Вісник Львівського університету. Серія філос.-політолог. студії. 2023. Випуск 51, с. 230–239
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 51, p. 230–239

УДК 32.341.1
DOI https://doi.org/10.30970/PPS.2023.51.27

ВИКЛИКИ ТА МОЖЛИВОСТІ РЕАЛІЗАЦІЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ НАТО

Олег Цебенко, Ольга Івасечко, Дар'я Хівренко
Національний університет «Львівська політехніка», Інститут гуманітарних і соціальних наук, кафедра політології та міжнародних відносин
вул. Митрополита Андрея, 5, 79013, м. Львів, Україна

У статті наголошено на тому, що сьогодні чимало недемократичних держав розглядають кіберпростір як сферу свого впливу та невід'ємну складову їхньої зовнішньої політики. Встановлено, що такі держави як Російська Федерація та Китай, а також злочинні хакерські угруповання становлять суттєву загрозу для кібернетичної безпеки НАТО. Презентовано нормативно-правову та інституційну базу в галузі кібербезпеки НАТО. Окреслено підхід Альянсу щодо потрактування терміну «кібероборона», який дефініюється як дії Організації, спрямовані на захист власної інформаційно-комунікативної інфраструктури від загроз з кіберпростору. Висвітлено ті загрози в кібепросторі, з якими зіштовхуються сьогодні держави-члени Північноатлантичного Альянсу. Резюмовано, що такі загрози варіюються від застосування кібернетичних атак на критично важливі об'єкти НАТО й атак з політичною мотивацією, до кібершпигунства й кампаній з дезінформації, якими займаються Російська Федерація й Китай. Визначено позиції держав-членів Альянсу в Глобальному індексі кібербезпеки, укладеним Міжнародним союзом електрозв'язку. Представлено авторський підхід щодо сценаріїв майбутнього розвитку кібербезпекової політики Північноатлантичного Альянсу. Зроблено висновок про необхідність вдосконалення чинної політики кібербезпеки НАТО й презентовано рекомендації, з-поміж яких: розвиток оборонних і наступальних можливостей НАТО, перехід до більш проактивної політики в кіберпросторі, використання кращого досвіду членів Альянсу з попередження кібератак за прикладом США, застосування розвідувальних можливостей НАТО, вдосконалення механізму застосування Статті 5 у випадку кібернетичної атаки й публічної атрибуції кібератак, а також поглиблення співробітництва з приватним сектором в галузі кібероборони.

Ключові слова: кібербезпека, кібератака, кібероборона, кіберзагроза, НАТО, Україна, Російська Федерація, Китай.

Розвиток сучасних інформаційних технологій, безперечно, став рушієм соціально-економічного й політичного добробуту держав світу. Кіберзлочинність на сьогодні є однією із найбільших загроз світовій безпеці. Особливо гостро питання подолання кіберзагроз стоїть перед найбільшим і найвпливовішим військовим альянсом світу – НАТО, який зазнає перманентно ворожими кібератак. Актуальність дослідження зумовлена суттєвим зростанням кількості гібридної та інформаційної агресії у світі, а розробка й імплементація ефективної політики в галузі кіберзахисту є пріоритетним завданням як для держав євроатлантичного простору, так і для України. В цьому контексті корисним є вивчення засадничих принципів, політики і практики у галузі кібербезпеки Організації Північноатлантичного договору, яка є найвпливовішою військово-політичною структурою й продемонструвала прогресивні підходи щодо реагування на новітні загрози в кіберпросторі.

НАТО, у своїх офіційних документах, доктринах й політичних заявах «кібероборону» визначає як «здатність захищати постачання й керування послугами в оперативній комунікативно-інформаційній системі у відповідь на потенційні, неминучі й актуальні зловмисні дії, які надходять з кіберпростору» [12].

