Руцький Сергій Васильович

Конфронтація взаємодії суб'єктів політики в інформаційному просторі

УДК 32.019.5
DOI https://doi.org/10.24195/2414-9616.2023-5.12

Руцький Сергій Васильович
аспірант кафедри політичних наук і права
ДВНЗ «Південноукраїнського національного педагогічного університету
імені К. Д. Ушинського»
вул. Старопортофранківська, 26, Одеса, Україна
ORCID: 0009-0008-2420-9745

Науковий напрям досліджуваної теми затребуваний викликами сьогодення. Трансформаційні процеси в цифровий простір стають щоденною діяльністю із залученням великої кількості громадян, які активно підтримують сучасні тренди у різних галузях суспільно-політичного розвитку. Катаклізми, які переживає людство також внесли корективи у форму людського спілкування, а тому суб'єкти політики вимушено перелаштувались до сучасного спілкування в інформаційному просторі, яке стало швидкою формою політичної комунікації.

Однак, певні публічні механізми спілкування з іншими учасниками політичного процесу стали офіційними формами спілкування. В такому спілкуванні основною метою є публічне підтвердження об'єктивності власної позиції, її аргументованості у сучасних політичних процесах. Разом з тим, і латентності окремих проявів політичної агресії щодо опонента.

У зв'язку з цим, актуальним є дослідження щодо конфронтаційної поведінки суб'єктів політичного процесу на стадії безпосереднього протиборства, яке відбувається в інформаційному просторі, адже усі публічні процеси демонструють ступінь небезпеки та потребу у протидії, або навпаки зниженні інформаційної активності, як ознаки суспільної байдужості щодо об'єкта протиборства. Метою дослідження є структурно-функціональний аналіз протидії в інформаційному просторі суб'єктами політики. Адже саме інформаційний простір є «полем бою», в якому приймають участь не лише політичні лідери, а й суспільство в цілому, що формує ефект не передбачуваності щодо наслідків.

З метою деталізації небезпек від конфліктних процесів в кіберпросторі використовувались статистичні дані атак на політичну систему, використання ботів у реалізації дезінформації, і як наслідок, дисбаланс в оцінці населенням політичних процесів, також застосовано компаративістський метод, метод спостереження та метод політичного прогнозування.

Сукупність використаних методів допомогла виявити недоліки та перспективи щодо врахування інформаційного простору в політичних процесах. Інформаційна пропаганда політичного опонента в кіберпросторі, демонструє сучасну реальність та оцінку політичних процесів в світі. Оскільки, суспільство активно розвивалось та швидко обмінювалось інформацією в інформаційному просторі виникла нова форма для психологічного впливу на сприйняття політичних процесів. Тому, виникає потреба в дослідженні політичних процесів в інформаційному просторі та поглиблення цифрової політичної грамотності політиків та громадян.

Ключові слова: *конфронтація, інформаційна політика, поведінка суб'єктів політики, кіберконфлікт, політичне суперництво.*

Вступ. У сучасній системі протиборства відбувається зростання ролі кіберсфери у конфронтації політичних суб'єктів, що здійснило зміни у реальній військовій справі та значно переформатувало спосіб взаємодії суспільства в мережі інтернет. Структура і зміст взаємодії на полі бою змінюються у світлі розвитку подій. Зміни форми конфліктної взаємодії суб'єктів політики в кіберплощину відбулися нещодавно, тому важко оцінити повноту знань про сучасні аспекти протиборства.

Експерти назвали конфронтацію в кіберпросторі «крутими війнами» через технології інформаційного простору. Кажуть, що конфронтаційні процеси відображають мінливу динаміку міждержавних взаємодій у світі після холодної війни. Держави не хочуть і не можуть взаємодіяти у відверто жорстокий спосіб, але повинні стримувати свої дії краще аніж в звичайному політичному конфлікті, що робить ці протиборства не холодними чи гарячими, а прохолодними. Особливість новітніх можливостей інформаційного простору полягає в тому, що структура, зміст і розташування взаємодій на полі бою суб'єктів протиборства змінилося у світлі цих подій.

