважував, що компанії на кшталт Facebook неохоче визнавали масштаб російських зловживань їхніми системами. Спершу Facebook применшував активність РФ довкола Brexit, визнаючи лише обмежений вплив платформи на процес референдуму і лише під тиском розкрив масштабніші операції. Логічним продовженням є нарощування прозорості соціальних мереж через механізми публічності архівів політичної реклами, обов'язок ділитися даними про скоординовану неавтентичну поведінку з незалежними аудиторами пошті (Lucas, 2019). ЄС вже рухається в цьому напрямі, зокрема через згаданий раніше акт DSA. Водночас він застерігає, що інструменти на кшталт фактчекінгу самі по собі недостатні. Потрібні структурні кроки: прозорість, автентифікація користувачів, регулювання політичної реклами, підвищення медіаграмотності.

Третій вимір — суспільні вразливості, що роблять демократії чутливими до маніпуляцій. Успіх дезінформації часто відбиває глибші проблеми — соціальну відчуженість, поляризацію, падіння довіри до еліт. Лукас позитивно оцінює досвід Балтії — «щеплення» населення від кремлівської пропаганди через медіаграмотність і вивчення історії, аби впізнавати спроби «переписати» минуле чи розпалити міжетнічну ворожнечу. Лукас розглядає «веапонізацію» соцмереж як ключовий виклик безпеці Європи та Заходу, а не як тимчасову проблему. На його думку, російські дезінформаційні наступи — частина стратегії підриву західної політичної згуртованості та самих засад ліберальної демократії. У «Winning the Information War» він попереджав: Росія «має на меті підірвати заснований на правилах багатосторонній безпековий порядок у Європі» і застосовує для цього всі інструменти — від сили до медіаманіпуляцій. Мова про розщеплення західного альянсу та демократичного консенсусу: дезінформація

«радикально кидає виклик євроатлантичній солідарності», розширюючи кожну тріщину — між державами ЄС і між Європою та США (Lucas & Pomerantsev, 2016).

Переповнюючи європейський інформаційний простір наративами, що ставлять під сумнів НАТО, ЄС і трансатлантичні зобов'язання, Кремль підточує взаємну довіру, яка є основою цих інституцій. Фейки на кшталт «НАТО спровокувало Росію» чи «ЄС валиться через міграцію» підживлюють націоналістичні та сепаратистські рухи, послаблюючи єдність ЄС. Кожна фейкова історія — від змонтованих відео, що розпалюють етнічну ворожнечу, до конспірології про закупівлі вакцин — зрештою підриває європейське врядування. Захист «довгострокового майбутнього європейського безпекового порядку» тепер означає і безпеку цілісності інформаційного простору в схожий спосіб як того вимагають фізичні кордони Євроунії. Лукас допомнює цей вимір й іншими авториратрними державами, демонструючи, що автократи по всьому світу агресивно застосовують дезінформацію у своїй зовнішній політиці. Китай послуговується доктриною «трьох видів війни» (психологічна, медійна, правова), кидаючи виклик міжнародним нормам — зокрема у Південно-Китайському морі — методами, паралельними до російських. Терористичні організації також майстерно використовують соцмережі для радикалізації, «доставляючи пропаганду адресно до домівок на Заході». Для авторитарних систем домінуючим є переконання, що ліберальні демократії можна знищити зсередини, роз'їдаючи соціальну довіру й блокуючи політичні процеси навіть без військових дій. Для ЄС — блоку демократій і регуляторної наддержави — виклик подвійний, адже вимагає захисту виборів, публічної сфери й процедури ухвалення рішень та одночасно випрацювати допустимі межі потенційної відповіді, задаючи норми та координуючи дії демократій. Одним із ключових спостережень, яке можна виокремити у Лукаса, є думка про те, що Захід реагує повільно й фрагментовано на зовнішні загрози, викликані інформаційногою добою, він закликає до більшої амбіції — фактично до оновлення підходів та створення нових безпекових

політик, які би взорзували на досвід Холодної війни, але були адаптовані до цифрової ери (Лукас, 2008).

Веапонізація соцмереж, таким чином, це оформлена загроза нацбезпеці й виклик управлінню. Воно вражає цінності та згуртованість ЄС, перетворюючи відкритість демократичних суспільств на їхню вразливість. У Кремлі ідеї й наративи сприймають як інструменти війни: незалежна журналістика, вільні вибори й права людини розглядаються як шкідливі загрози режиму — тож їх дискредитують. Так авторитарні режими намагаються зробити світ безпечним, в першу чергу, для самих себе. ЄС як велика спільнота ліберальних демократій — одна з головних цілей. Чи то російські тролі, що підігрівають суперечки довкола каталонської незалежності, чи китайські дипломати з дезінформацією про 5G — мета одна зробити Європу розділеною, заляканою та нерішучою. Як підсумував Померанцев, «якщо Захід навчиться боротися з російською дезінформацією, то буде краще підготовлений до майбутніх викликів» (Померанцев, 2019). Інакше кажучи, успішна протидія нинішнім атакам, які полегшують алгоритми соцмереж, зміцнить стійкість демократії у світі і потенційно створить нові підходи до врядування демократіями, які передбачатимуть не лише оборону, але і перевинайдення ідеї здатності євпропейцями використовувати силу у відповідь.

Відзначимо, що нині європейська політика безпеки не передбачає такого підходу. Паскаль Брюкнер переконливо доводить, що «відчуття провини» за власну історію живить віктимність європейських суспільств і вже не містить того елементу конструктивної критики, а натомість лише підіграє авторитарним режимам, котрі висувають претензії до держав Європи з вимогою віддати неіснуючі «борги» та шантажують уряди (Брюкнер, 2014). Популістичні сили, котрі часто оперують історичними категоріями та позірним традиціоналізмом, активно розповсюджують свої наративи в соціальних мережах, збираючи електорат невдоволених. Історичний ревізіонізм вже став одним із основних інструментів правих та крайніх правих сил по всьому ЄС. Соціальні мережі якнайбільше пасують до необмеженого роздмухування цих тез в найпростіший спосіб. Таким чином, «тиранія каяття» Брюкнера сприяє «веапонізації»

соціальних мереж, адже цей перегляд історії так само підживлюється автократами через проксі-сили в європейських виборних інституціях. Оскільки авторитарні держави розглядають соціальні мережі та інші платформи як поле політичної війни, самозаспокоєність Заходу додатково підживлює лакуни в безпеці інформаційного простору Європи.

Демократичні стандарти накладають обмеження навіть під час війни. Але політики в різних країнах Європи різняться, адже Великобританія, наприклад, інвестує у можливості своїх «offensive information operations», а в ФРН фактично існують лише регуляторні положення, які обмежують соціальні мережі та платформи. В рамках ЄС свідчення про «наступальні» вкрай обмежені — переважно акценти усіх оборонних документів містять посилання на «стійкості» та «спростуванні». Лише деякі акції-відповіді вдається зафіксувати, і їхня кількість поки є неспівмірною з кількістю атак, які безперервно здійснюють авторитарні системи. Один з таких прикладів – випадок 2019-го року, коли StratCom East запустив кампанію в соцмережах для російськомовного населення Балтії з просування успішних кейсів ЄС — щоб відбити наративи Кремля про «загниваючий Захід».

