Interdisciplinary Studies of Complex Systems
No. 27 (2025) 5–22

https://doi.org/10.31392/iscs.2025.27.005 UDC 001.891(1-622HATO)

Scientific and research aspects of NATO's activities

Borys Humeniuk[1]

Науково-дослідні аспекти діяльності НАТО

Борис Гуменюк

Abstract. In the current conditions of transformation of the global security environment, the study of the role of science and innovation in the activities of international security organizations is becoming increasingly important. Given the aggravation of hybrid threats, the growth of cyber risks, climate challenges and technological competition, the North Atlantic Alliance is adapting its strategic doctrine, integrating the research and development component as an important security tool. The article is devoted to the analysis of the scientific and technological dimension of NATO's activities, in particular through the prism of the Science for Peace and Security (SPS) program and the interaction of the Alliance with the scientific institutions of the member countries.

The aim of the study is to identify the mechanisms by which NATO implements innovative approaches to solving current security challenges, as well as to assess the effectiveness of the interaction between science, politics and the defense sector.

In the course of the research, a systematic and interdisciplinary approach was applied, which made it possible to comprehensively cover the functioning of NATO scientific initiatives, such as SPS, STO (Science and Technology Organization) and the NATO Center for Marine Research (CMRE).

It is determined that science in NATO not only supports the operational needs of the Alliance, but also forms long-term strategic decisions in the field of defense, cyber defense, energy and environmental security. Particular attention is paid to the analysis of applied projects implemented with the support of NATO in partnership with scientific institutions.

The conclusions emphasize the need for further development of institutional cooperation between NATO and the academic environment, in particular in the context of the war in Ukraine and growing competition at the global level. The emphasis is on the potential of science as a preventive safety tool and a source of technological advantage. The article confirms that the integration of scientific knowledge into security policy is a key condition for NATO's adaptation to the complex challenges of the 21st century.

Keywords: NATO, scientific activities of the alliance, NATO organizations, scientific research

[1] Dragomanov Ukrainian State University, Kyiv, Ukraine, b.gumeniuk@gmail.com, https://orcid.org/0000-0002-7152-8211

Анотація. У сучасних умовах трансформації глобального безпекового середовища дедалі більшого значення набуває дослідження ролі науки та інновацій у діяльності міжнародних безпекових організацій. З огляду на загострення гібридних загроз, зростання кіберризиків, кліматичні виклики та технологічну конкуренцію, Північноатлантичний альянс адаптує свою стратегічну доктрину, інтегруючи науково-дослідницьку складову як важливий інструмент забезпечення безпеки. Стаття присвячена аналізу науково-технологічного виміру діяльності НАТО, зокрема через призму програми «Наука заради миру і безпеки» (SPS) та взаємодії Альянсу з науковими установами країн-членів. Метою дослідження є виявлення механізмів, за допомогою яких НАТО впроваджує інноваційні підходи до вирішення актуальних безпекових викликів, а також оцінка ефективності взаємодії між наукою, політикою й оборонним сектором.
У процесі дослідження було застосовано системний і міждисциплінарний підхід, що дозволило комплексно охопити функціонування наукових ініціатив НАТО, таких як SPS, STO (Science and Technology Organization) і Центр морських досліджень НАТО (CMRE).
Визначено, що наука в НАТО не лише підтримує оперативні потреби Альянсу, а й формує довгострокові стратегічні рішення у сфері оборони, кіберзахисту, енергетичної та екологічної безпеки. Особливу увагу приділено аналізу прикладних проектів, що реалізуються за підтримки НАТО у партнерстві з науковими установами.
У висновках наголошено на необхідності подальшого розвитку інституційної співпраці між НАТО та академічним середовищем, зокрема в умовах війни РФ проти України та зростаючої конкуренції на глобальному рівні. Акцент зроблено на потенціалі науки як інструмента превентивної безпеки та джерела технологічної переваги. Стаття підтверджує, що інтеграція наукового знання у безпекову політику є ключовою умовою адаптації НАТО до складних викликів XXI століття.