На сучасному етапі досліджень варто відзначити, що найбільш популярний один метод кіберзлочинства, а саме відмова в обслуговуванні (DDoS), яка впливає на динаміку конфлікту та співпрацю між державами. Ефект — це погіршення відносин як інструмент зовнішньої політики.

Політична конфронтація крізь призму міжнародних відносин є суттєвою складовою сучасних відносин. Політичні протиріччя між державами спрямовані на вирішення питань у сфері зовнішньої політики. Такими питаннями можуть бути аспекти щодо етносів їх статусу, територій та ідентифікації груп населення, які активно обговорюються на розвиваються через інформаційний простір.

Мета та завдання. Запропоноване дослідження в політичному процесі сучасного світу в умовах загострення військових процесів зумовлене метою, яка звертає увагу на поведінці суб'єктів політики під час конфронтації в інформаційному просторі. Під час деталізації обраної

проблематики окреслено такі завдання: проаналізувати загрози, які виникають у інформаційному просторі перед суб'єктами політичного процесу; розглянути вплив інформації на різновекторність політичних поглядів; визначити роль інформаційної боротьби для суспільно-політичної свідомості; визначити орієнтири для глобального світу, щодо попередження негативного впливу інформаційної конфронтації політичної спрямованості.

Методи дослідження. Методологічна складова наукового дослідження актуалізованої теми містить ряд методів, які допомагають привернути увагу до суспільно-важливих питань та створюють умови для ефективних висновків. Тому, під час дослідження використано статистичний метод, він допоміг усвідомити сучасний стан конфронтації та кіберзагроз в інформаційному просторі, що створює умови для кібернетичного прояву небезпеки у формі кібервійни. Також метод моделювання, продемонстрував різні шляхи розвитку політичних процесів, для зменшення напруги у суспільстві та прояву проблематики в інформаційному середовищі, яка має вплив на політико-військові процеси. Разом з тим, використано порівняльний метод, що аналізує різні події, які уже продемонстрували суспільне обговорення з конструктивним варіантом вирішення, а метод спостереження показав, що українське суспільство використовує інформаційний простір для комунікації та розуміння політико-військової ситуації у країні, тому виникає потреба у визначення ролі політичної грамотності в періоди конфронтації в інформаційному просторі.

Результати. Питання того, як державні та недержавні суб'єкти використовують кібероперації разом із іншими засобами примусу підняло важливі питання щодо інструментів стратегічних переваг у майбутніх конфліктних процесах. Це важливі питання, щодо яких бракує наукового чи політичного консенсусу. Частина проблеми полягає в тому що базова технологія є новою, постійно розвивається та публічно не висвітлюється, що створює складні умови. У багатьох випадках вчені вдаються до використання концепцій з попередніх епох, таких як стратегічне ядерне стримування, і застосування їх до кібероперацій, хоча це підхід має значні обмеження [5]. Інформаційна конфронтація значно відрізняється від традиційних «кінетичних» війн: вона не включає пряму силу, не (поки що) руйнує у звичайному сенсі слова, і її важко віднести до конкретних акторів [5].

Ще більше плутанини викликає те, що програмісти та інженери, які знають технології, як правило розуміють науку, але не політику, тоді як політики розуміють політику, але практично не звертаються до науки. Ці виклики ускладнюють пошук кваліфікованих експертів або адекватну підготовку служби безпеки фахівців в інформаційному просторі; вони також призвели до розробки поганих продуктів кібербезпеки та гальмували створення чітких політичних і військових доктрин щодо кібервійни [13].

У більшості випадків питання щодо нових доктрин і технологій можна вирішити шляхом випробувань і помилок в реальному світі. Це особливо актуально у сфері кібербезпеки приватного сектора; компанії постійно інвестують і адаптуються, щоб запобігти загрозам або, якщо їх експлуатують через попередню невідому вразливість, швидко реконструювати атакуючий код і створити захист. Цей метод дозволяє доктринам і технологіям безпеки швидко й послідовно коригуватись й адаптуватись до нових викликів [3].

