**УДК 327.51**

**DOI https://doi.org/10.5281/zenodo.16885188**

# Трансформація безпекової парадигми НАТО та бюджетно-фінансова адаптація до загроз нового типу

**Джигора Ольга Миколаївна,**
к.е.н., доцент,докторант кафедри національної безпеки,
публічного управління та адміністрування
Державного університету «Житомирська політехніка»,
м. Житомир, Україна,
ORCID: https://orcid.org/0000-0001-8490-3917

**Прийнято: 28.08.2024 | Опубліковано: 17.09.2024**

***Анотація.*** *Мета дослідження полягає у науковому обґрунтуванні трансформації безпекової парадигми НАТО в умовах загроз нового типу загалом та кіберзагроз – зокрема. У статті розглянуто кіберзахист як ключовий елемент стратегії стримування та оборони НАТО. Визначено нові вимоги до захисту критичної інфраструктури країн-членів Альянсу. Акцентовано увагу на стрімкому зростанні кількості кіберінцидентів із політичним підтекстом у глобальному масштабі. Проаналізовано динаміку кількості кібератак із політичною складовою у світі (урядові установи, виборчі системи, енергетичні платформи, інформаційні канали впливу). Визначено зростання ролі гібридних інструментів впливу, зокрема інформаційно-психологічних операцій (ІПсО), як одного з ключових векторів*

*дестабілізації демократичних режимів. Проведено розподіл кібератак у світових галузях економіки. Визначено цілі російських кібератак проти інших країн світу, в тому числі України. Доведено, що російські хакерські угруповання здійснюють численні втручання в урядові системи, телекомунікаційну інфраструктуру та об'єкти енергетики, що підтверджується звітами Microsoft та Recorded Future. Констатовано, що серед головних цілей російських хакерських кампаній залишаються державні установи, які становлять понад 33% усіх атак, що здійснюються російськими угрупуваннями. Розраховано, що понад 80% країн НАТО у 2023 р. зазнали хоча б однієї масштабної кібератаки на державні або стратегічні об'єкти. Проаналізовано основні вектори політики кіберзахисту країн-членів Альянсу. Доведено, що в умовах стрімкої гібридизації конфліктів, кібероперації стають інструментом стратегічного шантажу, політичного тиску та порушення інформаційної суверенності, що вимагає від НАТО суттєвого посилення колективного кіберзахисту. Визначено необхідність створення та основні засади діяльності Інтегрованого центру кіберзахисту НАТО.*

***Ключові слова:*** *кібератака, кіберзагроза, ІПсО, хакерські компанії, кібербезпека, НАТО, кіберзахист.*

## Transformation of NATO's Security Paradigm and Budgetary-Financial Adaptation to New-Type Threats

**Olha Dzhyhora,**
PhD in Economics, Associate Professor,
Doctoral Student at the Department of National Security,
Public Administration and Management,
State University "Zhytomyr Polytechnic", Zhytomyr, Ukraine,
ORCID: https://orcid.org/0000-0001-8490-3917

***Abstract.*** *The purpose of the study is to provide a scientific basis for the transformation of NATO's security paradigm in the face of new types of threats in general and cyber threats in particular. The article examines cyber defence as a key element of NATO's deterrence and defence strategy. New requirements for the protection of critical infrastructure of NATO member states are identified. Attention is focused on the rapid growth in the number of cyber incidents with political overtones on a global scale. The author analyses the dynamics of the number of cyberattacks with a political component in the world (government agencies, electoral systems, energy platforms, information channels of influence). The author identifies the growing role of hybrid instruments of influence, in particular, information and psychological operations (IPO), as one of the key vectors of destabilisation of democratic regimes. The distribution of cyberattacks in global economic sectors is made. The goals of Russian cyberattacks against other countries, including Ukraine, are identified. It is proved that Russian hacker groups carry out numerous interventions in government systems, telecommunications infrastructure and energy facilities, which is confirmed by reports from Microsoft and Recorded Future. It is stated that government agencies remain among the main targets of Russian hacking campaigns, accounting for more than 33% of all attacks carried out by Russian groups. It is estimated that more than 80% of NATO countries experienced at least one large-scale cyberattack on state or strategic facilities in 2023. The main vectors of cyber defence policy of the Alliance member states are analysed. It is proved that in the context of the rapid hybridisation of conflicts, cyber operations are becoming an instrument of strategic blackmail, political pressure and violation of information sovereignty, which requires NATO to significantly strengthen its collective cyber defence. The necessity of establishing and the basic principles of the NATO Integrated Cyber Defence Centre are determined.*