Ключові слова: НАТО, наукова діяльність Альянсу, структури НАТО, наукові дослідження

1 Вступ

У сучасному безпековому середовищі, що характеризується динамічними змінами, зростанням гібридних загроз, мілітаризацією кіберпростору та розвитком новітніх технологій, забезпечення міжнародної стабільності набуває нового змісту. Традиційні засоби стримування все частіше виявляються недостатніми для ефективної протидії викликам, які виникають у сфері оборони, розвідки, комунікацій та критичної інфраструктури. У цьому контексті проблема інтеграції науки, інновацій і технологій у сферу безпеки стає однією з ключових як у теоретичному, так і в прикладному аспектах. Особливу роль у цьому процесі відіграє Північноатлантичний альянс (НАТО), який, адаптуючись до нових умов, посилює увагу до інноваційних розробок, міждисциплінарних досліджень та технологічної модернізації системи колективної безпеки. Проблема полягає в необхідності не лише розуміння науково-технологічного потенціалу Альянсу, а й в оцінці його реального впливу на здатність НАТО відповідати сучасним і майбутнім викликам. Таким чином, вивчення ролі науки, інновацій і технологій у діяльності НАТО є важливим як для формування науково-теоретичної бази з питань міжнародної безпеки, так і для розробки практичних рекомендацій щодо підвищення ефективності функціонування безпекових механізмів у глобальному масштабі.

2 Аналіз останніх досліджень і публікацій

Проблематика інтеграції науки та інновацій у безпекову політику НАТО знаходить відображення у працях західних дослідників, зокрема у звіті [8], де розглянуто потребу НАТО в стратегічному оновленні науково-технологічної політики. Деякі дослідники вже здійснювали спробу визначення поточного стану розвитку окремих напрямків розвитку наукового потенціалу НАТО, зокрема класифіковано шість напрямків досліджень, у яких Альянс розробляє свої технології, що впливають на високий рівень його мілітаризації: 1) великі дані, 2) автономія, 3) квантові технології, 4) штучний інтелект, 5) космічні технології, гіперзвукові можливості, 6) біотехнології та вдосконалення людини [4].

При цьому помітне значення відводиться і соціально-гуманітарній підтримці роботи НАТО, наприклад, сучасні автори доводять: поширений в емпіричній науці концепт «стійкість» наразі активно застосовується на практиці Міністерством оборони США та НАТО; в рамках нової структури НАТО позиціонуються «багаторівнева стійкість», коли оптимальна орієнтація на неї залишає відкритими можливості для трансформаційної адаптації та ідентичності [10]. Важливо також, що сучасні автори однаково значимими вважають спроможність НАТО розвивати дослідницькі зв'язки як з академічним сектором, так і з громадськими аналітичними організаціями, а також комерційними підприємствами та установами [див. напр. 7; 11].

Більшість актуальних публікацій з вказаної проблематики з'являється безпосередньо на ресурсах НАТО. Наприклад, практичні аспекти функціонування програми «Наука заради миру і безпеки» (SPS) та її еволюцію висвітлено у звіті [18], що акцентує увагу на розширенні співпраці з партнерами та зміщенні пріоритетів до гібридних загроз. Крім того, у доповіді [13] зазначено зростаючу роль інновацій для зміцнення спроможностей Альянсу.

Проте більшість наявних джерел акцентують або на загальній трансформації НАТО, або на практичних проєктах, залишаючи недостатньо опрацьованими такі аспекти, як стратегічна роль досліджень та інновацій в ухваленні рішень, інституційне оформлення науково-технічної співпраці та її вплив на політичну адаптацію Альянсу до нових викликів. Варто розглянути також основні науково-дослідницькі організації НАТО, їхню діяльність, місію та проекти. Саме на ці аспекти звертається увага в цій статті.

Метою цієї статті є дослідити, яким чином наукові дослідження та інновації інтегруються в сучасну безпекову політику НАТО, зосереджуючи увагу на ролі програми «Наука заради миру і безпеки» (SPS), а також проаналізувати внесок провідних науково-дослідницьких інституцій і академічних установ, які співпрацюють із НАТО, у формування технологічних рішень для протидії новітнім викликам у сфері безпеки.