Однак у сфері конфронтації міждержавної політики таке рішення є недоцільним, оскільки не вирішить конкретної проблеми, а лише місцево знешкодить. Держави можуть дозволити собі розкіш пристосуватися до кібершпигунства та одноразових подій, але такий підхід недостатньо реалізує політиків до їх потенційної ролі, яку кіберподії можуть зіграти в повністю скоординованій військовій кампанії. Масштабні політичні чи військові події, такі як криза великої держави чи війна, передбачають низку динамічних, здебільшого непередбачуваних факторів. Знаючи, як це зроблять держави та інші політичні актори використовувати кіберпотенціал під час криз і конфліктів складно, тому що відсутня достатня кількість «випадків» таких подій [2].

Проблема в тому що в кіберпросторі важко персоналізувати учасників, тому саме по цим причинам важко зрозуміти кінцевих замовників або учасників. Зрозуміло, що сторін протиборства є мінімум двоє, особливість їх дій в тому, що інші учасники можуть залучатись самостійно до такої форми конфлікту в кіберсередовищі лише через власне ставлення та відношення до такого типу конфлікту. Якщо деталізувати кіберконфлікти для політичних процесів на територіях постадянських країн, то учасниками політичної конфронтації є: суб'єкти політики, громадяни, підприємства, кіберфахівці. Суб'єкти політики можуть створювати публічні висловлювання щодо кіберборотьби, пересічні громадяни висловлюють власну позицію намаючись видати свою власну позицію за об'єктивну для більшості, а кіберфахівці вчиняють заходи щодо кіберзахисту, кібербезпеки та кібератак на опонента [6].

Політична конфронтація розпочинається ідентично звичайному конфлікту, а саме з інциденту, як першопричині зародження протидії сторін. Причинами прояву інциденту можуть бути: політичні рішення, висловлювання, дії (нормативні акти, які не підтримуються суспільством, дії політиків, які дискредитують себе, як політичних акторів). В свою чергу такі суспільні процеси як: питання мови, релігії, корупції стають тригерами етноконфліктів [6].

Політичне загострення дій суб'єктів політики по своїй суті небезпечні адже масштабами не контрольовані, бо кіберпростір не обмежує територіальні рамки країн. Визначити ступінь небезпеки для держави чи суспільства напевно нереально, оскільки все залежить від сторін конфлікту та об'єкта протиборства, тобто власне за що відбувається боротьба, як основна мета конфронтації. «За даними дослідження IBM Global Average Data Breach, у 2022 році глобальні втрати даних від кібератак становили 4,4 мільйона доларів, порівняно з 4,2 мільйона у 2021 році та 3,9 мільйона доларів у 2020 році» [7].

Звичайно, політика держав на пострадянському просторі в питаннях кібервзаємодії повинна бути чіткою та рішучою, навіть якщо питання кібератак ще не відчутно на політичній системі. Як показує практика європейських країн, то переважно реакція на кібератаки відбувається в момент виникнення проблеми, або при аналізі наслідків, які нанесли шкоду суспільству чи органам управління.

Так, на думку А.В. Пехник та Ю.В. Завгородньої «сутність політики міститься у боротьбі за владу та розподіл владних повноважень, а відповідно і бажанням кожного політичного та державного діяча є здобуття, збільшення влади, тоді як політичні партії метою своє діяльності ставлять саме збільшення підтримки серед населення для можливостей збільшення політичної сили, а відповідно і збільшення владних повноважень. Для досягнення таких цілей, і партія, і лідери застосовують ряд політичних технологій, які допомагають підтримувати і навіть збільшувати підтримку серед громадян. Категорія громадян на яких розповсюджують суб'єкти політики свій вплив для підтвердження ефективності власної політичної діяльності» [6].

До прикладу, в Україні, як країні пострадянській, таким самим чином відбувалась реакція на кібернетичні тригери, оскільки після анексії частини територій України розпочались серйозні атаки на банківські установи та сервіси критичної інфраструктури та державні сайти, що спонукало державу до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (2017 року)[1], а також Указом Президента України введено в дію Рішення Ради національної безпеки і оборони України «Про стратегію кібербезпеки України» (2021) [2].

