УДК 327
DOI https://doi.org/10.32782/2663-6170/2022.30.10

РОЛЬ НАТО У БОРОТЬБІ З КІБЕРКОНФЛІКТАМИ: ПОЛІТИКО-ПРАВОВИЙ АСПЕКТ

NATO'S ROLE IN FIGHTING CYBER CONFLICTS: POLITICAL AND LEGAL ASPECT

Завгородня Ю.В.,
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національного університету «Одеська юридична академія»

У статті акцентовано роль НАТО в сучасних питаннях безпеки у кіберпросторі. Однією із загроз, що виникає у світі є інформаційна боротьба у формі кіберконфліктів, яка набуває значимості у новітньому політичному протистоянні. Тому, виникає потреба в аналізі механізмів можливої боротьби з негативним наслідком кіберборотьби в політичних процесах.

Сучасний світ демонструє глобалізацію процесів, які мають регіональне значення, проте виникає підтримка або осуд діяльності політичної еліти на міжнародному рівні. Така тенденція координує діяльність політичних груп за допомогою кіберпростору. Сучасний простір інформаційного обміну містить позитивні можливості для суспільства та негативні наслідки, які лавиноподібно звалюються на політичну спільноту в інформаційному просторі у формі «хейту». Для демократичних форм управління політична думка більшості розвивається, в тому числі, через кіберпростір. Тому, аналіз кіберконфліктів в процесах прийняття політичних рішень та розвитку політичних подій є надзвичайно важливим.

Розвинуті країни глобального впливу приходять до думки, що боротися з інформаційними формами впливу важко лише в межах однієї країни, бо під час інформаційних атак політичні опоненти можуть застосовувати «армію» ботів, які займаються розкручуванням проблемного політичного рішення чи виборів політичних лідерів у демократіях.

Північноатлантичний альянс є однією з форм безпекового сектору на наддержавному рівні, а тому науковці та практики звертають свою увагу саме на цю міжнародну організацію, яка продемонструвала прогресивні підходи до сучасного розуміння військової справи та декларує нормативи у формі небезпеки кіберзагроз, що потребують нового сприйняття, а найголовніше нового захисту в інформаційній площині.

В науковому дослідженні деталізовано основи небезпеки кіберконфліктів на суспільство, нормативну реакцію НАТО на сучасні виклики та загрози, пріоритетні напрямки подальшого розвитку захисту кіберпростору від кіберконфліктів.

Ключові слова: НАТО, політичні кіберконфлікти, безпека, кібербезпека, міжнародні організації.

The article emphasizes the role of NATO in modern security issues in cyberspace. One of the threats emerging in the world is the information struggle in the form of cyber conflicts, which are gaining importance in the latest political confrontation. Therefore, there is a need to analyze the mechanisms of a possible fight against the negative consequences of cyber-warfare in political processes.

The modern world demonstrates the globalization of processes that have regional significance, but there is support or condemnation of the activities of the political elite at the international level. This trend coordinates the activities of political groups with the help of cyberspace. The modern space of information exchange contains positive opportunities for society and negative consequences, which fall like an avalanche on the political community in the information space in the form of "hate". For democratic forms of government, the political opinion of the majority develops, including through cyberspace. Therefore, the analysis of cyber conflicts in the processes of making political decisions and the development of political events is extremely important.

Developed countries of global influence come to the opinion that it is difficult to fight informational forms of influence only within the borders of one country, because during informational attacks, political opponents can use an "army" of bots that are engaged in promoting a problematic political decision or elections of political leaders in democracies.

The North Atlantic Alliance is one of the forms of the security sector at the supranational level, and therefore scholars and practitioners turn their attention to this international organization, which has demonstrated progressive approaches to the modern understanding of military affairs and declares norms in the form of the danger of cyber threats, which require a new perception, and most importantly new protection in the information plane.

The scientific study details the basis of the danger of cyber conflicts to society, NATO's normative response to modern challenges and threats, priority directions for the further development of cyberspace protection from cyber conflicts.