«Веапонізація» соціальних мереж — це виклик, кинутий самим устроєм відкритого суспільства. Євросоюз за останнє десятиліття усвідомив масштаб загрози і зробив суттєві кроки до захисту свого цифрового суверенітету. Попереду — інтеграція цих зусиль у дієву доктрину, своєрідну «цифрову громадянську оборону» за логікою Джина Шарпа. Окрім того, наступним етапом має бути розгортання випрацювання проактивної логіки протидії авторитарним режимам. Від комбінації успішності цих двох складових залежатиме, чи зможуть європейські демократії зберегти контроль над інформаційним простором та соціальними мережами, не поступившись своїми цінностями. Нинішня війна в Європі показала, наскільки важливо вигравати «битву наративів»; Україні це значною мірою вдалося на початку широкомасштабного вторгнення РФ, в тому числі завдяки підтримці ЄС та НАТО. Відтак, рішучі дії в інформаційному

просторі і згуртованість союзників може перемагати відпрацьовані автократами формули впливу.

Висновки до розділу 3

Протягом 2015–2025 років Європейський Союз вибудував комплексну багатовекторну стратегію захисту інформаційного суверенітету. Головним досягненням стала відмова від реактивного гасіння криз на користь системного регулювання. Ухвалення DSA та регламенту щодо протидії терористичному контенту онлайн закріпило суб'єктність ЄС як регуляторної наддержави, здатної примусити глобальні корпорації до відповідальності за безпекові наслідки їхньої діяльності.

Дослідження продемонструвало різноманітність підходів всередині Союзу: від жорсткого правозастосування в Німеччині (NetzDG) та судового захисту виборів у Франції до концепції «суспільного щита» та тотальної медіаграмотності в країнах Балтії. Саме цей синтез силових, правових та освітніх методів дозволяє ЄС формувати гнучку систему захисту, де кожен громадянин стає першою ланкою безпекового контуру.

Разом із тим, використання лише законодавчих обмежень – не дозволяє повноцінно захистити європейських громадян від зовнішніх інформаційних впливів в соціальних мережах. Також окремо варто відзначити, що жорстке регулювання зустрічає опір з боку опозиційних сил та частини суспільства, відкриваючи дискусію про межу цих заборон та потенційну загрозу безпеці персональних даних громадян та основоположних європейських принципів, зокрема, свободи слова.

В цьому контексті застосування теорії Джина Шарпа до сучасного медіаполя дозволяє змінити оптику та розглядати соціальні мережі як один із ключових «стовпів підтримки» демократичного ладу. «Цифрова громадянська оборона» має базуватися на принципі організованої неспівпраці з агресором —

коли суспільство, володіючи навичками критичного аналізу, позбавляє дезінформацію її головного ресурсу (швидкості поширення). Це перетворює оборону з пасивного очікування на активне зміцнення внутрішньої стійкості.

Ретроспективний аналіз праць Едварда Лукаса та сучасні кейси втручань у вибори в межаї ЄС (від Brexit до виборів президента Румунії 2024-го року) підтверджують, що виключно оборонна стратегія призводить до поступового стратегічного відставання ЄС від авторитарних систем. Для збереження європейського безпекового порядку необхідний перехід до проактивної логіки, що включає не лише спростування фейків, а й цілеспрямоване просування власних наративів на територіях та у мережах авторитарних опонентів. Російсько-українська війна стала остаточним доказом того, що соціальні мережі є невід'ємною частиною воєнних операцій. Досвід України у протидії цифровій агресії Кремля є унікальним активом для оборонних доктрин ЄС та НАТО.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та запропоновано розв’язання актуальної наукової проблеми — визначення ролі соціальних мереж як інструменту впливу на політичну стабільність ЄС. Отримані результати дозволили сформулювати наступні положення:

1. Удосконалено розуміння природи соціальних мереж через концепт «веапонізації» (weaponization). Доведено, що мережі трансформувалися у глобальні бази даних, де аналіз «цифрового сліду» користувачів дозволяє ворожим акторам здійснювати прецизійне профілювання та системно руйнувати «стовпи підтримки» демократичного ладу (легітимність, авторитет, довіру). Встановлено, що цей процес перетворює відкритість суспільства на його ключову вразливість.
2. Дістала подальшого розвитку лінгво-комунікаційна парадигма через призму «гострої сили» (sharp power). Обґрунтовано, що авторитарні режими інструменталізують демократичну відкритість для створення ефекту «фасадної демократії». Виявлено, що через імітацію демократичних інститутів та проведення операцій «hack-and-leak» автократії розмивають сутність народовладдя та здійснюють деструктивний вплив на політичну стійкість ЄС.
3. Удосконалено періодизацію безпекової політики ЄС, у межах якої зафіксовано перехід від «економічного ідеалізму» (1990-ті – 2010-ті рр.) до парадигми «стратегічного реалізму». Доведено, що повномасштабне вторгнення Росії в Україну стало остаточним каталізатором визначення соціальних мереж як фронтиру геополітичного протистояння, закріпленого у стратегії «Стратегічного компасу», що потребує перетворення ЄС на активного «постачальника безпеки».
4. Уточнено концептуальні засади «техноавторитаризму» та «алгоритмічної тиранії». Розкрито морально-етичний вимір впливу алгоритмів, що призводить до соціальної атомізації та провокує «моральні паніки». Доведено, що через доктрину «техноoптимізму» приватні корпорації

встановлюють нові поведінкові норми в обхід національних урядів, що веде до ерозії довіри до державних інституцій.

5. Систематизовано та класифіковано типи «цифрової зброї» за характером ураження: інфраструктурна, психологічна, алгоритмічна. Така класифікація дозволяє не лише ідентифікувати загрози, а й розробляти специфічні, пропорційні сценарії відсічі для кожного типу атаки, уникаючи стратегічної невизначеності у кризових ситуаціях.
6. Проведено порівняльний аналіз національних підходів країн ЄС та виявлено засадничі відмінності в їхніх безпекових моделях: від жорсткого юридичного примусу (Німеччина) до моделі «психологічної оборони» (країни Балтії, Швеція). Обґрунтовано, що інтеграція цих підходів у єдиний контур є необхідною умовою життєздатності всього Європейського Союзу в умовах гібридної агресії.
7. Здійснено критичний аналіз правозастосування Акту про цифрові послуги (DSA) та введено поняття «інфраструктурної заплутаності». Доведено, що перехід від добровільних кодексів до жорсткої відповідальності платформ є способом подолання критичної залежності держав від приватної інфраструктури (Amazon, Google, Starlink) та відновлення державного контролю над цифровим публічним простором.
8. Аргументовано неспроможність стратегії «вічної оборони» у цифровому середовищі. На основі адаптації теорії Джина Шарпа доведено легітимне право демократичних держав на проведення активних заходів-відповіді. Обґрунтовано необхідність актуалізації та адаптації досвіду стратегічних комунікацій доби Холодної війни, коли стабільність залежала від здатності держави активно домінувати в інформаційному просторі.
9. Розроблено трирівневу модель «цифрової громадянської оборони». Модель інтегрує: 1) індивідуальну неспівпрацю (медіагігієна як відмова бути провідником ворожих наративів); 2) мережеву солідарність (горизонтальні канали); 3) інституційну готовність демократії (залучення OSINT-спільнот до державних оборонних доктрин).

