Завгородня Юлія Володимирівна

Особливості поведінки учасників політичного процесу під час конфронтації в інформаційному просторі

УДК 32.019.5
DOI https://doi.org/10.24195/2414-9616.2022-4.4

Завгородня Юлія Володимирівна
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету
«Одеська юридична академія»
вул. Фонтанська дорога, 23, Одеса,
Україна

Дана стаття є актуальною та практично сконцентрованою в умовах повномасштабного вторгнення агресора на територію України. Досить часто, політичні лідери та особи уповноважені органами влади публічно висловлюються та формують оцінку окремих політичних подій, військових процесів, та окремих видів військово-політичної діяльності. Тим, самим формують базову оцінку подій та реальної політичної дійсності, ґрунтовну ситуацію на фронті та ефективність процесу реалізації поставлених завдань.

Однак, окремі публічні форми інформування є офіційними методами спілкування з протилежною стороною, з метою формування об'єктивності власної позиції, її доцільності та затребуваності у сучасних геополітичних процесах. А разом з тим, і відкритості до перемовин в умовах ескалації у крайньому прояві.

У зв'язку з цим, виникає необхідність дослідження поведінки учасників політичного процесу на стадії активної фази протиборства, яка відбувається в інформаційному просторі, оскільки усі публічні процеси демонструють міру конфронтації та рівень загострення протидії, або навпаки зниження напруги. Метою дослідження є аналіз протиборства в інформаційному просторі суб'єктами політики. Бо саме інформаційний простір є ще одним полем бою, в якому залучені не лише окремі лідери, а й суспільство загалом, яке може формувати індивідуальну позицію.

Для цього під час дослідження було використано, статистичні дані щодо атак на урядові сайти, використання ботів у створенні дезінформації, і як наслідок, деструкція в поведінці населення, також використано компаративістський метод, метод політичного прогнозування та метод спостереження.

Комплекс використаних методів сприяв моделюванню поведінки учасників протиборства в інформаційному просторі в умовах військової агресії на території України. Перемога на фронті може бути основою, для перемоги у кіберпросторі, бо інформаційна пропаганда агресора до звільнення останнього селища буде стверджувати про правильність своїх дій та плановість відступу військ, а не їх поразка. Саме для суспільної психо-емоційної стабільності в умовах війни, з метою зменшення деструктивних новин та їхнього впливу, виникає нагальна потреба у поглиблені політичної грамотності суспільства.

Ключові слова: *конфронтація, політична інформація, поведінка суб'єктів політики, кіберконфлікт, політичне суперництво.*

Вступ. Сучасні наративи про об'єднання суспільства в умовах війни є основою інформаційної політики держави, щодо боротьби проти агресора. Проте, політичній спільноті варто прийняти факт постійної конфронтації, яка залишається у суспільних обговореннях, діях та закликах. Однак, щодо питання перемоги у війні, то дійсно сучасне суспільство у своїй більшості в даному питанні консолідоване. Тому, власне деякі форми конфронтації можуть ставати приводом до консолідації, що власне демонструє демократичну площину, яка відкрита до нових викликів та загроз, які активно розвиваються в інформаційному середовищі паралельно з усталеними політичними процесами.

Сучасні учасники політичного процесу в умовах інформаційної форми взаємодії активно використовують соціальний простір, з метою особистого самоствердження, публічної діяльності в кіберпросторі та комунікації з власною аудиторією, яка розділяє обраний вектор розвитку. Проте, умови міжнародного управління та національної політики в напрямку кібербезпеки в умовах активного використання кіберпростору потребують активного постійного удосконалення та професійного дискутування. А злочини, в кіберпросторі повинні мати окремі санкції статей у національному законодавстві, як галузева злочинна діяльність, яка містить небезпеку, що виникає у кіберпросторі з метою підвищення рівня відповідальності користувачів кібермереж.

Останні пів року повномасштабного вторгнення агресора на територію України продемонстрували серйозні виклики для політичної системи та суспільства. Відбулася криза політичного управління в умовах війни, як отримала прояв у розпаді опозиційних осередків, виїзді політиків за кордон, відсутності відповідальності для політиків за колабораціонізм. Всі ці процеси, в умовах війни консолідували стійке суспільство і політичних суб'єктів, які залишились підтримувати країну в умовах війни. В свою чергу, політична риторика в кіберпросторі та демонстрація діяльності політичних лідерів на досягнення цілі у перемозі ворога та публічної підтримки суспільства зміцнюють дух та стійкість суспільства загалом.