У звязку з цим, «під час використання політичних технологій варто враховувати усі можливі особливості розвитку подій та враховувати усі можливі негативні наслідки та різні напрямки розвитку політичних процесів. Відповідно, до поданої інформації в різних інформаційних ресурсах, в різні регіонах сприйняття може бути інше, а відповідно і рівень підтримки може бути різним» [6].

Тому, важливим завданням для усіх учасників інформаційного простору, які не сформували єдиної політики у суспільстві щодо політичних процесів та мають протистояння в політичній площині, необхідно звернути увагу на сферу кіберзахисту, а саме: нормативне регулювання, суспільне обговорення, роз'яснення небезпеки використання піратських сайтів, створення захисту для власних пристроїв, які допомагають користуватись кіберпростором а найважливіше реальні види відповідальності за злочини в кіберпросторі.

Висновки. З розвитком суспільства розвивається система управління, а відповідно і розвиваються різновиди конфліктів. За останні п'ять років (через пандемію та повномастабну війну) велика частина комунікаційних процесів трансформувалась в кіберпростір, тому небезпека та загроза кіберпротиборства стала актуальною, а кіберзагрози реальністю суспільно-політичного буття. Питання кібеконфліктів у протиборстві суб'єктів політики на території пострадянських країн, є серйозною загрозою для великої кількості осіб, які особисто не приймають участь у конфлікті, проте можуть відчути її наслідки.

Щодо міжнародного рівня кіберзахисту, то він знаходиться на стадії теоретичного обговорення з визначенням статегічних завдань. На теперішній час, кожна країна намагається вирішувати це питання індивідуально та звичними для себе методами, як до прикладу Китай закритою внутрішньою системою кібервідносин, та США, як зразок демократичних основ та вільного користування кіберпростором орієнтованим на свідомості громадян з системним підходом щодо захисту громадян в усіх сферах.

Окрім того, у ЄС існує позитивний досвід щодо регулювання кіберзлочинності. Основним документом, на який потрібно звернути увагу й оцінити для вжитку в національному законодавстві, є Директива з мережевої та інформаційної безпеки. Даний документ позиціонує загальний підхід і правила ЄС у сфері кібербезпеки. Він направлений на активізацію співпраці з кібербезпеки між країнами ЄС.

Тому, сучасним інформаційним країнам потрібно чітко визначатись з вектором подальшого розвитку та виходити на міжнародний рівень кібербезпеки для ефективного захисту в кіберпросторі. Україна визначивши орієнтири співпраці офіційно приєдналася до Центру НАТО з питань співробітництва в галузі кіберзахисту для максимальної ефективності у кіберзахисті.

Отже, конфронтація суб'єктів політики в інформаційному середовищі несе ряд викликів, які потребують уваги для стабілізаційного розвитку національних політичних систем країн на глобальної системи взаємовідносин.

ЛІТЕРАТУРА:

1. 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

2. Указ Президента України №37/2022 «Про введення в дію рішення Ради національної безпеки і оборони України» від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України». 2021. URL: https://www.president.gov.ua/documents/372022-41289

3. 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.

4. 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/

5. Liudmyla Kormych, Yuliia Zavhorodnia The concept of modern political confrontation in cyber space. *Journal of Cybersecurity*, Volume 9, Issue 1, 2023. URL: https://academic.oup.com/cybersecurity/article/9/1/tyad017/7240366

6. Пехник А.В. Завгородня Ю. В. Сучасні загрози кібертехнологій в політичному процесі. *Актуальні проблеми політики* : зб. наук. пр. Одеса, 2021. Вип. 68. URL: http://www.app.nuoua.od.ua/archive/68_2021/14.pdf

7. Пехник А. В. Допомога Україні від міжнародної спільноти в галузі освіти під час війни: регіональний та глобальний аспекти. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.- практ. конф. (м. Одеса, 19 травня 2023 р.) / за заг. ред. С. В. Ківалова*. Одеса : Видавництво «Юридика», 2023. Т. 1. С. 175-178.