***Keywords:*** *cyberattack, cyber threat, IPSO, hacker companies, cybersecurity, NATO, cyber defence.*

**Постановка проблеми.** У XXI ст. безпекова політика зазнає глибинної трансформації під впливом нових форм загроз. Мова йде про гібридні операції, кібератаки, інформаційно-психологічний вплив. У результаті цифровий вимір поступово перетворюється на одну з ключових сфер глобального протистояння, де конфлікти розгортаються не лише у фізично. Для Північноатлантичного Альянсу це означає необхідність принципового переосмислення підходів до стримування, реагування та стратегічного управління ризиками. З огляду на те, що кібератаки дедалі частіше призводять до наслідків, співмірних із застосуванням збройної сили, НАТО офіційно визнав кіберпростір окремим операційним доменом. Така ситуація обумовила необхідність формування нової інституційної та фінансової основи для оперативного реагування та готовності до протидії цифровим загрозам. У цьому контексті актуалізується потреба у дослідженні стратегічних механізмів кібербезпеки в межах НАТО, які стають невід'ємною складовою колективної оборони, оперативної готовності та національної резильєнтності країн-членів. Розкриття даної проблематики дозволяє окреслити не лише практичні інструменти адаптації Альянсу до нових викликів, а й окреслити теоретико-методологічні засади нової парадигми безпеки в цифрову епоху.

**Аналіз останніх досліджень і публікацій.** У наукових працях В. Горлинського, Б. Горлинського [1], І. Діордіца [2], Н. Лугіна [3], А. Бойко, О. Бойко, В. Шендрука [4] та інших авторів підкреслюється, що кібербезпека у XXI ст. для НАТО – це не просто компонент цифрової інфраструктури, а ключовий елемент гарантування суверенітету країн-членів, підтримки оперативної готовності та забезпечення стійкості критичних систем управління, зв'язку, енергетики та оборони. З огляду на міждисциплінарний характер сучасних загроз, кіберпростір стає політичним, стратегічним і економічним простором взаємодії держав, у якому цифрові атаки здатні

викликати системні збої, зрив стратегічних операцій або вплинути на прийняття політичних рішень.

У працях українських та зарубіжних науковців простежується спільна думка щодо необхідності створення нових моделей оцінювання загроз, інтеграції аналітичної розвідки, а також фінансового інвестування в цифрову оборону на рівні НАТО. Таким чином, аналіз літературних джерел свідчить, що кібербезпека для НАТО трансформується із суто технологічного напряму у системну функцію стратегічного управління безпекою. У цьому контексті кіберзахист стає передумовою ефективного функціонування механізму колективної оборони та формує умови для адаптації Альянсу до загроз цифрової доби. Водночас складність, гібридність та новизна означеної проблематики потребують подальшого теоретико-методологічного опрацювання.

**Виділення невирішених раніше частин загальної проблеми.** Незважаючи на наявність значної кількості досліджень, присвячених дослідженню характеру загроз у кіберпросторі, недостатньо вивченими залишаються питання кібератак у світових галузях економіки. Недостатньо розкритими є питання щодо цілей російських кібератак проти інших країн світу, в тому числі України. Потребує подальшого дослідження аналіз національних політик кіберзахисту країн-членів НАТО.

Саме тому, у даній статті, дійснено комплексний аналіз трансформації фінансової політики НАТО в умовах ескалації кіберзагроз, який полягає у виявленні взаємозв'язку між стратегічними пріоритетами Альянсу та еволюцією бюджетних механізмів, спрямованих на посилення кібербезпеки. Обґрунтовано, що рішення, ухвалені на самітах у Вільнюсі (2023 р.) та Вашингтоні (2024 р.), стали ключовими у формуванні нової парадигми безпеки, в якій цифровий простір розглядається не як допоміжний, а як системоутворюючий елемент оборонного планування НАТО. Проаналізовано

механізми інтеграції витрат на кіберзахист до Програми інвестицій у безпеку (NSIP) та Цивільного бюджету НАТО, а також їхній вплив на гнучкість і резильєнтність фінансової моделі Альянсу.

