УДК 32.341.3

Завгородня Ю. В.
к. політ. наук, доцент,
кафедра політичних теорій,
НУ «ОЮА»,
вул. Фонтанська дорога, 23,
м. Одеса, 65009, Україна
E-mail: julija020890@gmail.com
ORCID ID: http://orcid.org/0000-0003-3500-8638
DOI https://doi.org/10.32782/2707-5206.2024.37.16

КРАУДСОРСИНГ ЯК ПОЛІТИЧНА СКЛАДОВА КІБЕРКОНФЛІКТІВ (КОНЦЕПТ КІБЕРДІЙ УКРАЇНИ ТА АГРЕСОРА)

Дворічна війна для української держави пронизана негативними процесами та трансформацією політичної свідомості. Разом з тим, події які супроводжують цю війну спонукають до оціночних та аналітичних дій з метою розвитку політико-правової дійсності, які переживає весь глобальний світ за ці два роки в кіберпросторі. Одним з актуальних процесів у російсько-українській війні є кібернетичне протиборство як важливий компонент до загальної боротьби, оборони та захисту, який здійснюється не на полі бою, а в цифровому просторі з виходом за межі територіального протікання військових дій. Кіберконфлікт між владою України та росії фактично розпочався задовго до повномасштабного вторгнення у 2014 році, а інтенсивність кібератак віщувала що певні політичні дій чи процеси. За пів року до повномасштабного вторгнення концентрація атак країни агресора збільшилась з геометричною прогресією та стала однією з ознак до підготовки ворога до масштабної війни з захоплення українських земель та кібернетичного простору, управління свідомістю громадян та впливу на політичну систему. Не реалізовані задуми спонукали сторони військово-політичного конфлікту до відшукання нових форм і методик з метою досягнення бажаних результатів. Механізмом до дій в кібернетичному просторі стала краудсорсингова кібервійна, яка дозволила залучати велику кількість талановитих людей, до боротьби у кіберпросторі. Тому, виникає актуальність дослідження такого явища, як питання політичного наслідку для суспільства, держави та глобального світу.
Ключові слова: краудсорсинг, кіберконфлікти, кібердії, Україна, країна агресор.

Постановка проблеми в загальному вигляді, її зв'язок з науковими або практичними задачами. Актуальність теми сформована сучасними політико-військовими діями російсько-українського протистояння у формі кібератак. Проблема краудсорсингової кібервійни для політичної системі криється у дестабілізації інститутів управління, як зовні так і зсередини. Адже, вирішення однієї проблеми провокує небезпеку для майбутнього. Оскільки рішення влади інколи не враховують інтереси окремих регіонів чи верств населення, а тому можлива провокація обурень та протестів. Проте, якщо звичайний мітинг чи протест регулюється нормативно, а тому порушення порядку провокує застосування санкцій, то кібернетичні дії мають волю до дій керуючись лише ідеологічними переконаннями чи нав'язаною політичною думкою, застосування санкційних норм ускладнено, містить політичний підтекст щодо волі до застосування санкцій та відсутність фактичних засобів щодо впливу не на виконавця дій у кіберпросторі, а на замовника.

Аналіз останніх досліджень і публікацій, методологічної основи дослідження. Роль інформаційного простору стрімко зростає і її роль відзначалась ще Кіссінджером Г. до повномасштабної війни в Україні, як складової формування нового світового порядку (Kissindzher, 2020, p. 231). В умовах повномасштабного вторгнення науковці активно розвивають тему кібернетичного протистояння, як загрози нового зразка, яка потребує обговорення, дискусії та нормативного становлення і регулювання. Так, варто підтримати думку авторського колективу Панченко О., Гнатенко В. про те, що «кібератаки, що здійснюються державами чи недержавними акторами, здатні посіяти хаос у країні, що стала їхньою мішенню, тому кібератаки мають бути прирівняні до воєнних злочинів» (Panchenko & Hnatenko, 2023, p. 16). Разом з тим, Хомик Х. вважає, що «Україні вкрай важливо продовжувати надавати пріоритет дискредитації російської пропаганди, дозволяючи своїм громадянам і світовій спільноті формувати добре поінформовану думку на основі точної інформації та протистояти поточним та запобігати майбутнім наслідкам цього руйнівного конфлікту» (Khomyk, 2023, p. 44).