Методи дослідження. У статті використано системний та інституційний аналіз для вивчення взаємозв'язків між наукою, інноваціями та безпековими підходами НАТО, а також аналіз офіційних звітів і публікацій Альянсу та партнерських наукових організацій. Порівняльний метод дозволив оцінити приклади міжнародної співпраці та визначити ефективні практики інтеграції наукового потенціалу у сферу безпеки.

3 Результати та дискусії

Північноатлантичний альянс (НАТО) є не лише військово-політичною організацією, але й потужною платформою для наукових досліджень і технологічних інновацій. У рамках своєї діяльності НАТО підтримує низку дослідницьких центрів, лабораторій і аналітичних установ, що працюють над розробкою передових технологій у сфері оборони, кібербезпеки, стратегічних комунікацій та енергетичної безпеки. Завдяки співпраці з провідними науковими установами світу Альянс посилює свою здатність протистояти сучасним викликам і загрозам, роблячи ставку на технологічну перевагу та інноваційний розвиток.

Наукові дослідження та технологічні інновації відіграють ключову роль у розвитку оборонних можливостей НАТО, сприяючи адаптації Альянсу до сучасних викликів безпеки. Інтеграція науки у військову сферу дозволяє ефективніше прогнозувати загрози, удосконалювати системи управління та розробляти новітні технологічні рішення для забезпечення стійкості та обороноздатності.

Оборонні концепції НАТО базуються на розвитку передових технологій, тобто на штучний інтелект, автономні системи, кібербезпеку, аналіз великих даних, автоматизацію ухвалення рішень тощо. Наукові дослідження у цих сферах спрямовані на підвищення ситуаційної обізнаності, покращення контролю операцій та розширення можливостей реагування на кризові ситуації. Одним із основних аспектів наукової діяльності є впровадження міждисциплінарного підходу, який поєднує військову аналітику, інформаційні технології та соціальні науки. Це дозволяє краще розуміти складні геополітичні процеси, аналізувати динаміку конфліктів і формувати ефективні стратегії протидії загрозам. Особлива увага приділяється питанням інформаційної безпеки та стійкості комунікаційних систем. Дослідження в цій сфері спрямовані на розробку методів захисту від кібератак, а також на аналіз інформаційних потоків для виявлення дезінформації та гібридних загроз. НАТО також активно співпрацює з науковцями, експертами та технологічними компаніями для впровадження інновацій у сфері оборони. Така взаємодія сприяє розробці нових підходів до управління ресурсами, прогнозування загроз та зміцнення стратегічного потенціалу. Таким чином, наука та наукові установи є невід'ємною частиною розвитку оборонної політики НАТО. Завдяки дослідженням та технологічним розробкам Альянс забезпечує варіативність та адаптивність, зміцнює обороноздатність та підтримує безпеку в умовах постійних змін у міжнародному середовищі.

Однією з найбільш революційних технологій, що змінює кіберпростір, став *штучний інтелект та машинне навчання*. З одного боку, вони дозволяють ефективніше захищати інформаційні системи, виявляючи та нейтралізуючи загрози в режимі реального часу. Однак фахівці застерігають: ті ж технології можуть бути використанні зловмисниками для автоматизації атак, підвищення їх складності та масштабності. Ворожі актори застосовують алгоритми для аналізу вразливостей, створення складних фішингових кампаній або розробки унікального шкідливого програмного забезпечення, яке складно виявити традиційними методами. Не менш значущим є