**Формулювання цілей статті (постановка завдання).** Метою статті є наукове обґрунтування трансформації безпекової парадигми НАТО в умовах загроз нового типу загалом та кіберзагроз – зокрема.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- розглянути кіберзахист як ключовий елемент стратегії стримування та оборони НАТО;

- проаналізувати динаміку кількості кібератак із політичною складовою у світі;

- провести розподіл кібератак у світових галузях економіки;

- визначити цілі російських кібератак проти інших країн світу, в тому числі України;

- проаналізувати основні вектори політики кіберзахисту Альянсу.

**Виклад основного матеріалу дослідження.** Особливе місце в новій архітектурі безпеки посідає кіберзахист як ключовий елемент стратегії стримування та оборони НАТО. Починаючи з 2016 р., кіберпростір офіційно визнано окремою операційною сферою Альянсу, на одному рівні із суходолом, морем та повітрям. Це означає, що кібератаки можуть розцінюватися як підстава для колективної відповіді відповідно до ст. 5 Вашингтонського договору [5]. Така концептуалізація дозволила Альянсу розвинути політичну, технологічну та військову координацію для реагування на зловмисну кібердіяльність як на потенційну загрозу колективній безпеці. У відповідь на загострення кіберзагроз, союзники ухвалили Зобов'язання щодо кіберзахисту, яке у 2023 р. було оновлено новими вимогами до захисту критичної інфраструктури та досягнення високих стандартів національної стійкості [6]. Наразі основна увага НАТО

зосереджується на трьох рівнях: захисті власних мереж, підвищенні кіберстійкості країн-членів, а також забезпеченні платформи для політичного консенсусу та колективних дій у разі масштабних інцидентів у цифровій сфері [5].

Аналітичні дані свідчать про стрімке зростання кількості кіберінцидентів із політичним підтекстом у глобальному масштабі. Якщо у 2014 р. таких випадків було зафіксовано 107, то у 2022 р. – вже 322, у 2023 – 723, а за перші шість місяців 2024 р. – 702, що свідчить про стабільно високий рівень загроз у цьому вимірі. Крім того, відбувається не лише кількісне зростання кіберзагроз, але й їхня якісна трансформація. Дедалі частіше об'єктами кібератак стають урядові установи, виборчі системи, енергетичні платформи, інформаційні канали впливу (рис. 1) [7].

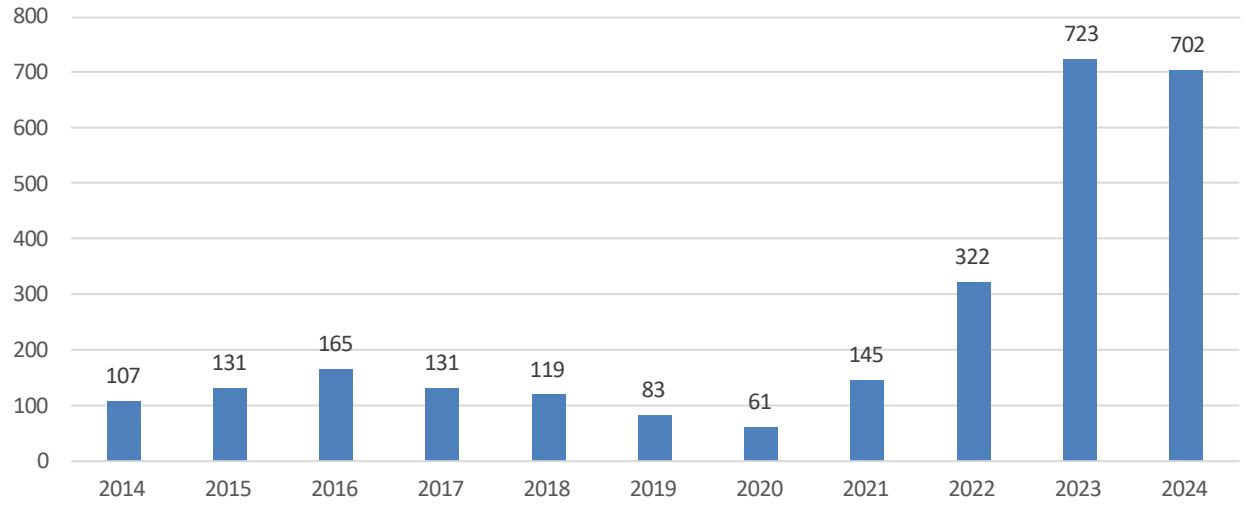


**Рис. 1. Динаміка кількості кібератак із політичною складовою у світі, 2014–2024 рр.**

*Джерело:* побудовано автором [7]