Отже, майбутнє Європейського Союзу та стабільність демократичного світового порядку залежатиме від спроможності держав опанувати глобальні цифрові платформи, вписавши їх у рамки верховенства права та перетворивши відкритість суспільства з вразливості на перевагу.

СПИСОК ДЖЕРЕЛ

1. Adorno, T., & Horkheimer, M. (1972). *The culture industry: Enlightenment as mass deception* (J. Cumming, Trans.). Herder and Herder.
2. Keyton D. (2019, May 22). *High-tech Estonia votes online in European elections* (D. Keyton, Rep.). Phys.org. https://phys.org/news/2019-05-high-tech-estonia-votes-online-european.html
3. Andreessen, M. (2023, October 16). *The techno-optimist manifesto*. a16z. https://a16z.com/the-techno-optimist-manifesto/
4. Anghel, V. (2025). *Global risks to the EU 2025*. Robert Schuman Centre for Advanced Studies; European University Institute. https://europeangovernanceandpolitics.eui.eu/wp-content/plugins/rscas-global-risks/documents/QM-01-25-018-EN-N.pdf
5. Applebaum, A. (2025, February). The New Rasputins Anti-science mysticism is enabling autocracy around the globe. The Atlantic. https://www.theatlantic.com/magazine/archive/2025/02/trump-populist-conspiracism-autocracy-rfk-jr/681088/
6. Ljungkvist K. (2025, August 13). *Participatory war and its challenges for total defense*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/08/participatory-war-and-its-challenges-for-total-defense
7. Atlantic Council's Digital Forensic Research Lab. (2023, February 24). *Russian War Report: DFRLab releases investigations on Russian info ops*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-dfrlab-releases-investigations-on-russian-info-ops-before-and-after-the-invasion/
8. Bajarūnas, E. (2025, December 2). *The hybrid threat imperative: Deterring Russia before it is too late*. Center for European Policy Analysis (CEPA). https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/

9. Banjo, S., Lung, N., & Lee, A. (2019). *How Hong Kong's leaderless protest army gets things done*. Bloomberg. https://www.bloomberg.com/graphics/2019-hong-kong-airport-protests/
10. Barnes, J. A. (1954). Class and committees in Norwegian island parish. University of London.
11. Barr, J. (2021, May 14). Fox News viewers are getting mixed messages about whether to take the coronavirus vaccine. *The Washington Post*. https://www.washingtonpost.com/media/2021/05/14/fox-vaccine-mixed-message/
12. Barr, J., & Ellison, S. (2023, April 24). Tucker Carlson is out at Fox News after Dominion lawsuit disclosures. *The Washington Post*. https://www.washingtonpost.com/media/2023/04/24/tucker-carlson-leaves-fox-news/
13. Belam, M. (2016, December). We're living through the first world cyberwar – but just haven't called it that. *The Guardian*. https://www.theguardian.com/commentisfree/2016/dec/30/first-world-cyberwar-historians
14. Bell, D. (2019). *The coming of post-industrial society*. In Social stratification (2nd ed., pp. 805–817). Routledge.
15. Berger, P. L., & Luckmann, T. (1966). *The social construction of reality: A treatise in the sociology of knowledge*. Penguin Books. https://amstudugm.wordpress.com/wp-content/uploads/2011/04/social-construction-of-reality.pdf
16. Bhargava, V. R., & Vikram, R. (2020). Ethics of the Attention Economy: The Problem of Social Media Addiction. *Business Ethics Quarterly, 30*(3), 324–349. https://www.researchgate.net/publication/344522964_Ethics_of_the_Attention_Economy_The_Problem_of_Social_Media_Addiction

17. Siedin O, Subarion A. (2024, July 17). *"Doesn't look like democracy": Russian propaganda on elections in France and the UK*. Detector Media. https://en.detector.media/post/doesnt-look-like-democracy-russian-propaganda-on-elections-in-france-and-the-uk
18. Boyd, D. M. (2007). Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210–230.
19. Beauchamp-Mustafaga, N., Green, K., Marcellino, W., Lilly, S., & Smith, J. (2024, October 1). *Dr. Li Bicheng, or How China Learned to Stop Worrying and Love Social Media Manipulation*. RAND. https://www.rand.org/pubs/research_reports/RRA2679-1.html
20. Braghieri, L., Levy, R., & Makarin, A. (2022). Social Media and Mental Health. *American Economic Review*, 112 (11): 3660-93. https://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.20211218
21. Bruckner, P. (2010). *The tyranny of guilt: An essay on Western masochism* (S. Rendall, Trans.). Princeton University Press.
22. Bryant, M. (2022, February 6). Sweden returns to cold war tactics to battle fake news. *The Guardian*. https://www.theguardian.com/world/2022/feb/06/sweden-returns-to-cold-war-tactics-to-battle-fake-news
23. Bryant, L. (2019, July 4). French lawmakers debate controversial bill to crack down on online hate speech. *VOA News*. https://www.voanews.com/a/europe_french-lawmakers-debate-controversial-bill-crack-down-online-hate-speech/6171094.html
24. Buholcs, J., Tetarenko-Supe, A., Torpan, S., Kõnno, A., Vorteil, V., Balčytienė, A., & Kasparaitė, R. (2024, May). *The regulation of fact-checking and disinformation in the Baltic states* (Deliverable D3.4). BECID Project; University of Tartu. https://becid.eu/results_and_studies/the-regulation-of-fact-checking-and-disinformation-in-the-baltic-states/
25. Caldwell, B., Murphy D. M., & Menning, A. (2009). Learning to leverage new media: The Israeli defense forces in recent conflicts. *Military Review*.

26. Callais, J., Harris, C., & Borchard, B. (2022). The moral costs of markets. *Journal of Economic Behavior & Organization, 204*, 200–220. https://doi.org/10.1016/j.jebo.2022.10.007
27. Carlson, T. [@TuckerCarlson]. (2023, June 7). *Ep.1* [Video attached] [Tweet]. Twitter. https://twitter.com/TuckerCarlson/status/1666203439146172419
28. Castells, M. (2000). *The rise of the network society*. Blackwell Publishers.
29. Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication, 1*, 238–266. https://ijoc.org/index.php/ijoc/article/view/46
30. Castells, M. (2011). *The rise of the network society* (2nd ed.). Wiley Blackwell. https://books.google.co.uk/books?id=FihjywtjTdUC&printsec=copyright#v=onepage&q&f=false
31. Clingendael. (2022, December). *Realising the EU hybrid toolbox*. https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf
32. Code of Practice on Disinformation. (2018). *European Commission*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation
33. Council of the European Union. (2022). *A Strategic Compass for a stronger EU security and defence*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
34. Council of the European Union. (2022, June 21). *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*. https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/
35. Council of the European Union. (2014). *Conclusions on the EU policy on cyber defence*. https://www.european-cyber-defence-policy.com/