Тому, виникає потреба у деталізації діяльності суб'єктів політики у кіберпросторі в період конфронтації політико-правових процесів, які розви-

ваються у суспільстві та активно проявляються у кіберпросторі.

Мета та завдання. Запропоноване дослідження в сучасному українському суспільстві в умовах військового розвитку політичних процесів зумовлене метою, що акумулює увагу на поведінці суб'єктів політики під час конфронтації в кіберпросторі. Під час аналізу обраної проблематики виділено такі завдання: проаналізувати загрози, які виникали у кіберпросторі між учасниками політичного процесу у зв'язку з низьким рівнем політичної грамотності; розглянути інформаційний вплив на різноманітність політичних поглядів; визначити позитивні та негативні аспекти інформаційної боротьби; спрогнозувати поведінку суспільства під час інформаційних атак політичної спрямованості.

Методи дослідження. Методологічна основа наукового дослідження містить сукупність методів, що сприяють акумулюванню уваги на важливих питаннях та створюють умови для змістовних узагальнень. Для цього, під час аналізу використано статистичний метод, який допоміг побачити сучасний стан кіберактивності та кіберзагроз в умовах війни, що допомагає зрозуміти, які напрямки протиборства популярні у сучасних кібервійнах. В свою чергу метод моделювання, сприяв продемонструвати різні варіанти розвитку політичних подій, з метою зменшення напруги у суспільству та демонстрації глобалізації проблематики, яка назрівала в політико-військовій площині. Також, використано компаративістський метод, що допомагає порівняти різні події, які уже стали центром обговорення та знайшли конструктивний шлях для вирішення, а метод спостереження допоміг показати, що у зв'язку з війною українське суспільство все більше використовує кіберпростір для комунікації для усвідомлення ситуації у країні, тому виникає необхідність в формуванні політичної грамотності.

Результати. Інформаційний простір пронизаний різними новинами, які мають своє завдання для аудиторії споживачів. Існують джерела найбільшого достовірного інформування, які констатують факти без прив'язки до суб'єктивної думки, що допомагають громадянам у формуванні персональних узагальнень про політичні процеси. Однак, є ряд інформації, яка насаджує встановлену думку, що обмежує споживачів у індивідуальних поглядах, або дезорієнтує та вводить в оману.

Усі ці процеси спеціально сформовані та предметно орієнтовані. Так, компанія Meta, яка є власником соціальних мереж Facebook та Instagram офіційно оприлюднила відомості, щодо видалених фальшивих акаунтів, які писали численні коментарі на підтримку російського вторгнення в Україну [1].

Представники компанії зазначають, що « було відключено 45 акаунтів «тролів» у соціальній мережі Facebook і 1 037 – у Instagram. Meta блокує їхні спроби відновити сторінки. «Тролі» працювали щодня «з невеликою перервою на обід», а деякі публікували і проросійські, і проукраїнські коментарі з різницею в кілька хвилин» [1]. Основними цілями такої негативної діяльності ставали офіційні сторінки політиків, журналістів, акторів та комерційних брендів по усьому світі. Тобто, усі, ті хто мав велику популярність в мережах та публічно засуджував російське вторгнення на територію України та висловлював підтримку українській державі та українському народові.

Така діяльність дезорганізує суспільство і після коментарів під постами публічних діячів з критикою створює недовіру та дисбаланс до політичних процесів в цілому. Основним доцільно мудрим рішенням на такі дії є відсутність будь-якої реакції на такі коментарі та суспільно погрозливі пости, як байдужість до такої думки, а найголовніше не розповсюдження її далі у соціальних мережах.

Активно процеси кіберзахисту та кібербезпеки можливо розвивати під час навчання з метою отримання спеціальних знань у сфері кібертехнологій. Так, варто звернути увагу на направленість праць Майкла Деніеля та Джошуа Кенуя, які досліджують особливості обміну інформацією, розвідувальними даними, а найголовніше реагуванням на негативний вплив, який можливий від інформації на окремі країни та суспільство в цілому. Також важливу увагу кіберконфліктам приділили Андреас Хаггманробить, Сінді Вонг, Лорін Б. Вайсінгер, які говорять про небезпеку конфліктного майбутнього і його вплив на соціальному, політичному і технічному рівнях.

