УДК 321.01
DOI https://doi.org/10.32782/app.v72.2023.6

Ю. В. Завгородня
orcid.org/0000-0003-3500-8638
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»

ІСТОРІЯ СТАНОВЛЕННЯ КІБЕРВІЙНИ ЯК СКЛАДОВОЇ ПОЛІТИЧНОГО ПРОЦЕСУ

Політична взаємодія правлячих еліт відбувається у формі перемовин та домовленостей, проте для ефективного процесу перемовин окремі політичні діячі використовують методи впливу та спонукання сторін конфлікту до прийняття необхідного політичного рішення. Принцип «хто сильніший, той і правий» актуальний і в сучасному використанні, проте з новітньою інтерпретацією сили, оскільки цінності та їх збереження частково відбуваються в кіберформаті. А тому, прояв сили реалізується через кіберпростір на кіберсайти, банківські системи, державні офіційні сайти, критичну інфраструктуру. Тобто, усе що містить певну ідеологічну, культурну чи матеріальну цінність в кіберпросторі стає об'єктом бажаного впливу політичного опонента.

Тривала атака в кіберпросторі з елементами захисту інформаційних систем та протидією опоненту з масштабними наслідками для сторін кіберпротиборства та пересічних користувачів кіберпростором містить назву «кібервійна». Елементи розвитку даного протиборства досить молоді саме 80-ті, 90-ті роки XX ст., проте в якості політичного кіберпротиборства стає зрощуміло з 2000-них років, коли з'являється розуміння вірусів та кібератак. Разом з тим, стрімкий розвиток технологічного прогресу проявляється вдало на політичних процесах та політичному протиборстві.

Сучасна війна між росією та Україною демонструє розуміння цінності інноваційних технологій у боротьбі, демонстрація цифровізації військових дій з метою збереження людського ресурсу, окрім того збільшення атак на сторону противника, з метою суспільно-політичного залякування та нанесення шкоди для державної стабільності.

Тому обрана тема дослідження становлення кібервійни, як складової політичного процесу є досить актуальною та затребуваною викликами сучасності. Окрім того, прогрес цифровізації суспільства робить залежним громадян та державу від кіберпростору у можливостях передачі даних, проведенні транзакцій, швидкості отримання та поширення інформації, що з одного боку створює комфортні умови комунікації в різних суспільно-важливих сферах, з іншого боку провокує ряд небезпек у системі кіберзахисту, як сучасного пріоритету для державної політики.

Наукові дослідження щодо розвитку політичного протиборства в кіберпросторі, активно розвиваються, з акцентом на політико-військові процеси в Україні. Так, дослідниками кіберконфліктів у вітчизняній науці варто відзначити Д. Дубов, В. Жадько, Ю. Завгородня, та інші, а питанням щодо кібервійни, як крайньої форми протиборства в кіберпросторі займались І. Аграфіотіс, Дж. Нурс, М. Голдсміт, С. Гріс, Д. Уптон.

У зв'язку з цим, військові та політичні процеси, які відбуваються в Україні, та кібератаки, які проходять по всьому світі, можуть бути взаємопов'язані та бути залежними від політичних рішень регіонального значення, а в окремих випадках і глобального значення. Закінчення війни в Україні може стабілізувати кібервідносини та стабілізувати акти агресії в кіберпросторі. Тому, виникає необхідність деталізації розуміння кібервійни, як складової політичного процесу на регіональному та глобальному рівні.

На підставі актуальності напрямку дослідження метою обрано систематизацію знань про кібервійну, як вагомий чинник політичного протиборства в кіберпросторі. Для досягнення мети дослідження поставлені такі завдання: розглянути становлення знань про форми кібер-

війни, її специфіку та особливості; охарактеризувати кібервійну, як складову російсько-української війни сучасності; провести аналіз небезпек від кібервійни; оцінити можливості завершення чи врегулювання кібернетичного протиборства. У зв'язку з цим, використано системний метод, кібернетичний метод, аналіз та синтез, історичний метод та прогностичний метод.