Окрім цього, авторським колективом Завгородньою Ю. та Кормич Л. відзначено, що «інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури піддаються впливу агресора з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності» (Kormych & Zavhorodnia, 2023). Тому, питання кібернетичної площини активно розвивається з формуванням системи заходів по захисті цифровізованих об'єктів, які мають суспільно-важливу роль.

Під час дослідження актуалізованої тематики було використано ряд методів, а саме: статистичний метод, який допоміг побачити математичні показники щодо ролі кіберпротиборства; метод моделювання, продемонстрував позитивні та негативні аспекти краудсорсингової кібервійни, працюючи на перспективу розвитку повоєнних політичних подій; компаративістський метод, що допомагає порівняти різні політичні події, які відбуваються в рамках кібервійни та сигналізують про краудсорсинг в кіберпросторі; метод спостереження допоміг показати, що у зв'язку з конфронтацією та подальшою ескалацією процесів у війні кібернетичні процеси також набувають активного вжитку.

Виділення невирішених раніше частин проблеми, яким присвячується стаття. Усі попередні дослідження в напрямку російсько-української війни демонструють узагальнену картину щодо ролі протиборства інформаційного у війні, проте аналіз окремої форми краудсорсингової кібервійни демонструє високий рівень ескалації, цифрову небезпеку та суспільний дисбаланс, стреси, психологічні розлади. Окрім того, не визначеним залишається питання що буде робити таке велике кібервійсько після фактичного закінчення протиборства та політичного балансу між сторонами конфлікту.

Виділення невирішених раніше частин загальної проблеми, яким присвячується стаття. Формулювання цілей статті. Основною ціллю наукового дослідження є визначення ролі краудсорсингової складової у російсько-українському кіберконфлікті. Адже, дослідження має в політичному процесі завжди акцентувало можливість непередбачуваного розвитку подій. Велика кількість людей об'єднаних ідеологічно в спільних діях досягають бажаного результату коли концентруються в просторі, кількості та часі.

Виклад основного матеріалу дослідження з повним обґрунтуванням наукових результатів. Сучасною формою об'єднання задля реалізації в спільних політичних діях та завданнях можна назвати кіберпроцеси, які мають негативні наслідки для інфраструктури, котра забезпечує ефективне функціонування політичної системи. Російсько-українська війна продемонструвала ряд негативних дій та процесів в кіберпросторі з залученням великої кількості людей, які мають мінімальну кількість знань про комп'ютерний світ, специфіку діяльності та цифровізовані процеси. Цей процес містить накопичувальну систему, адже процеси кібервпливу сторін розвиваються ще з 2014 року. Проте, для країни агресора це явище було актуальне і раніше, але відомостей про краудсорсинг немає, як правило, політичні еліти намагались робити це латентно.

Але, війна в Україні набула не лише матеріального значення (боротьба за українські землі, корисні копалини, матеріальні багатства розвинуті українським суспільством), але й духовно-ідеологічного характеру (боротьба за індивідуалізацію мови, релігії, культури українського народу), що спонукало кожного громадянина розпочати свій фронт боротьби. Як набули загострення процеси російсько-української війни на полі бою, так і загострилися процеси кіберпросторових атак, які проявилися з залученням великих мас людей.

Як відзначають кіберспеціалісти «краудсорсингова кібервійна може набувати різних форм, у тому числі розподілених атак типу «відмова в обслуговуванні» (DDoS), коли сервери цільової мережі переповнені трафіком, що робить їх тимчасово недоступними. Іншою поширеною тактикою є розповсюдження шкідливого програмного забезпечення через фішингові електронні листи або скомпрометовані веб-сайти, що дозволяє зловмисникам отримати несанкціонований доступ до систем і викрасти цінну інформацію. Ці атаки можуть мати далекосяжні наслідки, порушуючи критично важливу інфраструктуру, ставлячи під загрозу національну безпеку та завдаючи економічних збитків»(Kryvenko, 2023).