розвиток квантових обчислень, який у перспективі може зламати сучасні криптографічні системи. Сучасні алгоритми шифрування, які використовуються для захисту комунікацій та даних, можуть стати вразливими перед квантовими атаками. Це створює проблему для НАТО, адже необхідно розробляти нові криптографічні рішення, які будуть стійкими до атак квантових комп'ютерів. При чому, вчені підкреслюють, що розгортання 5G-мереж та поширення пристроїв Інтернету речей (IoT) також розширює можливості для вчинення злочинів. Через величезну кількість підключених пристроїв, більшість з яких має слабкі системи безпеки, хакери можуть використовувати їх для організації DDoS-атак, крадіжки конфіденційної інформації або створення ботнетів. Особливо небезпечною є можливість віддаленого проникнення у критичну інфраструктуру, що може паралізувати роботу стратегічно важливих об'єктів. Нові кіберзагрози, що виникають, вимагають від НАТО перегляду своїх підходів до кібероборони. По-перше, Альянс повинен розвивати технологічну співпрацю між країнами-членами, щоб забезпечити синхронізовану реакцію на загрози. Особливий акцент робиться на розширенні партнерств із приватним сектором, науковими установами та стартапами у сфері кібербезпеки. По-друге, НАТО необхідно інвестувати у розробку квантостійкої криптографії та нових методів захисту інформаційних систем. Важливим напрямом є впровадження засобів для автоматизованого аналізу загроз, які базуються на штучному інтелекті, та розробка проактивних заходів кібербезпеки. По-третє, кібероперації стають все більш важливими у сучасній військовій доктрині. НАТО визнає кіберпростір, як окрему сферу ведення бойових дій, поряд із сушею, морем, повітрям, космосом. Погодимося, це означає, що Альянс повинен розробляти стратегії не лише для оборони, а й для ведення наступальних кібероперацій, щоб стримувати потенційних супротивників. З огляду на все вищесказане, зрозуміло, що технологічний прогрес має двоякий вплив: з одного боку, він надає потужні інструменти для захисту кіберпростору, а з іншого — створює нові вразливості, які можуть використовувати зловмисники. НАТО має адаптувати свої наукові лани досліджень і стратегії, щоб залишатися ефективною силою в умовах стрімких змін у сфері кібербезпеки [9, С. 88–108].

У сучасному безпековому середовищі, де інформація відіграє ключову роль, НАТО активно впроваджує *технології аналізу великих даних та автоматизацію процесів ухвалення рішень*, що дає змогу Альянсу швидко адаптуватися до нових викликів, ефективно обробляти величезні масиви інформації та покращувати планування стратегій. Вчені стверджують, що використання великих даних дозволяє аналізувати інформацію з різних джерел, зокрема розвідувальних супутникових знімків, даних безпілотників, кіберрозвідки, польових звітів і відкритих джерел. Завдяки штучному інтелекту та машинному навчанню НАТО отримує можливість швидко ідентифікувати потенційні загрози, прогнозувати можливі сценарії розвитку подій і пропонувати оптимальні варіанти дій. Однак, величезний обсяг інформації та необхідність швидкого реагування вимагають автоматизації процесів ухвалення рішень. Інструменти штучного інтелекту допомагають аналізувати ситуацію в реальному часі, виявляти аномалії, що можуть сигналізувати про загрози, та оптимізувати військові операції.

Особливе значення ті ж дослідники відводять автоматизованим системам, що підвищують рівень ситуаційної обізнаності й мають змогу забезпечувати ефективне управління ресурсами. Водночас, попри високий рівень автоматизації, у процесі ухвалення стратегічних рішень зберігається людський контроль. Як військово-політичний союз, НАТО діє на основі консенсусу між державами-членами, що гарантує прозорість і відповідальність процесу. Жодне важливе рішення не ухвалюється без людського втручання, а алгоритми та автоматизовані аналітичні системи використовуються лише як допоміжні інструменти. Важливо, що застосування технологій аналізу великих даних та автоматизації відбувається в межах юридичних та етичних норм у згоді з принципами Альянсу. Інтеграція передових технологій у діяльність НАТО дозволяє Альянсу оперативно реагувати на загрози, а також покращувати координацію між союзниками, забезпечуючи високий рівень колективної безпеки. Проте, у світі, де технології розвиваються надзвичайно швидко, головним викликом все ще є пошук балансу між автоматизацією та людським контролем. Саме тому, підсумовують аналітики, НАТО продовжує роботу з інтеграцією штучного інтелекту та великих даних у свої стратегії, дотримуючись принципу консенсусу й відповідальності в ухваленні рішень [12].