36. Ciuriak. D. (2022, June 15). *Social media warfare is being invented in Ukraine*. CIGI. https://www.cigionline.org/articles/social-media-warfare-is-being-invented-in-ukraine/

37. Digital Services Act. (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

38. Drozdiak, W. (2019, February 4). *Europe's challenges in an age of social media and AI*. Hoover Institution. https://www.hoover.org/research/europes-challenges-age-social-media-advanced-technologies-and-artificial-intelligence

39. EEAS. (2023). *1st EEAS report on foreign information manipulation and interference threats*. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf

40. EEAS. (2025, March). *3rd EEAS report on foreign information manipulation and interference threats*. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

41. Elder, M. (2012, May 13). Russian protests: Thousands march in support of Occupy Abay. *The Guardian*. https://www.theguardian.com/world/2012/may/13/russian-protests-march-occupy-abay

42. EPRS. (2023, November). *EU space strategy for security and defence* (PE 753.929). https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754598/EPRS_BRI(2023)754598_EN.pdf

43. Erdos, P., & Renyi, A. (1960). On the evolution of random graphs. *Public Math Institute, 5*, 17–61.

44. EU DisinfoLab. (2022, September 27). *Doppelgänger: Media clones serving Russian propaganda*. https://www.disinfo.eu/publications/doppelganger-media-clones-serving-russian-propaganda/

45. European Centre for Press and Media Freedom. (2025). *Press freedom at risk: The democratic cost of the EU's chat control proposal*. https://www.ecpmf.eu/press-freedom-at-risk-the-democratic-cost-of-the-eus-chat-control-proposal/

46. European Commission. (2018, April 26). *Communication from the Commission: Tackling online disinformation: A European Approach* (COM/2018/236 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

47. European Commission. (2018, December 5). *Action Plan against Disinformation* (JOIN/2018/36 final). https://commission.europa.eu/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en

48. European Commission. (2019, October 9). *EU-wide coordinated risk assessment of 5G networks security*. https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

49. European Commission. (2020, September 10). *First baseline reports – Fighting COVID-19 disinformation monitoring programme*. https://digital-strategy.ec.europa.eu/en/library/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme

50. European Commission. (2020, December 5). *European Democracy Action Plan: Making EU democracies stronger*. https://ec.europa.eu/commission/presscorner/detail/ga/ip_20_2250

51. European Commission. (2022, November 10). *EU policy on cyber defence* (JOIN/2022/49 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022JC0049

52. European Commission. (2022). *About the Digital Markets Act.* https://digital-markets-act.ec.europa.eu/about-dma_en

53. European Parliament. (2025, October). *Eurobarometer 3592: Media and News Survey 2025*. https://europa.eu/eurobarometer/surveys/detail/3592

54. European Parliament & Council of the European Union. (2021, May 17). *Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:172:FULL&from=EN

55. European Union. (2024, June 13). *Artificial Intelligence Act*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

56. Evans, R. J. (2012, August 23). *Merchant, Soldier, Sage: A New History of Power* by David Priestland – review. *The Guardian*. https://www.theguardian.com/books/2012/aug/23/merchant-soldier-sage-priestland-review

57. Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

58. Foy, H. (2021, July). «An overdose of freedom is lethal to a state». *Financial Times*. https://www.ft.com/content/1324acbb-f475-47ab-a914-4a96a9d14bac?syn-25a6b1a6=1

59. Freedom House. (2018). *The rise of digital authoritarianism*. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

60. Freedom House. (2024). *The struggle for trust online: Freedom on the Net 2024*. https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online

61. Galeotti, M. (2018, March 5). I'm sorry for creating the Gerasimov doctrine. *Foreign Policy*. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

62. Galeotti, M. (2022). *The weaponisation of everything: A field guide to the new way of war*. Yale University Press. https://dokumen.pub/the-weaponisation-of-everything-a-field-guide-to-the-new-way-of-war-9780300265132.html

63. Google Threat Analysis Group (TAG). (2025, February). *M-Trends 2025: Special report on global cyber threats*. https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

64. Government Offices of Sweden. (2018, February). *Swedish statement at the UN Security Council*. https://www.government.se/statements/2018/02/swedish-statement-at-the-unsc-open-debate-on-the-purposes-and-principles-of-the-charter-of-the-un/

65. Government Offices of Sweden. (2023, February). *Government action against disinformation campaign*. https://www.government.se/press-releases/2023/02/government-taking-strong-action-against-disinformation-and-rumour-spreading-campaign/

66. Granovetter, M. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380. https://snap.stanford.edu/class/cs224w-readings/granovetter73weakties.pdf

67. *Habermas, J. (1993). The structural transformation of the public sphere. An Inquiry into a Category of Bourgeois Society*. MIT Press. https://arditiesp.wordpress.com/wp-content/uploads/2015/01/habermas_structural_transf_public_sphere.pdf

68. Hale, A. (2009). Moreno's sociometry. *Eastern Group Psychotherapy Society, 33*(4), 347–358. https://psychodrama.org.nz/wp-content/uploads/MorenosSociometry-AnnEHale.pdf

69. Harari, Y. N. (2018, October). Why technology favors tyranny. *The Atlantic*. https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/

70. Harold, S. (2020, January 13). China's footprint in Europe. *Rand Corporation*. https://www.rand.org/blog/2020/01/chinas-footprint-in-europe.html

71. Heath, T. R. (2019, March 7). Public Evidence of Huawei as a Cyber Threat May Be Elusive, but Restrictions Could Still Be Warranted. *Rand Corporation*. https://www.rand.org/blog/2019/03/public-evidence-of-huawei-as-a-cyber-threat-may-be.html

72. Hellman, M., Olsson, E.-K., & Wagnsson, C. (2016). EU armed forces' use of social media. *Media and Communication, 4*(1), 51–62. https://doi.org/10.17645/mac.v4i1.336

73. Howard, P. N., Duffy, A., Freelon, D., Hussain, M. M., Mari, W., & Mazaid, M. (2011). *Opening closed regimes: What was the role of social media during the Arab Spring? Project on Information Technology and Political Islam (PITPI)*. https://download.ssrn.com/15/04/16/ssrn_id2595096_code1148721.pdf

74. Huba, J., & McConnel, B. (2012). *Citizen marketers: When people are the message*. Lewis Lane Press.

75. Huntington, S. P. (1993). *The third wave: Democratization in the late twentieth century*. University of Oklahoma Press. https://books.google.com.ua/books?id=6REC58gdt2sC&printsec=frontcover&hl=uk#v=onepage&q&f=false

76. Huawei Cyber Security Evaluation Board. (2018). *Annual report 2018*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

77. Human Rights Watch. (2018, February 14). *Germany: Flawed social media law*. https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

78. Janda, J. (2016). *The "Lisa case": StratCom lessons for European states* (Working Paper No. 10/2016). Federal Academy for Security Policy (BAKS). https://www.baks.bund.de/en/working-papers/2016/the-lisa-case-stratcom-lessons-for-european-states