Яскравим прикладом таких дій є атаки країни агресора на компанію мобільного зв'язку в Україні «Київстар». Як виявилось пізніше, щоб досягти такого результату ворог більше року знаходився в системі компанії і накопичував сили. Такі наслідки лише частина публічно оголошеного впливу, які відчули користувачі мережі. Відчуття цифровізованого дисбалансу в умовах дворічного стресу насправді не мало такого значного ефекту, як планував агресор. Проте, перешкодив певним логістичним та економічним трансферам по країні на один день. Разом з тим, події блек-аутів та ракетних атак створили певні бар'єри психологічного захисту для більшості населення. Це лише створює бажання до відповіді.

Тому, такий затяжний процес війни на території української держави формує таке поняття як «кібервійна з натовпом» що означає практику вербування індивідів з громадськості для прийняття участі в кібератаках від імені організації чи нації. Як правило, такі особи мають володіти відповідними навичками у кодуванні, хакерстві чи інших сферах кібербезпеки. Особи, які приймають участь у кібератаках «мотивовані поєднанням ідеології, патріотизму та фінансових стимулів» (Kryvenko, 2023).

Краудсорсинг (англ, crowdsourcing; crowd – «натовп», sourcing – «підбір ресурсів») – це термін, який вперше введений письменником Джефом Хау та редактором журналу Wired Марком Робінсоном (Howe Jeff, 2009). У сучасному розумінні під даним поняттям варто розуміти: «передача виробничих функцій стороннім виконавцям або виконання інших завдань за допомогою добровільних помічни-

ків, при цьому здійснюється взаємодія із застосуванням сучасних інформаційних технологій; передача певних функцій зі створення споживчих цінностей, а потім, у зв'язку з цим, і інших маркетингових функцій невизначеному колу осіб з числа реальних і потенцій- них споживачів на підставі публічної оферти (пропозиції) з боку фірми-виробника; мобілізація ресурсів людей за допомогою інформаційних технологій з метою вирішення завдань, що стоять перед бізнесом, державою і суспільством загалом; практика отримання необхідних послуг, ідей або контенту шляхом прохань про сприяння, звернених до великих груп людей, особливо до онлайнового співтовариства, на відміну від звичайних співробітників або постачальників» (Maistrenko, 2017, p. 507).

Враховуючи специфіку існуючих визначень даного поняття, може дійти висновку, що краудсорсинг у кібервійні політичного спрямування це залучення правлячими елітами усіх бажаючих талановитих спеціалістів, які використовуються свої ресурси для політичних цілей та завдань, а також з економічним чи/та ідеологічним. Залучення до кіберпротиборства великої кількості людей, сприятиме впливу на кілька цілей одночасно, тим самим збільшуючи їхні шанси на успіх.

Саме російсько-українська війна продемонструвала численні приклади війни в кіберпросторі з використанням краудсорсингу. Так, ще у 2015 році «коли група українських хакерів, відома як «КіберБеркут», здійснила серію DDoS-атак на сайти російського уряду. Ці атаки були помстою за анексію Криму росією та мали на меті порушити їх присутність в Інтернеті. Український уряд публічно визнав і високо оцінив зусилля цих хакерів, вважаючи їх патріотами, які захищають інтереси своєї країни в кіберпросторі» (Kryvenko, 2023).

На противагу таким діям, «росія також прийняла краудсорсингову кібервійну, як засіб для досягнення своїх цілей. Російський уряд заснував ініціативу «Патріотичні хакери», яка вербувала кваліфікованих людей для здійснення кібератак від імені держави. Ці хакери атакували українські державні веб-сайти, засоби масової інформації та критичну інфраструктуру, викликаючи масові збої та посіявши недовіру серед українського населення» (Kryvenko, 2023).

В російсько-українській кібервійні мотиваційний чинник краудсорсингу може містити різні складові. Адже, кібервійна – це складна і багатогранна діяльність, де важко чітко визначити правила поведінки, умови на яких сторони змагаються та роль переконань, які ними керують. Якщо кіберфахівці відносяться до української чи російської кіберармії через приналежність до громадянства чи національності, то основним рушійним чинником їх діяльності є ідеологічні переконання, адже обидві країни працюють над переконанням власного населення щодо цінності патріотичного та ідеологічного чинників у свідомості власного населення. Тому, навіть з метою реалізації окремих завдань в кіберпросторі, кіберфахівці отримують завдання, орієнтири та напрямки до колегіальних атак в кіберпросторі та приступають до їх виконання.