Формування знань про небезпеку в інформаційному вимірі цифровізації розпочинається зі створення першого комп'ютерного обладнання, як механізму обміну даними. З періоду коли комп'ютери під'єдналися до Інтернету та почали обмінюватися повідомленнями, кіберзлочинність набула нового значення. Навіть якщо рівень ризику зараз значно вищий, ніж тоді, проте користувачів комп'ютерів хвилювали загрози, які вносили незручності в їх користуванні. Звичайно, кіберризики змінювалися з розвитком технологій. Кіберзлочинці постійно розробляють нові способи доступу до систем і викрадення даних.

Протягом 20-ти років після створення першого цифрового комп'ютера в 1943 році кібератаки було важко здійснювати. Невеликі групи людей мали доступ до величезних електронних машин, які не були об'єднані в мережу, і лише кілька людей знали, як ними керувати, що не створювало загрозу для користувачів. Джон фон Нейман вперше підняв питання щодо можливості самовідтворення комп'ютерних програм у 1949 році, коли вперше була оприлюднена теорія, що лежить в основі комп'ютерних вірусів.

Очевидно, що збір комп'ютерної інформації не був початковою метою злому. Навіть до середини 1960-х років більшість комп'ютерів зберігалися в безпечному середовищі з контрольованою температурою. Доступ залишався обмеженим навіть для програмістів через високу вартість цих громіздких пристроїв. Основний розвиток фрази «злом» припав на 1970-ті роки. Це було спричинено не використанням комп'ютерів, а скоріше тим, що певні особи зламали високотехнологічні потяги, що належать Клубу модельної залізниці MIT Tech. Вони хотіли змінити їхню функціональність. У цьому десятилітті ідея була перенесена на комп'ютери.

Проте, доступ до цих ранніх систем через «хакерство» не здавався «великим бізнесом». Метою цих ранніх хакерських інцидентів було просто отримати доступ до систем. Однак можливостей для політичних чи економічних здобутків не було. Перше хакерство полягало в першу чергу в створенні безладу, щоб перевірити, чи це можливо.

З часом з'явилися нові, швидші та ефективніші методи злому. 1967 рік став одним із найважливіших подій в історії інформаційної безпеки. У 1970-х роках відбувся фактичний початок кібербезпеки. Це було важливе десятиліття в еволюції кібербезпеки. Мережа агентств передових дослідницьких проектів (ARPANET) була першим заходом у цьому. Ця мережа зв'язку була побудована до того, як був створений Інтернет (Bhadwal, 2023).

У 1980-х роках почастішали резонансні атаки, включно з нападами на National CSS, AT&T і Національну лабораторію Лос-Аламоса. У фільмі «Військові ігри» 1983 року шкідливе комп'ютерне програмне забезпечення керує ракетно-ядерними системами, видаючи себе за гру. Терміни «троянський кінь» і «комп'ютерний вірус» стали відомі також в 80-ті роки (Bhadwal, 2023).

У 1990-тих роках відбувається швидкий розвиток, як цивілізаційного становлення інформаційних потоків так і небезпек, які набувають політичної цінності, оскільки коли небезпека глобалізується, а система захисту не ефективна, приходить розуміння потреба політичного впливу у формі міждержавних політичних рішень. Активність кібератак розкривають політизовану сутність таких дій, можливість впливати на політичну еліту та контролювати економічні потоки.

У 2020 році виклики хвороби коронавірусу також сфорвували ще більшу небезпеку для фахівців кіберзахисту. Проте, саме активна військова агресія в Україні розкрила розуміння великої кількості атак вкінці 2021 року, як передвісники початку повномасштабного вторгнення.

Період війни в Україні демонструє не просто підвищення кібератак, а й підвищення масштабів та глобальних форм кіберпротидії. Загострення атак, яке супроводжується політичними діями для стабілізації ситуації. А тому, аналізуючи війну в Україні варто наголосити на тому, що зараз відбувається перша світова кібервійна (Завгородня, 2022, с. 104).