Експерти НАТО розрізняють активну й пасивну кібероборону. Активна кібероборона (Active Cyber Defence) – це застосування проактивних заходів задля виявлення або отримання інформації про ймовірну кібератаку, кібероперацію або кібервтручання або визначення походження операції, що передбачає запуск попередньої, превентивної або кіберконтр-операції проти джерела. Пасивна кібероборона (Passive Cyber Defence) передбачає використання заходів з виявлення та ліквідації кібервтручань й наслідків кібератак, які не передбачають проведення застосування превентивних або контр-операцій проти джерела їхнього походження. [17, p. 260].

Варто виокремити низку пріоритетних завдань в політиці кібербезпеки Північноатлантичного Альянсу:

– захист власних мереж;

– надання допомоги державам-членам НАТО для розвитку їхніх власних можливостей і потужностей з кібероборони;

– поглиблення багатонаціональної співпраці у сфері кібербезпеки.

Ключовими завданнями співпраці в сфері кібербезпеки між державами-партнерами й НАТО є:

– розробка ефективних механізмів з протидії кібератакам;

– функціонування системи оперативного реагування на актуальні загрози в інформаційному й кібернетичному просторі держав;

– забезпечення стабільного функціонування об'єктів критичної інформаційно-комунікативної інфраструктури;

– у разі необхідності надання допомоги державам щодо відновлення нормального функціонування такої інфраструктури від негативних наслідків кібератак [3].

Концептуальне забезпечення політики кібербезпеки НАТО базується на таких правових нормах та документах: 1) Програма кібероборони НАТО; 2) Комлексна політика кібероборони НАТО; 3) Стратегічна концепція НАТО; 4) Оборонне планування НАТО; 5) Промислове кіберпартнерство НАТО; 6) Зобов'язання щодо кібероборони держав-членів Альянсу [1; 5; 12; 15].

Інституційний вимір політики НАТО у сфері кібербезпеки забезпечують: 1) Сили реагування НАТО на кіберінциденти; 2)Управління з питань кіберзахисту НАТО; 3) Групи швидкого реагування НАТО на кіберінциденти; 4) Агентство НАТО зі зв'язку та інформації; 5) Центр кібернетичних операцій НАТО; 6) Головний офіцер з питань інформації; 7) Віртуальні сили підтримки під час кіберінцидентів; 8) Комітет з кібероборони; 9) Керівна рада з питань кібероборони; 10) Агентство зв'язку та інформації НАТО; 11) Центр передового досвіду НАТО з питань кіберзахисту [7; 12; 15].

На сьогодні НАТО і держави-члени зіштовхуються із численними загрозами у кіберпросторі. З метою ґрунтовного дослідження проаналізовано ключові виклики для кібербезпеки НАТО, які презентовано у Таблиці 1.

Сьогодні ключовими акторами, які загрожують кібербезпеці Північноатлантичного Альянсу, є державні й недержавні суб'єкти, кіберзлочинці й інсайдери. Найбільш активними державами в кіберпросторі, які регулярно здійснюють деструктивні кібероперації проти держав-членів НАТО є Російська Федерація й Китай. Встановлено, що найбільш поширеним інструментарієм цих держав є застосування кібернетичних атак проти урядових інформаційних систем і об'єктів критичної інфраструктури, кібершпигунства, кібератак з метою викупу. Суттєву загрозу для Альянсу також становлять китайські технологічні проєкти й соціальні мережі.