REFERENCES:

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

2. Ukaz Prezydenta Ukrainy (2021) «Pro vvedennia v diiu rishennia Rady natsionalnoi bezpeky i oborony Ukrainy» [On the implementation of the decision of the National Security and Defense Council of Ukraine] vid 30 hrudnia 2021 roku *«Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy».* URL: https://www.president.gov.ua/documents/372022-41289 [in Ukrainian]

3. 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. [in English]

4. 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/[in English]

5. Liudmyla Kormych, Yuliia Zavhorodnia The concept of modern political confrontation in cyber space. *Journal of Cybersecurity*, Volume 9, Issue 1, 2023. URL: https://academic.oup.com/cybersecurity/article/9/1/tyad017/7240366[in English]

6. Pekhnyk A.V. Zavhorodnia Yu. V. (2021) Suchasni zahrozy kibertekhnolohii v politychnomu protsesi. [Modern threats of cyber technologies in the political process] *Aktualni problemy polityky :* zb. nauk. pr. Odesa, 2021. Vyp. 68. URL: http://www.app.nuoua.od.ua/archive/68_2021/14.pdf [in Ukrainian]

7. Pekhnyk A. V.(2023) Dopomoha Ukraini vid mizhnarodnoi spilnoty v haluzi osvity pid chas viiny: rehionalnyi ta hlobalnyi aspekty. [Aid to Ukraine from the international community in the field of education during the war: regional and global aspects]. *Yevropeiski oriientyry rozvytku Ukrainy v umovakh viiny ta hlobalnykh vyklykiv KhKhI stolittia: synerhiia naukovykh, osvitnikh ta tekhnolohichnykh rishen* : u 2 t. : materialy Mizhnar. nauk.- prakt. konf. (m. Odesa, 19 travnia 2023 r.) / za zah. red. S. V. Kivalova. Odesa : Vydavnytstvo «Yurydyka», T. 1. S. 175-178. [in Ukrainian]

Confrontation of the interaction of political subjects in the information space

Rutskyi Serhiy Vasylovych

Postgraduate Student at the Department of Political Sciences and Law
South Ukrainian National Pedagogical University named after K. D. Ushynsky
Staroportofrankivska str., 26,
Odesa, Ukraine
ORCID: 0009-0008-2420-9745

The scientific direction of the researched topic is demanded by today's challenges. Transformational processes in the digital space are becoming a daily activity with the involvement of a large number of citizens who actively support modern trends in various areas of social and political development. The cataclysms experienced by humanity also made adjustments to the form of human communication, and therefore political subjects were forced to adapt to modern communication in the information space, which became a fast form of political communication.

However, certain public mechanisms of communication with other participants in the political process have become official forms of communication. In such communication, the main goal is to publicly confirm the objectivity of one's own position, its argumentation in modern political processes. At the same time, the latency of individual manifestations of political aggression towards the opponent.

In this regard, it is relevant to study the confrontational behavior of the subjects of the political process at the stage of direct confrontation, which takes place in the information space, because all public processes demonstrate the degree of danger and the need for countermeasures, or on the contrary, the reduction of information activity, as signs of social indifference to the object of confrontation. The purpose of the study is a structural and functional analysis of countermeasures in the information space by policy subjects. After all, it is the information space that is a "battlefield" in which not only political leaders participate, but also society as a whole, which creates the effect of unpredictability in terms of consequences.

In order to detail the dangers of conflict processes in cyberspace, statistical data of attacks on the political system, the use of bots in the implementation of disinformation, and, as a result, an imbalance in the population's assessment of political processes, were also used.

The set of methods used helped to reveal the shortcomings and prospects for taking into account the information space in political processes. Information propaganda of a political opponent in cyberspace demonstrates the modern reality and assessment of political processes in the world. Since society was actively developing and rapidly exchanging information in the information space, a new form of psychological influence on the perception of political processes arose. Therefore, there is a need to study political processes in the information space and deepen the digital political literacy of politicians and citizens.

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