Ще однією складовою мотивації є матеріальний чинник, який допомагає підтримувати таку діяльність та залучати нових фахівців, спеціалістів з незалежних міжнародних організацій. Так, «уряди пропонують винагороди або можливості працевлаштування кваліфікованим хакерам, які сприяють їхнім зусиллям у кібервійні» (Kryvenko, 2023).

Така діяльність дестабілізує систему міжнародно-правових відносин, щодо правил працевлаштування, сплати податкових зборів та фактичного вербу-

вання кіберфахівців, як агентів для блага окремих політичних сил чи країни. Окрім цього, використання фактичної домовленості без нормативних форм взаємодії між урядами та децентралізованими мережами фахівців-хакерів зберігає можливість першим заперечувати причетність до здійснюваних атак. У зв'язку з такою специфікою мобілізація таких кіберфахівців важко визначити приналежність атак до конкретної держави чи політиків, а тому ускладнюється реакція міжнародного співтовариства на процеси ескалації.

Звичайно, що у кіберпротиборстві у російсько-українському конфлікті краудсорсингова війна мала значний вплив, є вигідною для сторін та обмежена у персоналізації кібердій сторін. Проте, протягом двох років повномасштабної війни великі ефективні операції в кіберпросторі навіть стали персоналізувати зі спецслужбами обох країн, демонструючи рівень професіоналізму таких фахівців, які виконують роботу щодо боротьби з кібератаками та кіберзахистом інфраструктури державного значення. Однак, залучення великої кількості фахівців з різних країн та регіонів не оприлюднюється та замовчується з різних причин, а саме:

– в цілях безпеки фахівців, які працюють на країну, яка має інші ідеологічні погляди, як країна громадянином якої є особа;

– в цілях зменшення ризиків щодо збільшення кібератак на країни, які допомагають в кіберборотьбі Україні;

– з метою зменшення ризиків розповсюдження планів щодо кібердій на агресора;

– задля зменшення можливостей підрахунку кібервійська сторонами протиборства;

– з метою зниження інформаційної дезінформації, посилення розколу в країні чи суспільстві, формування атмосфери низького рівня довіри до оточуючих.

Звичайно, що наявність великого кібервійська допомагає підірвати довіру до окремих інформаційних джерел чи комунікаційних платформ, а тому суспільство зменшує свою публічну активність з метою зменшення ризиків щодо можливих форм компроментації або відстеження певних дій. А тому, виникає попит на якісні форми кібербезпеки для політичних суб'єктів в кіберпросторі з метою збереження та захисту цифрових активів, збереження репутації.

Активні атаки та небезпеки, які активізувались в кіберпросторі стали стимулом до розвитку передових технологій щодо кібербезпеки, адже органи управління держав прагнуть відчувати захищеність від суспільних активних груп, які можуть нести небезпеку. Разом з тим, існує низький рівень захищеності для пересічних громадян, адже механізм їх захисту не розроблено, пріоритет це загальносуспільна інфраструктура.

Одну з вирішальних складових у сприянні краудсорсингу для війни в кіберпросторі відіграли платформи соціальних медіа. Адже, саме там можна вербувати осіб для отримання інформації, реалізовувати координацію дій між кіберфахівцями, поширювати пропаганду, яка привертає увагу прибічників такої думки, отримувати зворотній зв'язок у виглядів коментарів та підтримки, розуміючи що тебе можуть помітити на написати особисто.

Окрім того, соціальні мережі допомагають поширити дезінформацію, дозволяючи групам замовників маніпулювати думкою громадян, а однодумцям ділитися ресурсними можливостями, методами і технікою однотипних атак, разом з тим полегшуючи координацію атак.

Так, на думку Кривенко П. «поширеність соціальних мереж у сучасному суспільстві також полегшила урядам пошук потенційних новобранців. Відстежуючи онлайн-активність і аналізуючи профілі користувачів, спецслужби можуть ідентифікувати людей з бажаним набором навичок і ідеологічними пристрастями. Цей цілеспрямований процес набору гарантує, що лише найбільш кваліфіковані та віддані люди будуть відібрані для цих кіберкампаній» (Kryvenko, 2023).