Таблиця 1

Виклики для кібербезпеки НАТО та його держав-членів [12; 13; 14; 15; 17; 18]

Зміст загрози	Приклад
Дезінформація й просування ворожих наративів	Фейкові листи про виведення військ НАТО зі держав Балтії через COVID-19 (2020 р.)
Кібератаки злочинних угруповань з метою вимагання грошового викупу	Кібератака на паливопровід Colonial Pipeline в США (2021 р.)
Кібератаки з політичним підґрунтям	Кібератаки іранських хакерів проти Албанії (2022 р.); Кібератаки російських хакерів проти Литви через накладення санкцій на товарообіг з Калінінграду (2022 р.)
Викрадення конфіденційних даних НАТО	Кібератака угруповання SiegedSec, які викрали документи стратегічного планування й досліджень Альянсу (2023 р.); Кібератаки проти інформаційних ресурсів НАТО напередодні Вільнюського саміту (2023 р.)
Кібернетичне шпигунство, викрадення патентів, наукових і військових розробок	Кібератака КНР на сервер Microsoft, викрадення даних приватних компаній з інформацією про патенти й наукові розробки (2021 р.); Викрадення Китаєм секретних даних про винищувачі-невидимки США (2019 р.)
Кібератаки проти систем зв'язку НАТО (супутників, систем навігації)	Кібератака Росії на супутник Viasat в день вторгнення в Україну (2022 р.); Глушіння Росією систем GPS НАТО в Норвегії, які використовуються для військових навчань
Домінування китайських технологій, які займаються кібершпигунством й збором персональних даних	Побудова мереж 5G від китайської компанії Huawei, популярність застосунку TikTok в країнах-членах Альянсу

Загалом усі загрози політиці кібербезпеки НАТО умовно можна розділити на такі дві групи: ендогенні та екзогенні. Результати пропонуємо представити у вигляді схематичної таблиці (таблиця 2).

Незважаючи на географічну віддаленість, НАТО відзначає посилену загрозу зі сторони Китаю, як-от: активізація китайських операцій в кіберпросторі з викрадення промислових і військових секретів, розбудова власної мережі 5G й активне поширення китайських

Таблиця 2

Загрози і виклики для політики кібербезпеки НАТО [12; 13; 14; 15; 17; 18]

Екзогенні	**Ендогенні**
Дезінформаційні кампанії РФ і КНР	Відсутність узгодженого механізму щодо застосування Статті 5 НАТО у випадку кібератаки
Кібератаки з використанням програм-вимагачів	Концепція «стратегічної невизначеності» НАТО
Політично вмотивовані кібератаки	Відсутність практичних кейсів із застосування Статті 5 НАТО внаслідок кібератаки на державу-члена
Кібершпигунство й викрадення даних Росією й Китаєм	Складність публічної атрибуції кібератак
Кібератаки на об'єкти критичної інфраструктури, супутники, системи GPS та ін.	Відмінності у формуванні кібербезпекової політики держав-членів НАТО
Поширення китайських застосунків й інфраструктури 5G від Huawei	Утримання від застосування наступальних кібероперацій проти порушників у кіберпросторі

застосунків викликає занепокоєння серед країн-членів НАТО. Окрім цього, проаналізовано сучасну практику застосування політики кібероборони НАТО. Проблема, навколо якої постійно точаться дебати – це питання застосування Статті 5 НАТО в кіберпросторі, адже на сьогоднішній день Альянс не виробив чіткої стратегії дій у разі кібернападу й не встановив чітких ознак, коли кібератака може вважатися збройним нападом. Зокрема серйозним викликом є публічна атрибуція кібератак Альянсом. Проблема розбудови китайської інформаційної інфраструктури в державах НАТО також демонструє відсутність єдності серед держав-членів Альянсу у критичних безпекових питаннях.

Для виконання поставленого завдання пропонуємо розглянути актуальну статистику Глобального індексу кібербезпеки, складеного Міжнародним Союзом Електрозв'язку (ITU) в 2020 році.

В таблиці наведено дані Глобального індексу кібербезпеки держав-членів Північноатлантичного Альянсу; також до рейтингу авторами включено Україну. Зазначимо, що нова версія опитувальника була дещо змінена, тому вагові коефіцієнти відрізняються від попередніх ітерацій.

Таким чином, ми можемо відзначити тенденцію щодо покращення показників кібербезпеки серед багатьох держав-членів Альянсу протягом останніх років. Показовим також

Таблиця 3

Глобальний індекс кібербезпеки держав (2018, 2020 рр.)