Тому, на думку О. Бекстона «кібервійна – це кібератака або серія кібератак, спрямованих на країну чи державу з метою отримання стратегічної чи військової переваги. Акти кібервійни зазвичай передбачають проникнення в мережі або їх пошкодження, саботаж інфраструктури та порушення діяльності організацій та установ, життєво-важливих для інтересів цільової країни» (Buxton, 2023).

Головною метою кібервійни є послаблення країни шляхом підриву соціальної єдності, політичної стабільності та військово-промислового потенціалу. Незважаючи на те, що межі між кібервійною, кіберзлочинністю та кібертероризмом можуть бути розмитими, кібервійна в першу чергу не мотивується фінансовою вигодою, а здійснюється суб'єктами, пов'язаними з державою.

Кібервійна, яку іноді називають цифровою війною, може включати атаки на: цивільну інфраструктуру , наприклад електромережі або системи управління дорожнім рухом; фінансові установи , такі як банки та кредитні спілки; військові об'єкти , підрядники та інші установи національної безпеки; окремі громадяни країни (Buxton, 2023).

Яскравим прикладом сучасності є діяльність сторін військового протиборства росії та України в кіберпросторі. Росія проводить кібероперації проти України з 2014 року – операції зі збору розвідданих, операції впливу та спорадичні операції низької інтенсивності із підривом української національної інфраструктури. Атаки, що мають відношення до поточної війни, почалися приблизно за півтора місяці до початку наземних боїв.

Так, на початку січня 2022 року США попередили Україну, що її критичні державні інфраструктури знаходяться під загрозою кібератаки. Невдовзі після цього попередження сайти українських міністерств (освіти, внутрішніх справ, закордонних справ та інших) були зіпсовані та розміщені на них повідомлення із застереженнями жителів України щодо Росії. У СБУ тоді заявляли, що в ході нападів нічого не було викрадено. але тести, проведені американськими офіційними особами та корпорацією Майкрософт, виявили віруси в українських мережах, зокрема в критичних інфраструктурах, таких як Міністерство оборони України, об'єкти виробництва електроенергії, ядерні об'єкти та інші. Приблизно за два тижні до офіційного початку кампанії США надіслали експертну допомогу та технологічні рішення для захисту української інфраструктури (Pinko, 2023).

За день до початку повномасштабного вторгнення та в перший день було здійснено багато кібератак на національну інфраструктуру України, державні установи та банківську систему. Здебільшого це були атаки на відмову в обслуговуванні (DoS) і пошкодження веб-сайту. Україна, яка зазнала кібератак на свою електроенергетичну компанію в 2014 році була готова до нинішньої кампанії.

У перші місяці війни агресор неодноразово атакував стратегічні українські цілі та національну інфраструктуру, таку як банківські установи, електричні компанії, ядерні об'єкти та транспортну інфраструктуру, але атаки не вдалися. Росіяни завдали кількох ударів, в основному пов'язаних із видаленням інформації з серверів і комп'ютерів. Російське кіберугруповання під назвою «Армагеддон» атакувало цивільних осіб та організації в Україні, щоб зібрати розвідувальну інформацію про стан внутрішнього сприйняття ситуації, а також іншу інформацію, яка допоможе в наземній боротьбі та зупинці української національної інфраструктури. Більшість російських атак з початку лютого 2022 року по жовтень 2022 року були спрямовані проти державних установ, IT-інфраструктури та енергетичного сектору (Pinko, 2023).

В свою чергу Україна розпочала активно формувати систему захисту з одного боку, а з іншого відповідала вандалізмом на російських урядових веб-сайтах у перші дні війни, створюючи DoS-атаки та намагаючись створити в країні агресора розуміння того, що Україна відповість на російську агресію як у кіберсфері, так і на полі бою.