79. Javadi, M. (2025, November 25). Infrastructural entanglement and cloud hyperscalers in contemporary warfare: Insights from Ukraine, Israel and Taiwan. *Contemporary Security Policy, 47*(2), 469–506. https://doi.org/10.1080/13523260.2025.2593247

80. Jeangène Vilmer, J.-B., Escorcia, A., Guillaume, M., & Herrera, J. (2018). *Information manipulation: A challenge for our democracies*. Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs; Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

81. Juncker, J. C. (2017, September 13). *State of the Union Address 2017*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

82. Johnson, B. (2008, January 31). Faulty cable blacks out internet. *The Guardian*. https://www.theguardian.com/technology/2008/jan/31/internet.blackout.asia

83. Joint Research Centre. (2024, October 25). *Misinformation and disinformation: Debunking work*. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/misinformation-and-disinformation-both-prebunking-and-debunking-work-fighting-it-2024-10-25_en

84. Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014, June 2). Experimental evidence of emotional contagion through social networks. *PNAS, 111*(24), 8788–8790. https://doi.org/10.1073/pnas.1320040111

85. Kuzio, T. (2017). *Putin's war against Ukraine: Revolution, nationalism, and Crimea*. Chair of Ukrainian Studies, University of Toronto.

86. LaFrance, A. (2020, January 25). Hillary Clinton: Zuckerberg is «Trumpian» and «authoritarian». *The Atlantic*. https://www.theatlantic.com/politics/archive/2020/01/hillary-clinton-mark-zuckerberg-is-trumpian-and-authoritarian/605485/

87. LaFrance, A. (2021, September 27). The largest autocracy on earth. *The Atlantic*. https://www.theatlantic.com/magazine/archive/2021/11/facebook-authoritarian-hostile-foreign-power/620168/

88. LaFrance, A. (2024, January 30). The rise of the techno-authoritarians. *The Atlantic*. https://www.theatlantic.com/magazine/archive/2024/03/facebook-meta-silicon-valley-politics/677168/

89. Law Library of Congress. (2025, January). *Digital Services Act implementation in selected EU member states* (LL File No. 2025-024007). https://tile.loc.gov/storage-services/service/ll/llglrd/2025291250/2025291250.pdf

90. Lucas, E. (2015). *Cyberphobia: Identity, trust and security*. Bloomsbury.

91. Lucas, E., & Pomerantsev, P. (2016). *Winning the information war: Techniques and counter-strategies to Russian propaganda in Central and Eastern Europe*. Center for European Policy Analysis. https://www.lse.ac.uk/iga/assets/documents/arena/archives/winning-the-information-war-full-report-pdf.pdf

92. Macron, E. (2018, August 27). *Speech by the President at the Conference of Ambassadors*. Élysée. https://www.elysee.fr/en/emmanuel-macron/2018/08/27/speech-by-the-president-of-the-french-republic-at-the-conference-of-ambassadors

93. Marche, S. (2012, May). Is Facebook making us lonely? *The Atlantic*. https://www.theatlantic.com/magazine/archive/2012/05/is-facebook-making-us-lonely/308930/

94. Martin, J., Schoenbach K. (2016, April). Predictors of blogging activity in six Arab countries. *The International Communication Gazette, 78*, 733–754. https://www.researchgate.net/publication/301539341_Predictors_of_blogging_activity_in_six_Arab_countries

95. McBrien, T. (2020, December). *Defending the vote: Estonia creates a network to combat disinformation, 2016–2020*. Innovations for Successful Societies, Princeton University. https://successfulsocieties.princeton.edu/sites/g/files/toruqf5601/files/TM_Estonia_Election_FINAL%20edited_JG.pdf

96. McFaul, M. (2018). *From Cold War to hot peace: An American ambassador in Putin's Russia*. Houghton Mifflin Harcourt.

97. Mei, E. (2021). Youth-led activism in Hong Kong. *UCLA Undergraduate Research Journal, 18*, 148–166. https://escholarship.org/uc/item/0rz4v54g

98. Meyers, Z. (2023, April 20). *Will the DSA save Europe from disinformation?* CER. https://www.cer.eu/insights/will-digital-services-act-save-europe-disinformation

99. Ministère de l'Économie (France). (2022). *Le refus de communiquer le code de déverrouillage*. https://www.economie.gouv.fr/daj/le-refus-de-communiquer-le-code-de-deverrouillage-dun-telephone-portable-peut-constituer-un

100. Mueller, R. (2019, March). *Report on the investigation into Russian interference*. USDOJ. https://www.justice.gov/archives/sco/file/1373816/download

101. Murray, S. (2017, July 20). Beijing's new national intelligence law: From Defense to Offense. *Lawfare*. https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense

102. NATO Allied Command Transformation. (2025). *Cognitive warfare*. https://www.act.nato.int/activities/cognitive-warfare/

103. NATO Allied Command Transformation. (2025, November). *Cognitive Warfare Newsletter*. https://www.act.nato.int/wp-content/uploads/2025/11/20251105_CogWar-Newsletter_November.pdf

104. NATO Joint Warfare Centre. (2025, December). Digital transformation at JWC. *The Three Swords, 41*. https://www.jwc.nato.int/wp-content/uploads/2025/12/issue41_Art2_DigitalTransformationJWC.pdf

105. NATO Strategic Communications Centre of Excellence. (2024, May 20). *The Doppelganger Case: Assessment of Platform Regulation on the EU Disinformation Environment.* https://stratcomcoe.org/publications/the-doppelganger-case-assessment-of-platform-regulation-on-the-eu-disinformation-environment/304

106. Neudert, L.-M., & Marchal, N. (2019). *Polarisation and the use of technology in political campaigns and communication* (PE 634.414). European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf

107. O'Donnell, C. (2011, September 12). *New study quantifies social media in Arab Spring*. https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/

108. Office of the Director of National Intelligence. (2017, January 6). *Assessing Russian activities and intentions in recent US elections*. https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-filesations-ica-2017-01.pdf

109. Patrikarakos, D. (2017). *War in 140 characters*. Basic Books.

110. Pew Research Center. (2022, December 6). *Social media seen as mostly good for democracy across many nations, but U.S. is a major outlier*. https://www.pewresearch.org/global/2022/12/06/social-media-seen-as-mostly-good-for-democracy-across-many-nations-but-u-s-is-a-major-outlier/

111. Pew Research Center. (2024, January 31). *Social media use in 2024*. https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/

112. Pingen, A. (2022, June 22). *The strengthened Code of Practice on Disinformation*. eucrim. https://eucrim.eu/news/the-strengthened-code-of-practice-on-disinformation/

113. Polyakova, A., & Fried, D. (2019). *Democratic defense against disinformation 2.0*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf

114. Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models*. Foreign Policy. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

115. Priestland, D. (2012). *Merchant, soldier, sage: A new history of power*. Penguin UK. https://www.google.com.ua/books/edition/Merchant_Soldier_Sage/sNJ1-qK1GUIC?hl=uk&gbpv=1&dq=inauthor:%22David+Priestland%22&printsec=frontcover

116. Psychological Defence Agency (Sweden). (2025). *Mandate and mission*. https://mpf.se/psychological-defence-agency/about-us/our-mission