Місце в рейтингу (2018)	Держава	Кількість пунктів	Місце в рейтингу (2020)	Держава	Кількість пунктів
1	Великобританія	0.931	1	США	100
2	США	0.926	2	Великобританія	99.54
3	Франція	0.918	3	Естонія	99.48
4	Литва	0.908	4	Іспанія	98.52
5	Естонія	0.905	6	Литва	97.93
7	Іспанія	0.896	8	Канада	97.67
9	Канада	0.892	9	Франція	97.6
9	Норвегія	0.892	11	Туреччина	97.49
11	Люксембург	0.886	13	Люксембург	97.41
12	Нідерланди	0.885	13	Німеччина	97.41
19	Фінляндія	0.856	14	Португалія	97.32
20	Туреччина	0.853	15	Латвія	97.28
21	Данія	0.852	16	Нідерланди	97.05
22	Німеччина	0.849	17	Норвегія	96.89
24	Хорватія	0.840	19	Бельгія	96.25
25	Італія	0.837	20	Італія	96.13
29	Польща	0.815	22	Фінляндія	95.78
30	Бельгія	0.814	28	Греція	93.98
31	Угорщина	0.812	30	Польща	93.86
34	Північна Македонія	0.800	32	Данія	92.6
42	Португалія	0.758	33	Хорватія	92.53
44	Латвія	0.748	34	Словаччина	92.36
45	Словаччина	0.729	35	Угорщина	91.28

Продовження таблиці 3

46	Болгарія	0.721	38	Північна Македонія	89.92
48	Словенія	0.701	58	Ісландія	79.81
54	Україна	0.661	62	Румунія	76.29
61	Чорногорія	0.639	67	Словенія	74.93
62	Албанія	0.631	68	Чехія	74.37
71	Чехія	0.569	77	Болгарія	67.38
72	Румунія	0.568	78	Україна	65.93
77	Греція	0.527	80	Албанія	64.32
87	Ісландія	0.449	87	Чорногорія	53.87

Джерело: опрацьовано на основі звіту ITU [10; 11].

є той факт, що 2/3 держав НАТО знаходяться в топ-30 найкращих країн за показником кібербезпеки. Традиційними лідерами рейтингу, з несуттєвими відмінностями у показниках є Сполучені Штати Америки, Великобританія, Естонія, Литва, Франція, Іспанія, Канада.

Для здійснення комплексного аналізу кібернетичної стійкості НАТО пропонуємо застосувати методику SWOT-аналізу (таблиця 4).

На основі здійсненого аналізу, авторами виокремлено декілька ймовірних сценаріїв розвитку політики кібербезпеки НАТО. У найближчій перспективі поведінка агресивних держав в кіберпросторі не зазнає змін. Найімовірніше, що Росія, Китай, Іран та інші недемократичні держави й надалі продовжуватимуть використання агресивних дій в кібернетичному просторі задля досягнення власних цілей. Відповідно, представлено сценарії, які базуватимуться на тому, що НАТО регулярно стикається з ворожими кібератаками. Ці