Звичайно, сучасна суспільно-політична криза набуває глобального масштабу, а загрози регіонального значення розвивають вплив на глобальні політичні процеси. В українському суспільстві в умовах війни кіберпростір максимально політизований, кожен користувач сучасних гаджетів зайнятий у пошуку інформації, яка містить цікавий факт про ситуацію у розвитку військово-політичних процесів. В умовах історичних, регіональних, політичних, культурних та інших особливостей маніпуляторами використовуються такі кризові аспекти, як: питання мови, питання корупції у лавах ЗСУ та політичних суб'єктів, які використовують ситуацію для збагачення, питання бездіяльності політичних лідерів в окремих військових напрямках, релігійне питання, обговорення політичної освіченості політичних лідерів та інші питання, що суттєво дестабілізують суспільну стійкість до реальності військового стану.

Один із дописів, або відео політичного спрямування може стати основою для подальшого загострення та вчинення актів протидії. В українському законодавстві таку дію визначають, як кіберінцедент. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки Укра-

їни» під кіберінцедентом розуміють «подію або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів» [2].

Яскравим прикладом кіберінцеденту є відео записане президентом рф, щодо початку «спеціальної військової операції» на території України, що слугувало оголошенням кібервійни хакерами Anonymous росії [3]. Таким самим інцидентом до дій може бути публічне звернення того самого президента рф до громадян щодо оголошення часткової мобілізації. Критика та невдоволення уже стають в основі коментарів соціальних мереж, окрім того люди з кіберплощини переходять до фактичних дій у формі мітингів та страйків з метою протистояти рішенням військово-політичного характеру, які не підтримує суспільство [4].

Однак перші прояви невдоволення стають зрозумілі в інформаційній площині, а публічні дії протиборства стають паралельною формою впливу. Боротьба за ідейний шлях розвитку досить просто розтлумачується, однак важко завуальована в політичних посланнях. Тому, для політичних рішень, дій, трактувань важлива об'єктивність та підтримка суспільства. Оскільки від цього залежить шлях розвитку подій від негативних до позитивних.

На думку Пирожкова С. І. та Богуцького Ю.П. «кризовий стан, або біфуркаційний момент суспільства, є одночасно і загрозою, і перспективою для нього. При цьому консолідація суспільства у цей момент передбачає насамперед подолання наявної роз'єднаності людей» [5].

Тобто, криза у спільних поглядах на політичний розвиток між суспільством та діючою політичною елітою формує елемент невідомого, однак саме протиборство шлях до позитивних змін та вдосконалення політичної системи, а найважливіше політичних інститутів.

В умовах виникнення кіберінцеденту щодо політичних подій формується загроза до негативних наслідків діяльності сторони протиборства у кіберпросторі. Негативними наслідками можуть бути: економічні втрати держави через атаки в кіберпросторі; конфронтація дій сторін до форми кібервійни та переформатування у площину змін політичної системи, або її повалення. Позитивними наслідками дій політичного загострення у кіберпросторі є: політичні рішення для зменшення напруги та вичерпання конфронтації по окремих питаннях; удосконалення системи політичної діяльності демократичного режиму.

Однак, наскільки процес протиборства буде розвиватись у позитивному чи негативному напрямку буде залежати бажання сторін до деескалації суспільної напруги. Завдання сторін політичного кіберпротиборства це вчасно відреагувати на політично-суспільну ситуацію, здійснити заходи щодо узгодженої позиції сторін, локалізувати та мінімізувати можливі наслідки кібердіяльності, вчинити попереджувальні заходи на майбутнє щодо інформаційної атаки.

Окрім того, варто розуміти, що отримана інформація стаючи інцидентом до розвитку кіберконфлікту розповсюджується досить швидко та об'єднує велику кількість людей. Якщо звернути увагу на політичний конфлікт, який розвивається у межах парламенту чи окремої політичної партії, його можливо завчасно локалізувати, притягнути окремого політика до політичної відповідальності, або навіть юридичної відповідальності у разі наявності складу злочину.

Проте, в кіберпросторі виконувати дії щодо впливу на сторону протиборства можливо здійснювати неофіційно з новостворених сторінок та з відсутністю будь якої ідентифікації політичної особи. Здійснити будь-яку діяльність щодо притягнення до різних видів відповідальності складно, або взагалі не можливо. Єдиною ключовою основою сучасної кібербезпеки є формування ефективної системи захисту, однак не протидії (нападу). Усі дії щодо нападу відбуваються однак не регламентуються в українському законодавстві, акцент створюють лише на захисті.