Публічне звернення Президента України Володимира Зеленського щодо заклику хакерів з усього світу приєднатися до української кіберармії для атаки на російські веб-сайти та інфраструктуру, а також прийняти участь у кампанії кібервпливу є офіційним сигналом кіберборотьби, як сучасного механізму для військових дій. Одними з публічно відомих операцій українців є зламані російські урядові веб-сайти, розсилка на мобільні телефони громадян Росії повідомлень із засудженням війни, злам сайтів російського телебачення та трансляція на них повідомлень та навіть злам сайту Російського космічного агентства. Окрім того, організа-

ція Anonymous стверджує, що проникла та зламала сайт російської державної розвідувальної служби ФСБ. Основною ціллю українських та світових хакерів є бажання вплинути на світову та російську громадську думку, щоб припинити війну (Pinko, 2023).

Загалом, дослідники визначили п'ять ключових напрямків небезпеки, за якими можна класифікувати вплив кібератаки, який ще називають як кібершкода, а саме: фізичний/цифровий; економічний; психологічний; репутаційний; соціальний або суспільний(Agrafiotis, Nurse, Goldsmith, Creese, Upton, 2018).

Враховуючи усе вищезазначене, можемо дійти висновку, що розуміння процесу кіберборотьби та становлення явища кібервійна пройшло своє становлення від теоретичного сприйняття цих процесів, з становленням кібертехнологій, до практичної реалізації в сучасному світі. Зрозуміло, що явище кібервійни це процес набагато складніший, оскільки може реалізуватися невизначеною кількістю кібервійськ, які можуть реалізувати свою діяльність без територіальних обмежень. Тому, в сучасному військовому протиборстві між росією та Україною відбувається паралельна форма протиборства у технологічних можливостях, в яких залучені представники, усіх бажаючих країн, котрі підтримують позиції однієї із сторін конфлікту.

У зв'язку з цим, врегулювання політичного конфлікту, який досягнув своєї крайньої межі можливо на підставі прийняття політичного рішення обома сторонами конфлікту, а от чи закінчиться на цьому етапі кібервійна не можна впевнено стверджувати, адже кібервійсько може діяти без єдиного правителя та керуватися лише внутрішніми переконаннями.

Тому, аналіз історії становлення знань про кібервійну її практичну реалізацію, актуалізують питання подальшого вдосконалення кібербезпеки та кіберзахисту на державному та глобальному рівні. Наскільки швидкий технологічний розвиток, настільки повинен бути швидкий політичний компроміс, щодо врегулювання даного напрямку світової безпеки. Бо трансформація суспільних та політичних процесів в кіберпростір, створення певної залежності від цифровізованих засобів створює небезпеку для стабільного суспільно-політичного устрою в країні та світі.

Література

Akhil Bhadwal The History of Cyber Security: A Detailed Guide. *Blog Author*. 2023. URL: https://www.knowledgehut.com/blog/security/history-of-cyber-security

Завгородня Ю.В. Теоретичне усвідомлення сутності поняття «кібервійна» у політичному просторі. Політичні процеси сучасності: глобальний та регіональні виміри. Збірник матеріалів IV Всеукраїнської науково-практичної конференції (м. Івано-Франківськ, 27-28 жовтня 2022 р.). 2022. С.103-105

Eyal Pinko The Cyber Domain in the Russo-Ukrainian War. *Center for Strategic Studies*. 2023. URL: https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/

Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*. Volume 4, Issue 1, 2018 URL: https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288

Oliver Buxton Cyber Warfare: Types, Examples, and How to Stay Safe. *Academy*.2023. URL: https://www.avast.com/c-cyber-warfare

References

Akhil Bhadwal (2023) The History of Cyber Security: A Detailed Guide. *Blog Author.* URL: https://www.knowledgehut.com/blog/security/history-of-cyber-security [in English]

Zavhorodnia Yu.V. (2022) Teoretychne usvidomlennia sutnosti poniattia «kiberviina» u politychnomu prostori. Politychni protsesy suchasnosti: hlobalnyi ta rehionalni vymiry. [Theoretical awareness of the essence of the concept of "cyber war" in the political space.] *Zbirnyk materialiv IV Vseukrainskoi naukovo-praktychnoi konferentsii* (m. Ivano-Frankivsk, 27-28 zhovtnia 2022 r.). 2022. S.103-105 [in Ukrainian]

Eyal Pinko (2023) The Cyber Domain in the Russo-Ukrainian War. *Center for Strategic Studies* . URL: https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/ [in English]

Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity.* Volume 4, Issue 1, 2018 URL: https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288 [in English]

Oliver Buxton (2023) Cyber Warfare: Types, Examples, and How to Stay Safe. *Academy.* URL: https://www.avast.com/c-cyber-warfare [in English]

Анотація

Завгородня Ю. В. **Історія становлення кібервійни як складової політичного процесу. –** Стаття.