Key words: NATO, political cyber conflicts, security, cyber security, international organizations.

Постановка проблеми. Створення північноатлантичного альянсу (НАТО) – це результат боротьби за цінності індивідуальної свободи, верховенства права і демократії. Разом з тим, ця міжнародна організація націлена на мирне врегулювання суперечок, які можуть виникати на глобальному рівні та впливати та суспільно-політичний порядок у світі. Однак, новітні технології демонструють світу виникнення нових видів загроз, які потребують реального дієвого впливу, який має розумні межі, що встановлюються правовими нормами у цивілізованому світі.

Варто відзначити, що НАТО є над державною формою безпеки, яка містить впливові механізми стримування будь-якої форми агресії. Відповідно до статті 1 Північноатлантичного договору «сторони зобов'язуються, як це визначено у Статуті Організації Об'єднаних Націй, вирішувати всі міжнародні спори, учасниками яких вони можуть стати, мирними засобами і таким чином, щоб не ставити під загрозу міжнародний мир, безпеку та справедливість, а також утримуватись у своїх міжнародних відносинах від погроз силою чи застосування сили у будь-який спосіб, несумісний з цілями Організації Об'єднаних Націй»[1]. Однак, у сучасному світі протиріччя, погрози щодо застосування сили, розвиток конфліктної агресії переформатовуються у кіберпростір з використанням кібератак, як передумови до більш небезпечних форм агресії.

Оскільки, у світі залишаються авторитарні правителі, диктатори, «царі сучасного формату», які перебувають довгий період часу у владі, тому виникає проблема збройної боротьби, яка несе найбільшу небезпеку, а саме порушення верховенства права, влади народу, а найголовніше збереження індивідуальної свободи і здоров'я. Адже, сучасний розвинутий світ визначив чітку цінність життя та здоров'я індивіда, бо саме наявність людей формує необхідність існуванні інститутів управління на державному та глобальному рівнях.

Аналіз останніх досліджень і публікацій. Зацікавленість діяльністю НАТО, його впливом на збройні історичні форми протиборства завжди присутня зі сторони наукової спільноти. Окрім того, мова про трансформацію НАТО відбувається завжди, причому для різних цілей. Однією з причин є дискредитація організації, як інституції безпекового сектору у світі. Другою причиною є об'єктивна потреба в модернізації впливу на сучасні суспільно-політичні процеси, як невід'ємна умова стабільності та миру у світі.

На думку О.М. Суходоля важливою складовою, яку останнім часом, яскраво обговорюють в НАТО, є енергетична безпека, яка може стати важелем впливу на країни, які залежні від такого ресурсу[2]. Адже дійсно в сучасному світовому політичному процесі маємо приклади впливу Росії на європейським лідерів формою енергетичного шантажу, щодо їх ролі у війні в Україні.

Окрім того, важливу роль несуть нормативні акти НАТО, які реагують на сучасні проблеми кібернетичного світу та демонструють сучасну проблему інформаційних загроз. Так, у 2021 році Альянс схвалив Комплексну політику кіберзахисту НАТО з метою забезпечення мирного та безпечного кіберпростору[3]. Така діяльність демонструє формування основ кібернетичного захисту, оскільки країни учасники Альянсу відчувають негативний вплив кібератак, які є наслідком політичних рішень та діяльності органів управління.

Нормативна основа розширення спекоту впливу НАТО на кіберпростір регламентована викликами сучасності та необхідністю захисту країн-учасниць від негативного впливу в інформаційній боротьбі. Тому, Альянс проголошує, що кіберпростір відноситься до сфери відповідальності та діяльності НАТО, також Альянс визначає кібероборону основною в сучасному інформаційному світі, а найважливіше, що стаття 5 Північноатлантичного договору поширюється на колективну оборону і кіберпростір загалом [4].