117. Raban, D., & Gordon, A. (2011). The information society. *Information Communication and Society, 41*. https://www.researchgate.net/publication/263266148_THE_INFORMATION_SOCIETY

118. Rankin, J. (2018, May 16). *Mark Zuckerberg to give evidence at European parliament*. The Guardian. https://www.theguardian.com/technology/2018/may/16/mark-zuckerberg-facebook-to-give-evidence-at-european-parliament

119. Reagan, G. (2009, July 13). The evolution of Facebook's mission statement. *Observer*. https://observer.com/2009/07/the-evolution-of-facebooks-mission-statement/

120. Recorded Future. (2021, August 17). *Operation Secondary Infektion continues targeting Europe*. https://www.recordedfuture.com/research/secondary-infektion-targeting-democratic-institutions

121. Repucci, S., & Slipowitz, A. (2020). *Democracy under lockdown: The impact of COVID-19 on the global struggle for freedom*. Freedom House. https://freedomhouse.org/report/special-report/2020/democracy-under-lockdown

122. Reuters. (2022, March 2). *EU bans RT, Sputnik over Ukraine disinformation*. https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/

123. Reuters. (2025, June 10). *Russian MPs back new state messaging app to combat WhatsApp and Telegram.* https://www.reuters.com/technology/russian-mps-back-new-state-messaging-app-combat-whatsapp-telegram-2025-06-10/

124. Reuters Institute for the Study of Journalism. (2024). *Digital News Report 2024*. University of Oxford. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf

125. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Profile Books. https://books.google.com.ua/books?id=lWltDwAAQBAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false

126. Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., Radin, A., Magnuson, M., & Migacheva, K. (2018, April 5). *Modern political warfare: Current practices and possible responses*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1772.html

127. Rollins, J. (2011, March 8). *Terrorist Use of the Internet: Information Operations in Cyberspace*. CRS. https://www.files.ethz.ch/isn/127746/158490.pdf

128. Rossbach, N. (2017, November) *Psychological Defence: Vital for Sweden's Defence Capability*. FOI. https://www.foi.se/rest-api/report/FOI%20MEMO%206207

129. Sharp, G. (1973). *The politics of nonviolent action*. Porter Sargent.

130. Sharp, G. (1985). *Making Europe unconquerable*. Ballinger.

131. Sharp, G. (1990). *Civilian-based defense: A post-military weapons system*. Princeton University Press.

132. Simon, F., & Camargo, C. (2021, July 20). Autopsy of a metaphor: The origins, use and blind spots of the «infodemic». *New Media & Society, 25*(8), 2219–2240.

133. Singer, P. W., & Brooking, E. T. (2016, November). War goes viral. *The Atlantic*. https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/

134. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Eamon Dolan Books.

135. Smeltzer, M. (2023, August 10). Autocrats' favorite word? Democracy. *Freedom House*. https://freedomhouse.org/article/autocrats-favorite-word-democracy

136. Smith J. (2023, October 20). *PLA social media warfare and the cognitive domain*. The Jamestown Foundation. https://jamestown.org/pla-social-media-warfare-and-the-cognitive-domain/

137. Snyder, T. (2018). *The road to unfreedom: Russia, Europe, America*. Tim Duggan Books.

138. Stewart, E. (2019, August 23). How China used Facebook, Twitter, and YouTube to spread disinformation about the Hong Kong protests. *Vox*. https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitterhong-kong-protests-social-media

139. Stoltenberg, J. (2023, April 3). *Pre-ministerial press conference*. NATO. https://www.nato.int/en/news-and-events/events/transcripts/2023/04/03/pre-ministerial-press-conference?selectedLocale=uk

140. Strobel P. (2024, February 27). *Die sozialen Medien im Ukraine-Krieg*. KAS. https://www.kas.de/de/web/die-politische-meinung/blog/detail/-/content/die-sozialen-medien-im-ukrainekrieg

141. Strömbäck, J., & Esser, F. (2014). *Mediatization of politics: Understanding the transformative power of media*. Palgrave Macmillan. https://www.researchgate.net/publication/321485370_Understanding_the_Mediatization_of_Politics_An_Introduction

142. Sundelius, B., & Eldeblad, J. (2023). Societal Security and Total Defense: The Swedish Way. *PRISM, 10*(2), 99–111. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_10-2/prism_10-2_92-111_Sundelius-Eldeblad.pdf

143. Sunstein, C. R. (2017). *#Republic: Divided democracy in the age of social media*. Princeton University Press. https://assets.press.princeton.edu/chapters/s10935.pdf

144. Sweden Ministry of Defence. (2021). *Main elements of the Government bill Totalförsvaret 2021–2025*. https://www.swedenabroad.se/globalassets/ambassader/nederlanderna-haag/documents/government-bill-totalforsvaret-20212025.pdf

145. Swedish Civil Contingencies Agency (MSB). (2012). *Social media in exercises*. https://rib.msb.se/filer/pdf/26375.pdf

146. Swedish Civil Contingencies Agency (MSB). (2015). *Information security – trends 2015*. https://fra.se/download/18.55af049f184e92956c43d89/1531747326149/Trendreport-2015_eng.pdf

147. Swedish Civil Contingencies Agency (MSB). (2019). *Comprehensive cyber security action plan 2019–2022*. https://www.cyberwiser.eu/sites/default/files/Sweden_CyberPlan_March2019.pdf

148. Swinhoe, D. (2024, April 16). The Houthis and the Red Sea: A new risk to subsea cables. *DatacenterDynamics*. https://www.datacenterdynamics.com/en/analysis/the-houthis-and-the-red-sea-a-new-risk-to-subsea-cables/

149. Tofvesson M. (2022). *Defence Against the Dark Arts: Sweden's Psychological Defence Agency. Governance Matters Magazine.* https://www.chandlerinstitute.org/governancematters/defence-against-the-dark-arts-swedens-psychological-defence-agency

150. Tkachuk, N. (2025). *Ukraine as the Frontline of European Cyber Defence: Building Resilience in the Face of Russian Cyber Aggression*. NATO CCDCOE. Tallinn Paper №15. https://www.ccdcoe.org/uploads/2025/07/Tkachuk_N_Tallinn_Paper_15_Ukraine-as-the-Frontline-of-European-Cyber-Defence.pdf

151. Tanner, M. S. (2017). Beijing's new national intelligence law. *Lawfare*. https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense

152. Travers, J., & Milgram, S. (1969). An experimental study of the small world problem. *Sociometry, 32*(4), 425–443. https://doi.org/10.2307/2786545

153. Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. https://www.theguardian.com/world/2007/may/17/topstories3.russia

154. Treyger, E., Williams, H. J., & D'Arrigo, A. (2025, May 23). *Measuring the reach of Russia's propaganda in the Russia-Ukraine War*. RAND Corporation. https://www.rand.org/pubs/research_briefs/RBA3450-2.html

155. Thomas, M. (2020, February 19). *Defeating disinformation threats*. Foreign Policy Research Institute. https://www.fpri.org/article/2020/02/defeating-disinformation-threats/