Така динаміка свідчить про зростання ролі гібридних інструментів впливу, зокрема інформаційно-психологічних операцій (ІПсО), як одного з ключових векторів дестабілізації демократичних режимів. У зв'язку з цим НАТО активізує співпрацю з Європейським Союзом, ООН, ОБСЄ, а також

запроваджує такі інноваційні інституції, як Віртуальна система підтримки кіберінцидентів (VCISC) та Інтегрований центр кіберзахисту НАТО, спрямовані на підвищення ситуаційної обізнаності, оперативного реагування та колективного захисту в кіберпросторі [8]. Зміцнення кіберрезильєнтності стало не лише питанням технічного захисту, а й важливим елементом стратегічного фінансового планування, особливо в контексті розподілу ресурсів між традиційними (матеріально-технічними) та нематеріальними сферами оборони.

Кіберзагрози нового покоління мають багаторівневу природу. Йдеться як про атаки на критичну інфраструктуру (енергосистеми, логістичні ланцюги, фінансові системи), так і про складні операції впливу через соціальні мережі та дезінформаційні кампанії. Понад 80% країн НАТО у 2023 р. зазнали хоча б однієї масштабної кібератаки на державні або стратегічні об’єкти [9] (рис. 2).

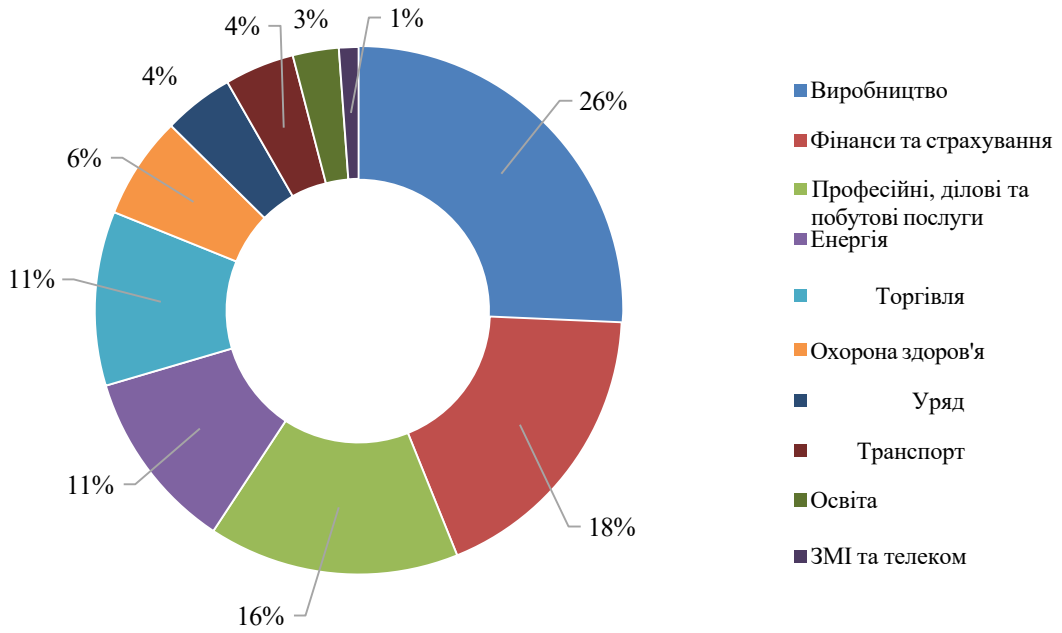


**Рис. 2. Розподіл кібератак у світових галузях економіки, 2023 р., %**

*Джерело*: побудовано автором на основі [7]

В умовах збройної агресії російської федерації проти України саме цифровий фронт набув особливого значення. Паралельно з фізичними атаками

російські хакерські угруповання здійснюють численні втручання в урядові системи, телекомунікаційну інфраструктуру та об'єкти енергетики, що підтверджується звітами Microsoft [10] та Recorded Future [11]. Особливого занепокоєння викликає цілеспрямована зловмисна діяльність державних органів рф у кіберпросторі, яка має ознаки системного втручання у внутрішні справи як держав-членів НАТО, так і партнерів. У 2023 р. ідентифіковано щонайменше 50 небезпечних атак, здійснених військовими угрупованнями, серед яких UAC-0056 (Ember Bear), UAC-0028 (APT28) та UAC-0082 (Sandworm), що мають безпосередній зв'язок із російськими державними структурами. Зокрема, щонайменше 11 інцидентів, які пов'язують безпосередньо з ГУР, були класифіковані як такі, що мають високий або критичний рівень тяжкості [12].