У зв'язку з цим, Кавин С. звертає увагу на формування кібербезпеки для країн Балтії, які формують власні стратегії щодо реагування на різні форми негативного впливу. Автор зазначає, що «технології розвиваються настільки швидкими темпами, що ані політики, ані юристи, ані економісти, навіть ІТ-фахівці просто не встигають за динамікою реальності» [5].

В свою чергу у наших попередніх дослідженнях акцентовано увагу на кіберконфліктах, які є однією з форм небезпечної діяльності у кіберпросторі щодо політичної взаємодії та публічних форм спілкування між суб'єктами політики [6]. Саме кіберконфлікти стають проявом діяльності сторін політичного протиборства в кіберплощині з можливим залученням компетентних безпекових міжнародних організацій для реакції(впливу) на такі негативні явища у глобальному світі. Саме такою міжнародною організацією є НАТО.

Враховуючи особливості актуальності наукового напряму дослідження, питання аналізу ролі НАТО у кіберпросторі займалися науковці щодо забезпечення безпеки у кібернетичному просторі такі: О. Звоздецька, О. Суходоля, В. Бутримас, В. Гвоздь, А. Ковалев, А. Балашов, С. Кавин, S. Dimitrova, S. Stoykov, Y. Kochev та ін.

Виділення невирішених раніше частин загальної проблеми. Питання трансформації НАТО залишається досліджуваним та продовжується пошук наукових висновків в різних аспектах, однак в сучасних політичних процесах важливо звернути увагу на ефективну систему протидії кіберконфліків, в яких НАТО може відіграти ключову регулятивну роль, стабілізувати хаотичні процеси взаємодії суб'єктів політики та сформувати принципи доброчесної діяльності**.**

Формулювання цілей статті (постановка завдання). У зв'язку з суспільно-політичною необхідністю впливу на кіберконфлікти, формується основна мета статті, а саме визначення ролі НАТО у боротьбі з кіберконфліктами враховуючи політичні особливості та нормотворчі аспекти діяльності організації. На підставі мети визначено такі завдання наукового дослідження: дослідити нормативно-правові форми регламентації кібернетичних загроз, конфліктів та кібербезпеки; проаналізувати сучасні форми впливу

НАТО на кіберконфлікти; визначити проблеми та перспективи вдосконалення впливу на кіберконфлікти Північноатлантичним альянсом.

Виклад основного матеріалу дослідження. Кіберконфлікти містять, як регіональне так і глобальне значення. Тому, відповідно і рівень небезпеки їхнього впливу може бути локальний (місцевий) або ж міждержавним, таким що зачіпає інтереси декількох окремих держав, що приводить у дисбаланс політичні системи таких країн. Світова політична еліта прагне створити так званий інформаційний захист на глобальному рівні, адже з великою системою захисту простіше здійснювати боротьбу на місцевому рівні. В науково-публіцистичному рівні виникають думки, щодо ключової ролі НАТО у такій формі боротьби.

З моменту формування інституційних складових даної міжнародної організації людський ресурс складався з професіоналів військових, які могли виконувати та виконували бойові завдання, щодо створення балансу у військових конфліктах, які підкріплялись політичною волею, окремих політичних лідерів. На сучасному етапі розвитку світу все більш частіше вживається та реалізується така діяльність, як «кібервійна», що розуміється як крайня форма кіберконфліктів. Тому, діяльність НАТО з форми безпосередньої військової боротьби паралельно потребує спеціалістів у сфері інформаційного захисту кіберпростору.

Окремі країни світу виділяють значний рівень видатків саме на інформаційну сферу, її захист та комфортне використання людьми, безпеку захисту інформаційних баз даних та збереження стабільності у політичній системі. Суспільства, які стали цифрованими, стають вразливими саме у кіберпросторі. Комфорт людей в таких країн досить високий, однак і рівень небезпеки вищий. Політичний конфлікт в кіберпросторі – це трансформація політичної боротьби за допомогою гаджетів, комп'ютерів та інших технологічних ресурсів, які допомагають «словом» в глобальних мережах впливати на політичні процеси. Коли відбувається вплив інформаційного послання він може супроводжуватись реальними мітингами, демонстраціями, сприяти зміні правлячої еліти та ін.