156. Tucker, J., Metzger, M., & Barberá, P. (2014, February 28). *SMaPP Lab data report: Ukraine protests 2013-2014*. NYU Social Media and Political Participation (SMaPP) Lab.. (2014). *Ukraine Protests 2013-2014*. Social Media Lab, NYU. https://csmapnyu.org/assets/publications/2014_02_28_Ukraine_Protests.pdf

157. Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press. https://d-nb.info/124031910X/34

158. Van Bavel, J. J., Robertson, C. E., del Rosario, K., & Rasmussen, J. (2023, October). Social Media and Morality. *Annual Review of Psychology*, *75*, 431-458. https://doi.org/10.1146/annurev-psych-022123-110258

159. Volokh, E. (2021). Social media platforms as common carriers? *Journal of Free Speech Law, 1*(1), 377–450. https://www.journaloffreespeechlaw.org/volokh6.pdf

160. Vosoughi, S., Roy D., Aral S. (2018, March 9). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

161. Wagstyl, S. (2016, December 29). Germans detect hand of Russia as cyber war escalates. *Financial Times*. https://www.ft.com/content/cff20452-c1fb-11e6-9bca-2b93a6856354

162. Walker, C., & Ludwig, J. (2017). *Sharp power: Rising authoritarian influence*. NED. https://www.ned.org/wp-content/uploads/2017/12/Introduction-Sharp-Power-Rising-Authoritarian-Influence.pdf

163. Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. *Nature, 393*(6684), 440–442. https://doi.org/10.1038/30918

164. Wilson, L. (2017). Understanding the appeal of ISIS. *New England Journal of Public Policy, 29*(1), 1–10. https://scholarworks.umb.edu/nejpp/vol29/iss1/5/

165. Wolff, L. (1994). *Inventing Eastern Europe: The map of civilization on the mind of the Enlightenment*. Stanford University Press.

166. Wyne, A., & Harold, S. (2020, January 13). China's footprint in Europe. *Rand Corporation*. https://www.rand.org/blog/2020/01/chinas-footprint-in-europe.html

167. Zakharchenko, A., Maksimtsova, Y., Iurchenko, V., Shevchenko, V., & Fedushko, S. (2019). Under the conditions of non-agenda ownership: Social media users in the 2019 Ukrainian presidential elections campaign. CEUR Workshop Proceedings. https://arxiv.org/abs/1909.01681

168. Zannettou, S., Caulfield, T., Bradlyn, B., De Cristofaro, E., Stringhini, G., & Blackburn, J. (2019). *Characterizing the use of images in state-sponsored information warfare operations by Russian trolls on Twitter*. Proceedings of the 13th International Conference on Web and Social Media (ICWSM). https://arxiv.org/pdf/1901.05997

169. Zhang, S., Li, M., Wang, X & Gao, K., (2017). A survey on information diffusion in online social networks: Models and methods. *Information, 8*(4), 118. *IEEE Access*. https://www.mdpi.com/2078-2489/8/4/118

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

197. Андерсон, Б. (2001). *Уявлені спільноти*. Критика.

198. Бауман, З. (2016, 2 лютого). *Соціальні мережі – це пастка* (Г. Грабовська, реф.). *Збруч*. https://zbruc.eu/node/47024

199. Барановський, Ф. (2017). Вплив засобів масової комунікації на політичну стабільність суспільства. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України, 5*(61), 160–173. https://ipiend.gov.ua/wp-content/uploads/2018/07/baranovskyi_vplyv.pdf

200. Безверха, А. О., та ін. (2021). *Впливи у цифровому просторі: План для України* (Звіт). https://ufss.com.ua/wp-content/uploads/2021/06/UFSS_countering_influence.pdf

201. Бокрош, Л. (2015). *Регрес: Відкочування реформ в Угорщині після обнадійливого початку.. Велике перородження уроки перемоги капіталізму над комунізмом*. Інститут міжнародної економіки Пітерсона http://kyiv-heritage-guide.com/sites/default/files/%D0%90%D0%A1%D0%9B%D0%A3%D0%9D%D0%94%20-%20%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%B5%20%D0%BF%D0%B5%D1%80%D0%B5%D1%80%D0%BE%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%202014(2015)%20320%D1%81.pdf

202. Буено де Мескіта, Б. (2024). *Винайдення влади. Королі, папи і розквіт Заходу*. Лабораторія.

203. Віднянський, С. В., & Мартинов, А. Ю. (2009). *Об'єднана Європа: від мрії до реальності. Історичні нариси про батьків-засновників Європейського Союзу*. Інститут історії України НАН України.

204. Гаврилюк, Г. І. (2010). Результати третьої хвилі демократизації: можливі варіанти та інтерпритації. *Вісник НЮУ імені Я. Мудрого, 5*.

205. Гончар, М. (Уклад.). (2017). *Війни XXI: Полігібресія Росії*. Центр глобалістики «Стратегія XXI». https://geostrategy.org.ua/storage/app/public/files/nodes/1/book/1/Xa8si15867659506KcE7.pdf

206. Гончар, М. В. (2023). Вплив соціальних мереж на політичну стабільність та національну безпеку: досвід Королівства Швеція. *Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методики викладання соціально-політичних дисциплін, 33*, 54–63. https://enpuir.udu.edu.ua/entities/publication/bf3f2944-179a-4200-ada6-8e4e152e2239

207. Гончар, М. В. (2024). Вплив соціальних мереж на політичні системи у контексті суперництва демократичних та авторитарних режимів. *Політикус, 5*, 11–18. http://dspace.pdpu.edu.ua/bitstream/123456789/21502/1/Social%20networks%20impact%20on%20political%20systems%20in%20the%20context%20of%20the%20democratic%20and%20authoritarian%20regimes%20competition.pdf

208. Гончар, М. В. (2025). Між згодою та спротивом: адаптація теорії Джина Шарпа для протидії цифровим загрозам у Європейському Союзі. *Український політико-правовий дискурс, 17*. https://doi.org/10.5281/zenodo.17839092

209. Грамші, А. (2017). *В'язничні зошити. Вибрані записи*. Вперед. https://shron1.chtyvo.org.ua/Antonio_Gramsci/Viaznychni_zoshyty_Vybrani_zapysy_vyd_2017.pdf

210. Гусєва, Н. Ю., Філіпенко, Л. В., & Герасимович, В. А. (2024). Політична комунікація в епоху цифрових технологій: можливості та ризики для демократії. *Politicus, (5)*, 24–30. https://doi.org/10.24195/2414-9616.2024-5.4

211. Давидюк, М. (2018). *Як працює путінська пропаганда*. Vivat.