Для того, щоб говорити про можливість впливу на краудсорсингову кібервійну варто враховувати такі аспекти:

– технологічний прогрес;

– міжнародна співпраця;

– інвестування в інфраструктуру кібербезпеки критично важливих систем країнами консолідовано.

Оскільки, повернутись до попередніх варіантів уже не можливо, варто враховувати співіснуванні в кіберпросторі таких дій, а урядові форми впливу можуть сформувати захист для глобальної системи. Цифровізація усіх суспільно-політичних процесів повинна спонукати органи управління до безпеки кіберпростору, комп'ютерної техніки, та розширити знання про соціальні мережі їх можливості та небезпеку серед пересічних громадян.

Висновки дослідження та перспективи подальших досліджень у даному напрямку. Як показує практика саме в зимовий період коли на полі бою відбуваються позиційні бої, а суспільству потрібно надавати певні рівні досягнень, активно використовується кіберпростір у боротьбі та застосуванні краудсорсингової війни.

Тому, краудсорсингова кібервійна – це зростаюче явище, котре трансформує ландшафт для сучасної боротьби. Російсько-українська війна є підтвердженням тощо, що уряди використовують можливості людей, задля того, щоб максимізувати власні кібер-можливості. Тому, що напруженість між державами лише підвищується, очікується, що кількість кібератак з боку натовпу збільшуватиметься.

У зв'язку з цим, міжнародна діяльність щодо колегіального вирішення проблеми кібератак натовпу транснаціонального характеру потребує чітко встановлених вказівок щодо дій урядів у правилах реалізації кіберпротиборства, створення кіберкультури та культури спілкування в соціальних мережах, заохочувати поведінку відповідальних користувачів, створювати перешкоди для протиправних/шкідливих дій. Також, важливо обмінюватись даними розвідки, що стало практикою допомоги в умовах війни в Україні.

Сучасні тенденції щодо реакції на загрозу краудсорсингу для політики та політичних процесів є досить повільна та знаходиться на стадії обговорення та дискусії, проте самі форми комунікації мас удосконалюються та покращуються, а політичні рішення не несуть важливого значення. Наслідки бездіяльності лише спонукають до подальшої ескалації в глобальному масштабі. Небажані наслідки для системи управління, підприємств, установ та організацій можуть лише зростати, а відсутність міжнародної чіткої позиції створює простір нестабільності і невизначеності, де нації самостійно формують порядок ведення кібердій.

В сучасних видатках держав з'являється нова галузь, яка потребує якісного інвестування це кіберпросторова сфера з чіткими правила поведінки міжнародного характеру. Активність краудсорсингової війни залежить від консолідованих зусиль урядів щодо кібербезпеки та моніторингу кіберпросторового порядку.

Новизна дослідження направлена на виявлену небезпеку масштабних хаотичних атак у кіберпросторі, спричинених політичними процесами та рішеннями. Російсько-українське військове протистояння сприяло виявленню в кіберпросторовій діяльності специфічної форми активності з залученням великої кількості людей, які підтримують ідеологічні вподобання сторін конфлікту, без офіційно встановлених відносин з органами управління країнами.

References [Список використаної літератури]

Kissindzher, H. (2020). World order. Reflections on the nature of nations in a historical context. K.: Vyd-vo Nash Format [in Ukrainian]. [Кіссінджер Г. Світовий порядок. Роздуми про характер націй в історичному контексті. К.: Вид-во Наш Формат, 2020. 320 с.]

Panchenko, O., & Hnatenko, V. (2023). Information security in the modern dimension. *Political consequences of the war of the Russian Federation against Ukraine and ways to overcome them: scientific and practical materials. seminar (Kyiv, May 26, 2023)* / edited by G. P. Sytnyk, L. M. Shipilova. Kyiv: Education and Science. University of Publ. example and state services Kyiv. national Taras Shevchenko University, 14–17 [in Ukrainian]. [Панченко О., Гнатенко В. Інформаційна безпека в сучасному вимірі. *Політичні наслідки війни російської федерації проти України та шляхи їх подолання: матеріали наук.-практ. семінару* (Київ, 26 трав. 2023 р.) / за ред. Г. П. Ситника, Л. М. Шипілової. Київ : Навч.-наук. ін-т публ. упр. та держ. служби Київ. нац. ун-ту імені Тараса Шевченка, 2023, С.14–17].