Діяльність НАТО в питанні кіберзагроз та кіберконфліктів декламує принципи взаємної відповідальності у діяльності усіх членів Альянсу щодо захисту кіберпростору та реакції на можливі публічні загрози. Так, « в контексті Статті 3 Вашингтонського договору, де сказано, що «члени Альянсу будуть підтримувати і розвивати свої індивідуальні і колективні можливості протистояти збройному нападу». Оскільки в цьому просторі неможливо повністю відокремити військові, цивільні і промислові питання, НАТО великою мірою зацікавлена в удосконаленні сил і засобів кіберзахисту організацій, які не належать до оборонного істеблішменту» [7].

Окрім того, усі члени НАТО обмінюються досвідом щодо захисту та впливу на існуючі загрози в кіберпросторі. На підставі чого здійснюють узагальнюючу характеристику загроз та їх негативного впливу в кіберпросторі. Проте, варто відзначити, що сучасна характеристика негативних процесів в кіберпросторі констатується, як кібератаки, або початок військової агресії з метою послаблення органів управління [7].

Звичайно, таке твердження є фактичною формою тих подій, які сьогодні відбуваються в Україні. Коли було здійснено повномасштабний напад збройної агресії зі сторони рф, то одночасно вчинені кібератаки на офіційні сайти багатьох органів управління в Україні. Проте, варто відзначити, що така діяльність уже стала наслідком існуючого конфлікту, в політичній площині між рф та Україною, щодо анексії частини українських територій. Кіберконфлікти стали частиною конфліктної протидії сторін, ще з 2014 року, коли українські банки та державні установи піддавались збою у роботі, кібератакам, що суттєво підривало ефективність політичної влади.

Тому, для аналізу кібератак та захисту від них потрібно розуміти, причинно-послідкові процеси, щодо можливих суб'єктів протиборства, мети такої діяльності, подальших дій сторін та інших аспектів конфліктної активності в кіберпросторі. У зв'язку з цим, конфлікт у кіберпросторі це не лише продовження подій у інформаційній площині, це власне незалежна форма протиборства, яка допомагає здійснювати вплив на процеси управління на регіональному та глобальному рівні.

Під час обговорення Комплексної політики кіберзахисту НАТО 2021 року регламентована чітка позиція щодо «підвищення стабільності й зниження ризику конфліктів, підтримуючи міжнародне право та добровільні норми відповідальної поведінки держави в кіберпросторі»[3].

Яскравим проявом норм права щодо діяльності окремих держав у боротьбі з кіберзагрозами є країни Балтії, які формують систему права, інститутів та механізмів, щодо реалізації кібербезпеки з урахуванням участі даних країн в діяльності НАТО. Варто відзначити, що країни Балтії є прогресивними в сфері інформаційної безпеки, а сучасні інститути управління націлені на створення умов ефективного управління та виконання принципів свободи, демократії та рівності усіх перед законом.

Разом з тим, продовжується співпраця по лінії ОБСЕ та НАТО країнами Балтії щодо інтеграції національних законодавств «в уніфіковану міжнародно-правову платформу з метою зниження ризиків виникнення конфліктів унаслідок використання інформаційно-комунікаційних технологій. Вони визнають взаємозв'язок між сферою кібер- і національної безпеки і усвідомлюють, що проблеми кібербезпеки, такі як руйнування системи інформаційно-комунікаційних технологій

чи критичної інфраструктури, можуть завдати шкоди національній безпеці і функціонуванню економіки держави»[5, с. 319].

Тому, спектр особливостей кіберконфлікту широкий та включає в себе: визначення позитивних аспектів кіберборотьби; здійснення публічного інформування про політичні кризи в кіберпросторі; створення кіберплатформи обговорення конфлікту, який несе політико-інформаційну кризу або навпаки прорив у розвитку та інші аспекти. В системі НАТО деталізується єдиний напрямок – це кібероборона. Коли кіберконфлікт містить небезпеку для членів Альянсу відповідно до ст. 5 Договору.