212. Данько, А. (2015). Соціальні мережі у протестних акціях. *Сучасне суспільство, 28*. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=cuc_2015_1(1)__6

213. Детектор медіа. (2019, 20 березня). *Як працює Rapid Alert System — система протидії фейкам від Єврокомісії*. https://ms.detector.media/media-i-vlada/post/22635/2019-03-20-yak-pratsyuie-rapid-alert-system-systema-protydii-feykam-vid-ievrokomisii/

214. Дзьобань, О. П., & Мануйлов, Є. М. (2015). Віртуальні комунікації: до проблеми філософського осмислення сутності. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія, 3*, 7–19. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vnyua_2015_3_3

215. Європейська Комісія. (2024). *План дій щодо цифрової освіти 2021-2027*. https://education.ec.europa.eu/focus-topics/digital-education/actions/plan

216. Європейська правда. (2017, 14 березня). *У Німеччині схвалили штрафи до 50 млн євро за фейкові новини в соцмережах*. https://www.eurointegration.com.ua/news/2017/03/14/7063007/

217. Кондратенко, О. Ю., & Верховцева, І. Г. (2025). Системні особливості іномовлення автократій (кейси РФ, КНР та КНДР). *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право, (1)*(65). https://visnyk-psp.kpi.ua/article/view/332564

218. Корольчук, Л. В. (2019). Сучасні виклики для розвитку світових інтеграційних процесів. *Економічні науки. Серія: Економічна теорія та економічна історія, 16*, 49–58. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA%3D&2_S21STR=ecnet_2019_16_9

219. Кузь, О. М., Потоцька, Ю. І., Застава, І. В., та ін. (2020). *Теорія та історія європейської інтеграції*. ХНЕУ ім. С. Кузнеця. https://repository.hneu.edu.ua/bitstream/123456789/26375/1/2020-%D0%9A%D1%83%D0%B7%D1%8C%20%D0%9E%20%D0%9C%2C%20%D0%9F%D0%BE%D1%82%D0%BE%D1%86%D1%8C%D0%BA%D0%B0%20%D0%AE%20%D0%86%2C%20%D0%97%D0%B0%D1%81%D1%82%D0%B0%D0%B2%D0%B0%20%D0%86%20%D0%92%20%D1%82%D0%B0%20%D1%96%D0%BD.pdf

220. Кундера, М. (2025). *Викрадений Захід, або Трагедія Центральної Європи*. Видавництво Старого Лева.

221. Лукас, Е. (2009). Нова холодна війна. Як Кремль загрожує і Росії, і Заходу (П. Таращук, пер.). Темпора. (Оригінальна робота опублікована 2008) http://search.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

222. Макіавеллі, Н. (2007). *Флорентійські хроніки; Державець*. Фоліо.

223. Мак-Люен, М. (2014). *Галактика Ґутенберга*. Лабораторія.

224. Макнамі, Р. (2020). *Зафейсбучені. Як соцмережа штовхає світ до катастрофи*. Наш Формат. https://nashformat.ua/products/zafejsbucheni-yak-sotsialna-merezha-shtovhae-svit-do-katastrofy-923466

225. Мартинов, А. Ю. (2015). «Пан'Європа» Ріхарда Куденхова-Калергі та започаткування процесу європейської інтеграції. *Європейські історичні студії, 2*, 69–91. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=eis_2015_2_6

226. Моне, Ж. (2017). *Спогади*. Фоліо.

227. Опришко, Д. (2021, 10 червня). *Пошук балансу між правом на свободу вираження та регулюванням соціальних мереж: досвід Німеччини*. Центр демократії та верховенства права https://cedem.org.ua/analytics/sotsmerezhi-nimechchyna/

228. Новакова, О., & Черненко, О. (2023). Розвиток стратегічних комунікацій як засіб боротьби з дезінформацією в українському суспільстві. *Вісник Львівського університету. Серія філософсько-політологічні студії, (49)*, 308–314. https://files.znu.edu.ua/files/2020/scachano/VLUFPS/VLUFPS2023v49/308.pdf

229. Павленко, Д. (2023). Динаміка соціальних медіа в Україні. *Наукові праці НБУВ, 67*. https://nbuviap.gov.ua/images/e_biblioteka/naukovi_resursi/Socialni%20komunikacii/Pavlenko%20D.%20Dinamika%20sucasnih%20socialnih%20media.pdf

230. Перепелиця, Н. (2019). Еволюція геополітичних поглядів Фукуями. *Вісник ЛНУ, 26, 178-185*. https://fps-visnyk.lnu.lviv.ua/archive/26_2019/24.pdf

231. Південна Корея закликає Північ не надсилати пропагандистські листівки через кордон (2020, червень 22). *Радіо Свобода*. https://www.radiosvoboda.org/a/newskndr/30683844.html

232. Померанцев, П. (2020). *Це не пропаганда*. Yakaboo Publishing.

233. Померанцев, П. (2025). *Як виграти інформаційну війну*. Meridian Czernowitz.

234. Проноза, І. І., & Цимбал, С. Ю. (2025). Інформаційна війна в сучасних інтернет-комунікаціях: українсько-європейські практики та виклики. *Politicus, (3)*, 97–102. http://dspace.pdpu.edu.ua/bitstream/123456789/23216/1/Pronoza%20Inna%20Ivanivna.pdf

235. Рамо, Дж. К. (2018). *Сьоме чуття. Влада в епоху мереж*. Наш Формат.

236. Романюк, О. (2009). Чи може демократія бути неліберальною? *Політичний менеджмент, №2*, 73-87. http://nbuv.gov.ua/UJRN/PoMe_2009_2_10

237. Себайн, Дж. Г., & Торсон, Т. Л. (1997). Історія політичної думки (М. Габлевич та ін., пер.). Основи. (Оригінальна робота опублікована 1973). http://litopys.org.ua/istpolit/ipd.htm

238. Стельмах, С. (2023). *Zeitenwende. В республіці страху*. Наш Формат.

239. Тоффлер, О. (1996). *Третя хвиля*. У Сучасна зарубіжна філософія.

240. Україна. Верховна Рада. (2025). *Про основні засади забезпечення кібербезпеки України* (Закон України № 2163-VIII). https://zakon.rada.gov.ua/laws/show/2163-19

241. Фергюсон, Н. (2018). *Площі та вежі*. Наш Формат.

242. Філіпенко, Л. В. (2024). Роль соціальних мереж у війні. *Соціополіс, 1*. https://sociopolis.in.ua/index.php/journal/article/download/5/3

243. Фуко, М. (2020). *Наглядати й карати*. Комубук.

244. Фукуяма, Ф. (2019). *Ідентичність. Потреба в гідності й політика образи* (Т. Сахно, Пер.). Наш Формат.

245. Харарі, Ю. Н. (2018). *21 урок для XXI століття* (О. Дем'янчук, Пер.). BookChef.

246. Чумаченко, Б. М. (2009). *Вступ до культурології античності*. КМА.

247. Шарп, Д. (1993). *Від диктатури до демократії*. https://www.nonviolent-conflict.org/resource/from-dictatorship-to-democracy-a-conceptual-framework-for-liberation-ukrainian/

248. Швеція надає допомогу Україні для боротьби в інформаційному просторі (2023, червень 13). *Європейська правда*. https://www.eurointegration.com.ua/news/2023/06/13/7163568/

249. Шмідт, Е., & Коен, Д. (2015). *Новий цифровий світ*. Літопис.

250. Шуст, Н. Б. (2022). Демократичні концепції та їх зв'язок з брендом країни на міжнародній арені через індекси демократії. *Наукові інновації та передові технології, (6)*(8), 544–551. https://doi.org/10.52058/2786-5274-2022-6(8)-544-551