Безпекове середовище, що швидко змінюється, стимулює НАТО зосереджувати значні зусилля на *впровадженні новітніх технологій* і адаптації до нових загроз. Інноваційні технології не лише змінюють характер сучасної війни, а й визначають здатність Альянсу підтримувати військову перевагу та ефективно реагувати на нові виклики. В умовах глобальної конкуренції та технологічного розвитку НАТО приділяє особливу увагу модернізації своїх військових можливостей і посиленню співпраці з цивільним сектором. Одним із основних аспектів цього процесу є впровадження NATO 2030 — комплексної стратегії, направленої на інтеграцію передових технологій та розширення спроможностей Альянсу. Ця ініціатива передбачає посилення технологічної взаємодії між державами-членами, розвиток оборонної інфраструктури та впровадження нових стандартів у сфері стримування та оборони. Важливе місце у цій стратегії займає оцінка технологічного потенціалу цивільно-військової співпраці, яка дозволяє НАТО швидше реагувати на нові виклики та розробляти ефективніші механізми захисту. Дослідники питання акцентуєть на технологічній конвергенції, яка сприяє інтеграції військових і цивільних інноваційних рішень. Цей підхід дозволяє використовувати напрацювання приватного сектору, стартапів та наукових установ у розробці нових оборонних технологій. У цьому контексті ключову роль відіграє поглиблення співпраці між НАТО та Європейським Союзом, що забезпечує обмін знаннями, ресурсами та технологічними рішеннями. Також ще одним важливим напрямом є розширення партнерських ініціатив у сфері штучного інтелекту, автономних систем, кібербезпеки та аналізу великих даних. Впровадження цих технологій дозволяє НАТО підвищити ситуаційну обізнаність, покращити координацію військових операцій та оптимізувати процес ухвалення рішень. Таким чином, сучасна стратегія НАТО спрямована на те, щоб інновації не лише підтримували адаптацію Альянсу до змін, а й всіляко випереджали потенційні виклики у сфері безпеки. Інтеграція передових технологій,

посилення співпраці з державами-членами та цивільним сектором, а також розширення міжнародних партнерств — усе це, на думку дослідників, сприяє посиленню оборонних можливостей і гарантуванню безпеки у довгостроковій перспективі [19].

Важливо також окреслити, що науково-дослідні напрями роботи НАТО нерідко пов'язанні з недержавним сектором, зважаючи на специфіку академічної та аналітичної роботи в різних країнах. Зокрема Д. Шаротт, Ф. Коллі та І. Рейкерс досліджують таку взаємодію між НАТО та неурядовими організаціями (НУО) у сфері захисту цивільних осіб. Вони аналізують, як і чому НАТО почало активно співпрацювати з НУО, незважаючи на традиційну закритість військових структур до зовнішнього впливу. *Залучення НУО* до розробки політик із захисту цивільного населення стало важливим кроком у трансформації Альянсу. Традиційно військові організації обмежували контакти з громадянським суспільством, однак з часом з'ясувалося, що НУО володіють унікальними знаннями та експертизою, які можуть бути корисними під час проведення операцій чи розробок. Особливо це стало очевидним у випадках складних гуманітарних криз, коли військові місії потребували розширеного розуміння соціальних, економічних і політичних аспектів конфлікту. Автори статті пояснюють цей процес через концепцію організаційного навчання. НАТО змушене було адаптуватися до сучасних викликів і шукати альтернативні підходи до управління операціями. У цьому контексті співпраця з НУО стала не лише засобом покращення ефективності військових місій, а й важливим елементом стратегічного планування. Представники громадянського суспільства надавали НАТО аналітичні матеріали, допомагали розробляти політичні стратегії, орієнтовані на захист мирного населення, а також сприяли розробці нових стандартів ведення бойових дій із врахуванням гуманітарного аспекту. У статті зазначається, що одним із ключових викликів була відмінність у підходах до ухвалення рішень. НАТО працює на основі консенсусу між державами-членами, в той час як НУО мають гнучкіші механізми реагування на кризи, що виникають. Це створювало труднощі в координації дій, однак згодом Альянс адаптував свої механізми взаємодії, що сприяло більшій ефективності місій. Окремо автори наголошують на тому, що взаємодія між військовими структурами та НУО сприяла розвитку нових стандартів у військових операціях, НАТО почало враховувати гуманітарні ризики ще на етапі планування операцій, що дозволило знизити кількість жертв серед мирного населення. Крім того, Альянс став більш прозорим та відкритим у питаннях використання сили та військових інтервенцій [7].