У суспільному вжитку все частіше використовуються такі поняття як: «кібервійсько», «кібератака», «кіберпротиборство» та «кібервійна». Усі ці терміни нерозривно пов'язані з типи процесами, котрі відбуваються в світі, а найважливіше в серці Європи – Україні, яка уже в стані повномасштабної війни знаходиться більше року. Адже, кіберпростір України перший відчув атаки агресора, які розпочались ще за декілька місяців до повномасштабного вторгнення. Тому, тема щодо історії становлення кібервіни відбуває у реальному часі та спонукає політичну та наукову спільноту до роздумів, щодо глобального значення кіберборотьби.

Окрім того, з моменту анексії окремих територій України відбуваються постійні атаки на критичну інфраструктуру, що створило потребу в нормативному становленні кібербезпеки та практичних навиках такої діяльності, відбувається розвиток спеціальностей ІТ- спеціальностей та щороку збільшується набір у даному напрямку, що свідчить на потребу через виклики сучасності.

Історія становлення кібервійни у політичних процесах демонструє стрімкість модернізації інформаційних процесів, їх використання в різних сферах суспільного життя та залежність від політичної діяльності та стабільності політичної системи країни. Існуючих знань про політичну реальність уже не вистачає, оскільки політичні процеси постійно набувають нових форм, а відповідно і нових механізмів до реалізації.

Такою новою формою впливу на політичні процеси є «кіберагресія», яка в крайньому своєму прояві кваліфікується як «кібервійна», котра містить ряд небезпек для глобального простору. Деталізований аналіз становлення та розвитку явища кібервійни з політичним спрямуванням демонструє ускладнення політичних процесів з використанням новітніх форм впливу, що в кінцевому результаті можуть стати не контрольованим процесом.

Ключові слова: кіберпростір, кіберпротиборство, політична взаємодія, кіберконфлікти, цифровізація військових дій, кібервійна.

Summary

Zavhorodnya Yu. V. **The history of the formation of cyber war as a component of the political process. –** Article.

In social usage, such terms as: "cyberarmy", "cyberattack", "cyberresistance" and "cyberwar" are increasingly used. All these terms are inextricably linked with the types of processes taking place in the world, and most importantly in the heart of Europe – Ukraine, which has been in a state of full-scale war for more than a year. After all, the cyberspace of Ukraine was the first to feel the attacks of the aggressor, which began a few months before the full-scale invasion. Therefore, the topic of the history of cybercrime takes place in real time and prompts the political and scientific community to think about the global significance of cyber warfare.

In addition, since the annexation of certain territories of Ukraine, there have been constant attacks on critical infrastructure, which has created a need for the normative formation of cyber security and practical skills for such activities, the development of IT specialties is taking place, and recruitment in this direction is increasing every year, which indicates the need due to the challenges of modernity.

The history of the emergence of cyber warfare in political processes demonstrates the speed of modernization of information processes, their use in various spheres of public life, and their dependence on political activity and the stability of the country's political system. Existing knowledge about political reality is no longer enough, as political processes are constantly taking on new forms and, accordingly, new mechanisms for implementation.

Such a new form of influence on political processes is "cyber aggression", which in its extreme manifestation is qualified as "cyber war", which contains a number of dangers for the global space. A detailed analysis of the formation and development of the phenomenon of cyber war with a political direction demonstrates the complication of political processes using the latest forms of influence, which in the end can become an uncontrolled process.

Key words: cyber space, cyber warfare, political interaction, cyber conflicts, digitalization of military operations, cyber war.