Таблиця 4

SWOT-аналіз політики кібербезпеки НАТО

Strengths (сильні сторони)	**Weaknesses (слабкі сторони)**
Наявність сильної інституційно-правової бази у сфері кібербезпеки, технічних можливостей і спеціальних груп для протидії кібератакам; Великий акцент на здійснення навчань спеціалістів з кібербезпеки; Більшість держав-членів Альянсу займають провідні позиції у рейтингу кібербезпеки; США, Велика Британія, держави Балтії, які є членами НАТО, вважаються одними з найбільш захищених держав у сфері кіберпростору	Відсутність практики із застосування Статті 5 внаслідок атаки в кіберпросторі; Розбіжність у поглядах щодо застосування механізмів протидії кібератакам; Розмитість й нечіткість у формулюваннях в документах, які стосуються кібербезпеки; Різні підходи до будування відносин з третіми державами (такими як Росія й Китай) серед країн НАТО; Складність здійснення публічної атрибуції кібератак
Opportunities (можливості)	Threats (загрози)
Створення Центру кібернетичних операції; Інтегрування кібернетичної складової у військові операції і місії НАТО; Використання досвіду провідних держав (США, Великобританії, Естонії) НАТО у боротьбі з кібератаками; Посилення співпраці з приватним сектором; Розвиток оборонних й наступальних кібероперації НАТО, базуючись на успішному досвіді країн Альянсу	Кібератаки РФ, Китаю та інших злочинних кібератакорів проти інформаційних систем НАТО; Викрадення конфіденційних документів Альянсу, інформації про наукові й військові розробки; Кібернетичне шпигунство; Кібератаки проти об'єктів критичної інфраструктури й об'єктів військового застосування (супутники, системи навігації) НАТО

сценарії значною мірою зумовлюються наступними факторами: подальшою агресивною поведінкою акторів в кіберпросторі (наскільки агресивними будуть дії РФ, Китаю та інших суб'єктів), здатністю держав-членів НАТО досягнути консенсусу і їхньої політичної волі, геополітичного середовища й технологічних змін. Отже, ми бачимо такі три сценарії.

Найбільш ймовірним ми вважаємо сценарій, який передбачає збереження статусу-кво. Протягом останніх років не спостерігається якихось кардинальних змін чи глобальних рішень, які би ознаменували докорінну зміну політики кібербезпеки Альянсу. Виглядає на те, що, перехід до більш «агресивних» дій і заходів в кіберпросторі, які ведуться від імені Альянсу, можуть спричинити погіршення відносин з Росією. Отже, акцент робитиметься на розвитку вже існуючих механізмів й практик й на зміцненні кібероборони Альянсу.

З огляду на проаналізовані нами актуальні виклики та загрози в віртуальному просторі, вважаємо за необхідне надати власні рекомендації щодо вдосконалення політики кібероборони й посилення кібербезпеки НАТО: 1) Державам Альянсу необхідно встановити чіткі «тригери» й «червоні лінії», які визначають, коли буде застосована Стаття 5; 2) Створення власних наступальних й вдосконалення оборонних кіберможливостей

Таблиця 5

Сценарії розвитку політики кібербезпеки НАТО

№	Назва та рівень ймовірності сценарію	Обґрунтування
1	Оптимістичний	Розробка й застосування ефективної кібербезпекової політики Альянсу, яка відповідає сучасним загрозам. Такий сценарій включає в себе: створення кіберармії НАТО, розгортання діяльності роботи Центру кібероперацій НАТО, створеного внаслідок Брюссельського саміту, зростання ролі й застосування наступальних кібероперації проти ворожих до НАТО акторів в кіберпросторі, ефективне виявлення та ліквідація загроз від злочинних угруповань в віртуальному просторі; повна відмова від застосування китайської зв'язкової інфраструктури. Внаслідок цієї політики наслідки ворожих кібератак від значних і деструктивних знижуються до мінімальних й таких, які не загрожують стабільності й безпеці Альянсу і його членів. Оцінюємо цей сценарій як середньо ймовірний.
2	Збереження статусу-кво	Розвиток політики кібербезпеки НАТО в актуальному руслі, з акцентом на стримування й оборону від кібератак. Кібератаки зі сторони Китаю, Росії й інших недержавних акторів й надалі матиме місце й становитимуть загрозу для Альянсу, однак матимуть змінний успіх: негативні наслідки від кібератаки будуть варіюватися залежно від типу загроз, рівня кіберзахисту й співпраці держав-членів НАТО. НАТО продовжуватиме працювати над зміцненням стійкості національних систем кібербезпеки держав, заохочуватиме дво- й багатосторонню співпрацю у сфері кіберзахисту між державами Альянсу й партнерами, а також приватними компаніями та іншими регіональними й безпековими інституціями.
3	Песимістичний	Провал політики кібероборони НАТО. Сценарій передбачає ескалацію кібератак й вихід на рівень кібервійни між Північноатлантичним Альянсом й Російською Федерацією з Китаєм. Зростання кількості й складності кібератак, внаслідок яких будуть виведені з ладу усі інформаційно-комунікативні мережі, веб-сайти й центри командування НАТО, пошкодження роботи критичної інфраструктури й каналів зв'язку держав-членів Альянсу. Вважаємо такий сценарій на сьогоднішній день малоймовірним.