Оскільки використання кібервпливу на політиків, на політичну систему стають системними заходами щодо політичної реальності, тому важливу увагу варто приділити реакції суспільства на кіберконфлікті, адже вона може бути зовсім різною. Для покоління похилого віку такі дії взагалі не будуть вважатись чимось серйозним, бо не висвітлені у газетах чи не проговорені на радіо, як основних джерелах інформації. Проте, усі громадяни України, які користуються гаджетами та слідкують за суспільно-політичними подіями на державному та світовому рівні питання конфронтації політичної ситуації дуже хвилює, а кіберконфлікти сприймають як складову політичного процесу.

Висновки. Кіберплощина перенасичена кіберзагрозами політичного спрямування. Основним завданням суспільства та політичної еліти є консолідація дій щодо питань, які стають об'єктом суспільно-політичної кризи та переростають в конфліктну активність та утворюють деструктивні процеси.

Серйозною помилкою стає недооцінювання кіберситуації відносно політичних процесів. Конфронтація у кіберпросторі у сучасному суспільстві є великою силою для суспільного супротиву у реальних діях населення. Лише великі маси здатні вплинути на зміну вектору політичного розвитку. Основні процеси розвитку можуть розпочинатись у кіберпросторі. Тому, для демократичного суспільства важливим завданням є дослухатись до поглядів та коментарів населення, виявляти ботів, які підбурюють суспільство та дискредитують владу та постійно реагувати на суспільні обурення по різним питанням. Адже, українське суспільство дійсно відмінне від населення країни агресора своєю рішучість та швидкістю реакції на політичні процеси, які виходять за межі суспільного сприйняття та законного процесу, що суперечить загальнолюдським принципам існування.

Тому, конфронтація в інформаційному просторі є частиною політичної комунікації в демократичному суспільстві, з метою досягнення консенсусу у прийнятті політичних рішень з урахуванням думки населення. Проте, більшість маніпулятивних питань, які у суспільстві викликали загострені протиріччя з урахуванням військової агресії мають втратити свою актуальність, оскільки стають причиною дій агресора (питання регіональних мов, економічне переформатування бізнесу на європейський ринок, створення системи заходів по боротьбі із диверсійними групами, які спонукають до повалення державності, зміна партійної системи щодо вектору розвитку та ін.).

Отже, системне публічне тлумачення політичних процесів, відкрита взаємодія суб'єктів політики з суспільством, ціннісні демократичні орієнтири – це сучасні першочергові завдання післявоєнної спрямованості українського суспільства та суб'єктів управління для стабілізаційного розвитку політичної системи в оновленій країні.

ЛІТЕРАТУРА:

1. Meta видалила більше 1 000 ботів, які підтримали війну Росії проти України. *LB.ua. дорослий погляд на світ.* 05.08.2022. URL: https://lb.ua/tech/2022/08/05/525424_meta_vidalila_bilshe_1_000_botiv_yaki.html

2. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. *Відомості Верховної Ради України*. № 45. 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Хакери Anonymous оголосили «кібервійну» Росії. Сайти Кремля та Міноборони РФ «лягли». Суспільне новини. 2022. URL: https://suspilne.media/210658-grupa-anonymous-ogolosila-kibervijnu-rosii/

4. У Росії люди вийшли на протести проти мобілізації. Суспільне новини. 2022. URL: https://suspilne.media/284222-u-rosii-ludi-vijsli-na-protesti-proti-mobilizacii-suspilne-videonovini/

5. Україна: шлях до консолідації суспільства: національна доповідь / ред. кол.: С. І. Пирожков, Ю.П. Богуцький, Е. М. Лібанова, О. М. Майборода та ін.; *Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України*. – К. : НАН України, 2017. – 336 с.

6. Живило Є., Черноног О. Міжнародні кібернавчання LOCKED SHIELDS – 2022. Проблемні питання в підготовці складових сил оборони та безпеки України. *Сучасні інформаційні технології у сфері безпеки та оборони.* Том 43 № 1 (2022). URL: file:///C:/Users/38096/Downloads/252774-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-597439-1-10-20220621.pdf

7. A. Ertan (Eds.) Cyber Threats and NATO 2030: Horizon Scanning and Analysis: URL://https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.

8. Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world: URL://https://ccdcoe.org/exercises/locked-shields/

REFERENCES:

1. Meta vydalyla bilshe 1 000 botiv, yaki pidtrymaly viinu Rosii proty Ukrainy. [Meta removed more than 1,000 bots that supported Russia's war against Ukraine] LB.ua. doroslyi pohliad na svit. 05.08.2022. URL: https://lb.ua/tech/2022/08/05/525424_meta_vidalila_bilshe_1_000_botiv_yaki.html [in Ukrainian]

2. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» [About the main principles of ensuring cyber security of Ukraine] № 2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy. № 45. 2017. Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian]

3. Khakery Anonymous oholosyly «kiberviinu» Rosii. Saity Kremlia ta Minoborony RF «liahly». [Hackers Anonymous declared a "cyber war" on Russia. The websites of the Kremlin and the Ministry of Defense of the Russian Federation "went down"] Suspilne novyny. (2022) URL: https://suspilne.media/210658-grupa-anonymous-ogolosila-kibervijnu-rosii/ [in Ukrainian]

4. U Rosii liudy vyishly na protesty proty mobilizatsii. [In Russia, people protested against mobilization] Suspilne novyny. 2022. Rezhym dostupu : https://suspilne.media/284222-u-rosii-ludi-vijsli-na-protesti-proti-mobilizacii-suspilne-videonovini/ [in Ukrainian]

5. Ukraina: shliakh do konsolidatsii suspilstva: natsionalna dopovid [Ukraine: the path to the consolidation of society: a national report]/ red. kol.: S. I. Pyrozhkov, Yu.P. Bohutskyi, E. M. Libanova, O. M. Maiboroda ta in.; Instytut politychnykh i etnonatsionalnykh doslidzhen im. I. F. Kurasa NAN Ukrainy. – K. : NAN Ukrainy, 2017. – 336 s. [in Ukrainian]

6. Zhyvylo Ye., Chernonoh O. Mizhnarodni kibernavchannia LOCKED SHIELDS – 2022. Problemni pytannia v pidhotovtsi skladovykh syl oborony ta bezpeky Ukrainy. [International cyber training LOCKED SHIELDS – 2022. Problematic issues in the training of the components of the defense and security forces of Ukraine.] Suchasni informatsiini

tekhnolohii u sferi bezpeky ta oborony. Tom 43 № 1 (2022). URL: file:///C:/Users/38096/Downloads/252774-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-597439-1-10-20220621.pdf [in Ukrainian]

7. A. Ertan (Eds.) 2022. Cyber Threats and NATO 2030: Horizon Scanning and Analysis: URL:// https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf. [in English]

8. Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world. 2022. URL://https://ccdcoe.org/exercises/locked-shields/ [in English]

Features of the behavior of participants in the political process during the confrontation in the information space

Zavgorodnya Yuliia Volodymyrivna

Candidate of Political Science, Associate Professor,
Associate Professor at the Department of Political Theory
National University «Odesa Law Academy»
Fontanska doroha str., 23, Odesa, Ukraine

This article is relevant and practically concentrated in the conditions of a full-scale invasion of the aggressor on the territory of Ukraine. Quite often, political leaders and persons authorized by the authorities publicly express themselves and form an assessment of certain political events, military processes, and other types of military-political activity. Thus, they form a basic assessment of events and real political reality, a thorough situation at the front and the effectiveness of the process of implementing the set tasks.

However, certain public forms of information are official methods of communication with the opposite party, with the aim of forming the objectivity of one's own position, its expediency and demand in modern geopolitical processes. And at the same time, openness to negotiations in conditions of escalation in extreme manifestation.

In this regard, there is a need to study the behavior of participants in the political process at the stage of the active phase of confrontation, which takes place in the information space, since all public processes demonstrate the degree of confrontation and the level of exacerbation of opposition, or on the contrary, a reduction of tension. The purpose of the study is to analyze the struggle in the information space by political subjects. Because the information space is another battlefield, in which not only individual leaders are involved, but also society in general, which needs to form its position and bear responsibility for it.

For this, statistical data on attacks on government websites, the use of bots in the creation of disinformation, and as a result, destruction in the behavior of the population, the comparativist method, the method of political forecasting and the method of observation were used.

The set of methods used contributed to the modeling of the behavior of the participants in the confrontation in the information space in the conditions of military aggression on the territory of Ukraine. Victory on the front can be the basis for victory in cyberspace, because the information propaganda of the aggressor before the liberation of the last village will assert the correctness of his actions and the planned retreat of the troops, and not their defeat. It is for social psycho-emotional stability in the conditions of war, with the aim of reducing destructive news and their influence, that there is an urgent need for in-depth political literacy of society.

Key words: *confrontation, political information, behavior of political subjects, cyber conflict, political rivalry.*