Співпраця між НАТО та НУО є ефективним інструментом захисту цивільного населення. Вона дозволяє поєднати військові можливості Альянсу з експертизою громадянського суспільства, що сприяє більш гуманному та стратегічно виваженому підходу до ведення сучасних конфліктів. У перспективі така взаємодія може стати важливим механізмом для зміцнення міжнародної стабільності та запобігання гуманітарним кризам.

Стрімкий розвиток новітніх технологій суттєво впливає на глобальну систему безпеки та військові стратегії НАТО. Військові операції більше не обмежуються традиційними фізичними просторами — вони тепер охоплюють кібернетичний та космічний домени, що створює нові викли-

ки та можливості для наукової діяльності Альянсу. Однією з ключових тенденцій наукових розробок є *розширене використання безпілотних літальних апаратів (БПЛА) та автономних бойових платформ.* Сучасні БПЛА можуть виконувати розвідувальні, ударні та логістичні завдання без прямого втручання оператора. Впровадження роєвих технологій (swarm technology), коли сотні автономних дронів працюють у синхронізації, значно ускладнює протидію традиційними методами. Окрім повітряних дронів, активно розвиваються наземні та морські автономні системи, які можуть виконувати завдання з розвідки, розмінування, атак на ворожі об'єкти та навіть забезпечення логістики. Усе це формує нову тактику ведення бойових дій, де автономні машини стають ключовими учасниками бойових операцій. Також космос стає критично важливою ареною військових операцій. НАТО визнає космічний простір як стратегічний домен, у якому забезпечення домінування в розвідці, зв'язку та навігації має велике значення. Супутникові угруповання Альянсу використовуються для відстеження військових переміщень противника, управління бойовими операціями та забезпечення точності високоточної зброї. Розвиток протисупутникової зброї з боку потенційних супротивників (зокрема Росії та Китаю) стимулює НАТО розробляти засоби захисту орбітальних активів, включно з маневреними супутниками, технологіями штучного інтелекту для автоматичного ухилення від атак та системами активного захисту супутників. У чомусь подібним фронтом, де ведуться сучасні конфлікти, і де активно розвивається аналітична діяльність, став кіберпростір. Удосконалені кібератаки можуть виводити з ладу критичні інфраструктури, системи зв'язку, логістичні платформи та навіть автоматизовані оборонні механізми. НАТО інвестує у розвиток штучного інтелекту для виявлення та нейтралізації кіберзагроз, а також працює над створенням адаптивних мережевих архітектур, здатних самостійно відновлюватися після атак. Електронна війна (Electronic Warfare) стає одним з важливих інструментів у протистоянні з ворогами. Глушіння радіочастотних каналів, перехоплення та модифікація сигналів, створення хибних цілей та маніпулювання сенсорами противника — усе це стає невід'ємною частиною сучасного поля бою [11], а також і сучасного наукового пошуку.

Втім цей вимір досліджень потребує залучення додаткових зацікавлених акторів політики. Щоб максимально використати переваги нових технологій, НАТО реформує свою командну структуру та адаптує концепцію багатодоменних операцій (MDO). Це передбачає інтеграцію всіх військових доменів (сухопутного, морського, повітряного, кібернетичного та космічного) в єдиний бойовий механізм, що діє швидко та скоординовано. Одним із ключових аспектів такої інтеграції є єдина інформаційна платформа НАТО, яка дозволяє обмінюватися розвідувальними даними, автоматично оцінювати загрози та надавати рекомендації щодо дій у реальному часі. Тож важливим фактором є *взаємодія з комерційним технологічним сектором.* Оскільки приватні компанії часто випереджають державні установи у розробці новітніх технологій, НАТО активно співпрацює з технологічними гігантами, стартапами та приватними дослідницькими інститутами для впровадження нових рішень у військову сферу. Погодимося з дослідниками, що попри всі переваги технологічного прогресу,

впровадження інновацій у військову сферу стикається з низкою труднощів: 1) високий рівень витрат, оскільки розробка та впровадження передових військових технологій потребують значних фінансових ресурсів, що не всі країни-члени НАТО можуть собі дозволити; 2) різний рівень технологічного розвитку союзників, через те, що деякі країни Альянсу мають обмежені можливості для адаптації нових військових рішень, а це створює нерівномірний рівень боєздатності всередині блоку; 3) ризики кібершпигунства та саботажу через використання високотехнологічних систем, тож військова інфраструктура НАТО стає вразливою до хакерських атак та витоку конфіденційної інформації; 4) правові та етичні аспекти, наприклад, використання автономної зброї, бойових ШІ-систем та кібернетичних атак, які піднімають питання міжнародного права та військової етики [11].