Альянсу; 3) НАТО повинно здійснювати активний кіберзахист в координації зі своїми країнами; 4) Елементом активної кібероборони повинна стати практика з використання професійних груп-мисливців для викриття загроз й попередження майбутніх атак на критично важливі для Альянсу системи; 5) Північноатлантичний Альянс повинен бути більш консолідованим у питанні публічної атрибуції кібератак; 6) Цінність НАТО може полягати в тому, що воно може стати найкращою платформою для обміну кіберінформацією; Північноатлантичний Альянс також повинен використовувати свої можливості розвідки для систематичного моніторингу загроз з боку Росії, КНР та інших ворожих суб'єктів; 7) Важливим елементом для посилення кіберстійкості НАТО, на нашу думку, є посилення співпраці з приватним сектором, який, по суті, став новітнім партнером державних установ у сфері кіберзахисту; 8) Члени Альянсу також повинні вдосконалити колективний процес прийняття рішень й досягнути спільного розуміння гібридних загроз і відповідей на них [3; 4; 12; 15].

Отож, можемо висновувати про те, що сьогодні кібернетичний простір став справжньою ареною для протистояння, адже гібридні інструменти впливу й інформаційні технології надають чимало можливостей для досягнення політичних і економічних переваг недемократичними державами. З кіберзагрозами регулярно стикається і Північноатлантичний Альянс, який продемонстрував передові підходи до реагування на актуальні виклики в кіберпросторі. Встановлено, що Північноатлантичний Альянс застосовує поняття «кібероборона», яке означає здатність захищати складові елементи власних інформаційно-комунікативних від неминучих зловмисних дій з кіберпросторі. Було виявлено, що зусилля НАТО в політиці кіберзахисту більшою мірою спрямовані на посилення власних оборонних можливостей проти актуальних загроз. Пріоритетами Альянсу в сфері кібербезпеки є захист власних інформаційних мереж, підтримка держав-членів й поглиблення міжнародної співпраці у протидії кібернетичним загрозам. Щодо інституційно-правової бази, проаналізовано інституційні засади та концептуальні норми у сфері кібербезпеки НАТО. Реалізацією кібербезпекової політики займається як вище політичне керівництво Альянсу, так і спеціалізовані інституції, такі як Об'єднаний центр передових технологій з кібероборони НАТО, Центр кібернетичних операцій, Групи реагування в кіберпросторі та інші. Встановлено, що загрозу для НАТО становлять недружні держави – головним чином Російська Федерація й Китай, проксі-актори, такі як хактивісти й злочинні угруповання, які можуть співпрацювати з державами. Сучасні загрози для кіберпростору НАТО ми можемо окреслити таким чином: це кампанії з дезінформації, які мають на меті похитнути довіру до Альянсу й спричинити розкол всередині його членів; кібернетичні атаки з політичною метою, атаки на критично важливі об'єкти й інфраструктуру, що включає в себе атаки на системи GPS, навігації, супутники та ін. Актуальною загрозою для Альянсу є також діяльність китайського уряду, яка здебільшого зосереджена на кібершпигунстві й викраденні даних про передові технології і військові розробки НАТО. Занепокоєння також викликає розгортання мережі 5G від Huawei й робота китайських застосунків та території країн Альянсу. Розглянуто результати дослідження Міжнародного союзу електрозв'язку й встановлено, що більшість країн Альянсу є лідерами у Глобальному індексі кібербезпеки. Динаміка також свідчить про те, що їхні показники покращуються. Виявлено, що на сьогоднішній день найбільш стійкими до кіберзагроз є такі країни як США, Великобританія, Естонія, Литва й Франція, які працюють над вдосконаленням власних оборонних й наступальних можливостей в кіберпросторі й успішно їх застосовують на практиці. Внаслідок здійсненого нами аналізу ми виокремили три можливі сценарії розвитку політики кібероборони НАТО.