Аналітика за період з липня 2023 р. по червень 2024 р. засвідчує, що серед головних цілей російських хакерських кампаній залишаються державні установи, які становлять понад 33% усіх атак, що здійснюються російськими угрупуваннями (рис. 3).

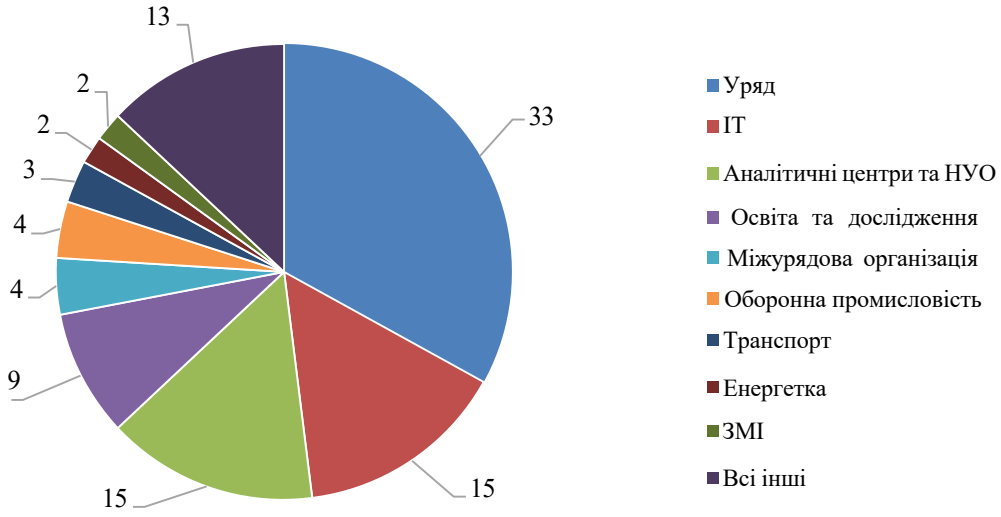


**Рис. 3. Цілі російських кібератак проти інших країн світу, в тому числі України, з липня 2023 р. по червень 2024 р.**

*Джерело*: побудовано автором на основі [12]

Наступними за ступенем загроз є IT-сектор, аналітичні центри, а також неурядові організації. Сукупно на ці сфери припадає понад 15% атак. Значна частка атак, понад 9%, спрямована також на освітні установи, що вказує на розширення вектора впливу на гуманітарну сферу та молодіжне середовище, з метою довгострокової інформаційної дестабілізації. Таке спрямування агресії свідчить про прагнення російської федерації не лише завдати технічної шкоди, але й вплинути на інституційну сталість, стратегічну автономність та довіру до публічних органів демократичних держав. В умовах стрімкої гібридизації конфліктів, кібероперації стають інструментом стратегічного шантажу, політичного тиску та порушення інформаційної суверенності, що вимагає від НАТО суттєвого посилення колективного кіберзахисту.

На тлі зростаючої складності кіберзагроз НАТО системно нарощує власні спроможності. Комплексна політика кіберзахисту, оновлена у 2021 р., підтримує загальну позицію Альянсу в системі стримування, сприяє формуванню стандартів кібербезпеки та впровадженню міжсекторальної взаємодії. У 2023 р. на саміті у Вільнюсі було затверджено нову концепцію кіберзахисту, що передбачає активнішу інтеграцію цифрових інструментів у систему колективної оборони, а також запуск Віртуальної системи підтримки кіберінцидентів НАТО (VCISC), яка надає країнам-членам можливість оперативної взаємодії під час кризових інцидентів [13]. Подальше посилення цифрового компоненту відбулося на саміті НАТО у Вашингтоні в 2024 р., де було ухвалено рішення про створення Інтегрованого центру кіберзахисту НАТО. Його завданням стане не лише моніторинг та протидія кіберзагрозам, а й стратегічне прогнозування, оперативне реагування та координація дій із партнерами, зокрема Європейським Союзом, Організацією Об’єднаних Націй і ОБСЄ [14].