Khomyk, Kh. (2023). Countering disinformation during the Russian Federation's war against Ukraine. *Political consequences of the war of the Russian Federation against Ukraine and ways to overcome them: scientific and practical materials. seminar (Kyiv, May 26, 2023)* / edited by G. P. Sytnyk, L. M. Shipilova. Kyiv: Education and Science. University of Publ. example and state services Kyiv. national Taras Shevchenko University, 43–44 [in Ukrainian]. [Хомик Х. Протидія дезінформації під час війни російської федерації проти України. *Політичні наслідки війни російської федерації проти України та шляхи їх подолання: матеріали наук.-практ. семінару* (Київ, 26 трав. 2023 р.) / за ред. Г. П. Ситника, Л. М. Шипілової. Київ : Навч.-наук. ін-т публ. упр. та держ. служби Київ. нац. ун-ту імені Тараса Шевченка, 2023, С. 43–44].

Kormych, L., & Zavhorodnia, Y. (2023). The concept of modern political confrontation in cyber space. *Journal of Cybersecurity*, Volume 9, Issue 1 [in English]. [Kormych L., Zavhorodnia Y. The concept of modern political confrontation in cyber space. *Journal of Cybersecurity*. 2023. Vol. 9, Is. 1. URL: https://academic.oup.com/cybersecurity/article/9/1/tyad017/7240366 (дата звернення: 27.03.2024)].

Kryvenko, P. (2023). Joint cyber conflict: Russia and Ukraine engage in ground-breaking crowdsourcing. *Cyber security: comments from experts* [in Ukrainian]. [Кривенко П. Спільний кіберконфлікт: росія та Україна беруть участь у новаторському краудсорсингу. *Кібербезпека: коментарі експертів*. 2023. URL: https://cacds.org.ua/ (дата звернення: 27.03.2024)].

Howe, J. (2009). Crowdsourcing: Why the power of the crowd is driving the future of business. *Crown Business* [in English]. [Howe J. Crowdsourcing: Why the power of the crowd is driving the future of business. *Crown Business*, 2009. 336 p.].

Maistrenko, O.V. (2017). Crowdsourcing: essence, types, principles and application tools. *Economy and society,* 9, 507–511 [in Ukrainian]. [Майстренко О. В. Краудсорсинг: сутність, види, принципи та інструменти застосування. *Економіка та суспільство*. 2017. №9. С. 507–511].

Стаття надійшла до редакції 28.02.2024

Zavhorodnya Yu. V.
Department of Political Theories
National University "Odesa Law Academy"
Fontanskaya road str., 23, Odesa, 65009, Ukraine

CROWDSOURCING AS A POLITICAL COMPONENT OF CYBER CONFLICTS (THE CONCEPT OF UKRAINE CYBER AND THE AGGRESSOR)

Summary

The two-year war for the Ukrainian state is permeated by negative processes and the transformation of political consciousness. At the same time, the events that accompany this war encourage evaluative and analytical actions in order to develop the political and legal reality that the entire global world is experiencing in these two years in cyberspace. One of the relevant processes in the Russian-Ukrainian war is cybernetic confrontation as an important component of the general struggle, defense and protection, which is carried out not on the battlefield, but in the digital space, going beyond the territorial flow of military operations.

The cyber-conflict between the authorities of Ukraine and Russia actually began long before the full-scale invasion in 2014, and the intensity of cyber-attacks foreshadowed certain political actions or processes. Half a year before the full-scale invasion, the concentration of attacks by the aggressor country increased exponentially and became one of the signs of the enemy's preparation for a large-scale war to seize Ukrainian lands and cyberspace, control the consciousness of citizens and influence the political system. The unrealized ideas prompted the parties to the military-political conflict to find new forms and methods in order to achieve the desired results. The mechanism for actions in cyberspace was crowdsourced cyberwar, which allowed to attract a large number of talented people to fight in cyberspace. Therefore, there is an urgency to study such a phenomenon as a question of political consequences for society, the state, and the global world.

Key words: crowdsourcing, cyber conflicts, cyber activities, Ukraine, aggressor country.