Вважаємо, що наразі політика Альянсу у сфері кібербезпеки залишиться у статусі-кво. Аналізуючи кібербезпекову політику НАТО, ми дійшли до висновку, що, зважаючи на актуальні міжнародні події й агресивну поведінку в кіберпросторі таких держав як Російська Федерація й Китай, Альянс повинен зайняти більш активну позицію, а не виключно оборонну. НАТО має великий потенціал для проведення наступальних кібероперацій під керівництвом Центру кібероперацій НАТО, який має інтегрувати й координувати можливості, сили та засоби держав-членів у протидії ворожим суб'єктам в кіберпросторі. Також ми рекомендуємо вдосконалити позицію Альянсу про застосування Статті 5 у випадку кібератаки на державу-члена, адже на сьогоднішній день, попри численні кейси таких деструктивних кібератак, ця позиція ні разу не була застосована у реальності через відсутність чітких ознак, коли кібератака набуває ознак збройного нападу й механізму дій Альянсу у таких випадках. Зокрема корисним є досвід Сполучених Штатів із використання професійних груп із полювання на загрози в кіберпросторі аби ефективно виявляти й знешкоджувати їх до того, як вони будуть використати проти НАТО і союзників. Ефективною також виявилася співпраця НАТО із технологічними компаніями приватного сектору, яку, на нашу думку, можна поглибити. Альянс також може більше використовувати власні можливості для здійснення розвідки й постійного моніторингу загроз зі сторони Росії й Китаю, які можуть бути застосовані проти демократичних інститутів держав Альянсу, важливої інфраструктури й об'єктів військового призначення НАТО. Вважаємо, що держави-члени Альянсу також мають досягнути консенсусу щодо питань, які мають більш політизований характер, такі як встановлення публічної атрибуції держави-порушника в кіберпросторі й питання співпраці із КНР.

Список використаної літератури

1. Завгородня Ю. В. Роль НАТО у боротьбі з кіберконфліктами: політико-правовий аспект. *Регіональні студії*. 2022. № 30. С. 62–65.
2. Калетнік В. В., Калетнік В. Н. Кібератаки як ключові елементи «інформаційної війни» Російської Федерації. *Науковий журнал «Молодий вчений»*. 2022. № 1. С. 37–42.(13)
3. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.(18)
4. Alexander D. D. Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses. *DergiPark Akademik*. URL: https://dergipark.org.tr/tr/download/article-file/89251 (дата звернення: 20.11.2023).(27)
5. Allied Joint Doctrine for Cyberspace Operations. *NATO Stadnardization Office*. URL: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137 675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (дата звернення: 27.10.2023).(28)
6. Ciaran M. Out-of-Control Cybercrime Will Cause More Real-World Harm. *WIRED UK*. URL: https://www.wired.co.uk/article/cyber-criminals-physical-harm (дата звернення: 09.10.2023).(35)
7. Davis S. NATO In The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence. URL: https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf (дата звернення: 17.10.2023).(43)
8. Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape. *Google Threat Analysis Group (TAG) report*. URL: https://services. google.com/fh/files/blogs/google_fog_of_war_research_report.pdf (дата звернення: 29.10.2023).(51)