Серед основних напрямів роботи НАТО у сфері кібербезпеки слід віднести проведення регулярних тренувань, міжурядових навчань, аналіз

національних політик країн-членів, а також забезпечення платформ для обміну досвідом та практиками. Ухвалене у 2016 р. Зобов'язання щодо кіберзахисту, а також його оновлення у 2023 р., фіксують прагнення Альянсу до створення спільних стандартів протидії цифровим загрозам, особливо у контексті захисту критичної інфраструктури. Таким чином, НАТО дедалі активніше реалізує інтегровану модель кібероборони як ключового елементу сучасної концепції стримування, що вимагає адекватного фінансового забезпечення, модернізації цифрових інфраструктур, а також розвитку людського капіталу – від технічних спеціалістів до аналітиків стратегічного рівня.

**Висновки.** Проведене дослідження довело, що зростаюча складність, частота і багатовекторність кіберзагроз у XXI ст. детермінують необхідність фундаментальної трансформації оборонної політики Північноатлантичного альянсу. В умовах, коли кібератаки дедалі частіше мають наслідки, співмірні із застосуванням збройної сили, кібербезпека більше не може розглядатись як периферійна чи суто технічна проблема. Натомість вона перетворюється на базовий компонент стратегічного управління, на рівні з класичними військовими компонентами – суходолом, морем, повітрям і космосом.

Встановлено, що рішення, ухвалені на самітах НАТО у Вільнюсі (2023 р.) та Вашингтоні (2024 р.), сприяли поступовій інституціоналізації кіберпростору. У рамках цієї трансформації відбувся не лише перегляд стратегічних підходів до стримування, але й адаптація бюджетної політики НАТО, зокрема шляхом інтеграції питань, пов'язаних з кіберзахистом, у систему стратегічного планування, а витрат на їх розв'язання – у фінансову структуру Програми інвестицій у безпеку (NSIP), а також Цивільного бюджету Альянсу. Особливе місце при цьому посідають проєкти у сфері розвитку комунікаційної інфраструктури, раннього попередження, аналітичної обробки даних і штучного інтелекту. Таким чином, вектор цифрової безпеки у діяльності НАТО поступово еволюціонує від допоміжного елементу до

системоутворюючого чинника, що формує нові параметри політики стримування, колективної безпеки та фінансової стійкості Альянсу. Кібербезпека виступає не лише як оперативна необхідність, а як ідеологічна основа нової парадигми безпеки, що охоплює як фізичну, так і інформаційну територію союзників.

**Список використаних джерел**


1. Горлинський В., Горлинський Б. Кіюербезпека як складова інформаційної безпеки України. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13). С.136-148.
2. Діордіца І. В. Поняття та зміст кіберзлочинності. Глобальна організація союзницького лідерства. URL:http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti
3. Лугіна Н. А. Перспективи та тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. Соціологія права. 2022. Вип. 1-2. - С. 58-60. URL:http://nbuv.gov.ua/UJRN/sprav_2022_1-2_13
4. Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science. 2019. Vol. 149. P. 65–70. URL: https://doi.org/10.1016/j.procs.2019.01.108
5. NATO. Cyber defence. NATO Topics. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm
6. NATO. Cyber Defence Pledge – Enhanced Commitments. NATO Official Website. URL: https://www.nato.int/cps/en/natohq/topics_132160.htm
7. Statista. Annual number of political cyberattacks worldwide 2014–2024 YTD. URL: https://www.statista.com/statistics/1298650/political-cyberattacks-worldwide/
8. NATO. Vilnius and Washington Summits – Outcomes and Strategic Concepts. NATO Official Reports. URL: https://www.nato.int

9. CyberPeace Institute. Cyber Attacks on Critical Infrastructure. Geneva: CPI. URL: https://cyberpeaceinstitute.org

10. Microsoft. Special Report: Ukraine – One Year of Russian Hybrid War. URL: https://www.microsoft.com/en-us/security/business/security-insider/reports/ukraine

11. Recorded Future. Russian Cyber Operations in Ukraine. URL: https://www.recordedfuture.com/blog/russian-cyber-operations-ukraine

12. Національний інститут стратегічних досліджень. Кіберзагрози та гібридні операції Російської Федерації: оцінка ризиків для національної безпеки України та партнерів НАТО. 2024. Київ: НІСД. URL: https://niss.gov.ua

13. NATO Summit Vilnius 2023 – Final Declaration. NATO. URL: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

14. NATO. Washington Summit Declaration 2024. URL: https://www.nato.int/cps/en/natohq/official_texts_227678.htm