Висновки та перспективи подальших розвідок у цьому напрямі. Політика НАТО щодо впливу на кіберконфлікт, як нову форму політичного протистояння виражається у системній боротьбі членів Альянсу з кібератаками та фейками. Уваги потребує причинно-наслідковий зв'язок виникнення таких форм протиборства, оскільки саме в об’єкті та суб’єктах кіберпротиборства формується розуміння необхідності впливу на ці процеси.

Нормативна складова декларована НАТО дозволяє формувати існуючі принципи оборонної сфери в кіберпросторі навіть за межами Альянсу, що фактично прирівнюється до норм міжнародно-правових. Звичайно, існують проблеми у загальносвітовому порядку користування кіберпростором, однак у окремому демократичному суспільстві вирішуються важливі питання більшістю, такий принцип актуальний для глобального впливу на виклики.

Інформованість суспільства демонструє нові виклики для системи управління у державі та світі загалом. Міжнародна спільнота об’єднує власні зусилля на нормативному та політичному рівні, що з однієї сторони демонструє свободу для громадян, а з іншої сторони пошук механізмів захисту інформаційної свободи. Міжнародні об’єднання є проявом спільної діяльності окремих націй об’єднаних спільними принципами діяльності та ціннісними орієнтаціями.

Безперечно, питання щодо впливу на кіберконфлікти важливе для українського суспільства. Окрім того, українське суспільство та органи управління в переважній більшості готові до щільної співпраці з НАТО, як безпекової інституції. Тому, важливим залишається питання щодо співпраці України з НАТО з метою попередження та врегулювання конфліктів у кіберпросторі.

З 2018 року Україна уже розпочала будівництво системи оборони кіберпростору від негативних впливів по зразку НАТО, що демонструє ефективний прояв у відбитих атаках нашими фахівцями, які обчислюються у сотнях. Така трансформація є проявом засобу необхідності в умовах, які склалися в державі. Проте, в практичній реалізації завдань українські фахівці демонструють освіченість та прогресивність у можливості реагувати на нові виклики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Північноатлантичний договір. *Вашингтон, округ Колумбія*, 4 квітня 1949 р. URL: https://zakon.rada.gov.ua/laws/show/950_008#Text.

2. Суходоля О.М. Роль НАТО у забезпеченні енергетичної безпеки та захисту енергетичної інфраструктури. *Національна безпека*. №18. 2015. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/rol-nato-v-zabezpechenni-energetichnoi-bezpeki-ta-zakhisti.

3. Лідери країн НАТО схвалили комплексну політику кіберзахисту альянсу. *Інтерфакс-Україна.* 14.06.2021 р. URL: https://ua.interfax.com.ua/news/general/750063.html.

4. Гвоздь В. Кіберконфлікт і геополітика — новий фронт «холодної війни». 28-й *Економічний форум на тему «Європа загальних цінностей або Європа спільних інтересів?»* 05.09.2018 р. URL: https://bintel.org.ua/nash_archiv/arxiv-voyenni-pitannya/arxiv-gibridnia-vijna/09_05_krynica.

5. Кавин С. Нормативно-правові механізми забезпечення кібербезпеки в країнах Балтії. *Підприємство, господарство і право. Міжнародне право.* № 12. 2020. URL: http://pgp-journal.kiev.ua/archive/2020/12/56.pdf.

6. Завгородня Ю.В. Кіберконфлікти, як елемент політичних технологій в інформаційному просторі. *Актуальні проблеми філософії та соціології.* № 32/2021. Видавничий дім «Гельветика». С. 144-148.

7. Роль НАТО в кіберпросторі. *НАТО Ревю.* 12.02.2019р. URL: https://www.nato.int/docu/review/uk/articles/2019/02/12/rol-nato-v-kberprostor/index.html.