9. Furry hackers claim to have breached NATO, stolen 3,000 files. *DailyDot*. URL: https://www.dailydot.com/debug/siegedsec-nato-hack/ (дата звернення: 17.11.2023).
10. Global Cybersecurity Index (GCI) 2018. *International Telecommunication Union*. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (дата звернення: 24.11.2023).(55)
11. Global Cybersecurity Index (GCI) 2020. *International Telecommunication Union*. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (56)
12. Gökhan T. NATO as a Global Cybersecurity Power. *Işık University Institutional Repository*. URL: https://acikerisim.isikun.edu.tr/xmlui/bitstream/handle/11729/5191/Nato_as_a_Global_Cybersecurity_Power.pdf?sequence=1&isAllowed=y (дата звернення: 24.11.2023) (57)
13. Hakala J., Melnychuk J. Russia's Strategy in Cyberspace. *NATO Strategic Communications Centre of Excellence*. URL: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf (дата звернення: 20.11.2023).(58)
14. Loverdos A. The Offence-Defence Balance: NATO's Growing Cyber Challenge. *NATO Parliamentary Assembly*. 2022. URL: https://www.nato-pa.int/document/2022-offence-defence-natos-cyber-challenge-report-pinotti-015-dscfc (дата звернення: 20.11.2023). (67)
15. Maigre M. NATO's Role in Global Cyber Security. *German Marshall Fund*. URL: https://www.gmfus.org/news/natos-role-global-cyber-security (дата звернення: 05.11.2023) (69)
16. Marrone A., Sabatino E. Cyber Defence in NATO Countries: Comparing Models. *IAI Papers*. 2021. №. 5. P. 1–37.(70)
17. Tallinn Manual on the International Law Applicable to Cyber Warfare. *Georgetown Law Library*. URL: https://guides.ll.georgetown.edu/c.php?g=363530&p=4821482 (дата звернення: 17.11.2023).(89)
18. Wiedemar S. NATO and Article 5 in Cyberspace. *Center for Security Studies (CSS), ETH Zürich*. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf (дата звернення: 11.10.2023).(99)

CHALLENGES AND OPPORTUNITIES FOR IMPLEMENTATION OF THE NATO CYBERSECURITY POLICY

Oleh Tsebenko, Olha Ivasechko, Daria Khivrenko
Lviv Polytechnic National University, Institute of Humanities and Social Sciences, Department of Political Science and International Relations
Metropolitan Andrey str., 5, 79013, Lviv, Ukraine

The article emphasises that today many non-democratic states consider their own dominance in cyberspace as an integral part of their foreign policy. It is established that states such as the Russian Federation and China, as well as criminal hacker groups, pose a significant threat to NATO's cyber security. It is found that NATO has a solid legal and institutional framework in the field of cybersecurity. It is emphasised that the Alliance uses the term «cyber defence» to refer to actions aimed at protecting its own information and communication infrastructure from threats from cyberspace. In particular, the article examines in detail the current threats in cyberspace faced by the Alliance. It is established that such threats range from the use of cyber attacks on critical NATO facilities and politically motivated attacks to cyber espionage and disinformation campaigns by the Russian Federation and China. The article analyses the positions of the Alliance states in the Global Cybersecurity Index compiled by the International Telecommunication Union. The authors identify three scenarios for the development of the Alliance's cybersecurity policy. The authors highlighted the need to improve NATO's current cybersecurity policy and provided practical

recommendations, such as: developing NATO's defensive and offensive capabilities, moving to a more proactive policy in cyberspace, using the best practices of Allies in preventing cyberattacks following the example of the United States, using NATO's intelligence capabilities, improving the mechanism for applying Article 5 in the event of a cyberattack and public attribution of cyberattacks, as well as deepening cooperation with the private sector in the field of cyber.

Key words: cyber security, cyber attack, cyber defence, cyber threat, NATO, Ukraine, Russian Federation, China.