Загалом науково-дослідні аспекти діяльності НАТО займають ключове місце в стратегічному розвитку Альянсу, забезпечуючи технологічну перевагу та адаптацію до сучасних викликів у сфері оборони й безпеки. Інновації та передові дослідження, що проводяться за підтримки НАТО, спрямовані на розвиток нових матеріалів, кіберзахисту, штучного інтелекту, квантових технологій, біотехнологій та інших перспективних напрямків, які можуть кардинально змінити характер ведення військових операцій та підхід до оборонного планування. Наукова діяльність Альянсу не лише формує майбутнє військових технологій, а й сприяє тісній кооперації між союзниками та міжнародними партнерами, забезпечуючи спільний підхід до розвитку безпекових стратегій.

Особливе місце у фінансуванні та координації наукових досліджень займає *програма НАТО «Наука заради миру та безпеки» (SPS)*. Це ключовий механізм підтримки досліджень у сферах, які безпосередньо впливають на оборону та стійкість до нових загроз. Програма надає гранти, організовує спільні наукові проєкти та сприяє обміну знаннями між країнами-членами та партнерами Альянсу. Значна увага приділяється розвитку новітніх матеріалів, що можуть підвищити безпеку та мобільність військових підрозділів, а також сприяти технологічному реформуванню оборонної інфраструктури. Серед таких досліджень виділяються проєкти, спрямовані на створення ультралегких і надміцних броньованих матеріалів, самовідновлюваних покриттів, а також передових наноструктур, здатних сильно підвищити стійкість техніки до ворожих атак. На додаток до технологічних досліджень НАТО активно підтримує ініціативи у сфері енергетичної безпеки, що спрямовані на розробку стійких джерел живлення для військових баз і мобільних підрозділів. Дослідження в цьому напрямку охоплюють альтернативні енергоносії, ефективні системи накопичення енергії та технології автономного енергозабезпечення. Зокрема, розробляються ефективні рішення для використання відновлюваних джерел енергії в умовах бойових дій, які можуть суттєво підвищити автономність військових формувань та знизити їхню залежність від традиційних паливних ресурсів. Не менш важливим напрямком досліджень також є розвиток передових сенсорних систем та біометричних технологій, які дозволяють значно покращити рівень безпеки як на військових, так і цивільних об'єктах. Використання розширених сенсорів у поєднанні з алгоритмами штучного інтелекту дає можливість автоматично ідентифікувати потенційні загрози —

це може значно скоротити час реакції на небезпеку. Особливо перспективним є застосування таких технологій у системах раннього попередження про терористичні загрози та несанкціоноване проникнення на об'єкти критичної інфраструктури. Однак, попри численні переваги впровадження новітніх технологій, їх розвиток супроводжується низкою викликів. Однією з головних проблем є фінансове навантаження на бюджети країн-членів НАТО, оскільки розробка та впровадження передових військових технологій потребує вкладання значних ресурсів. Ще однією складністю є різний рівень технологічної спроможності країн Альянсу, що створює певні перешкоди у процесі інтеграції інноваційних рішень. Крім того, вже згадані вище виклики кібербезпеки та ризики шпигунства з боку ворожих держав потребують постійного вдосконалення механізмів захисту та конфіденційності в т.ч. і дослідницької інформації [16].

Варто розглянути детальніше *основні установи, що забезпечують науково-дослідницьку діяльність НАТО*, їхню історію, діяльність і спеціалізацію, для кращого розуміння наукового підходу Альянсу.

Одна з організацій, яка є ключовою для НАТО є організація НАТО з науки і технологій (STO), що відповідає за координацію науково-дослідної діяльності та технологічного розвитку. Її мета полягає у забезпеченні технологічної переваги НАТО через обмін знаннями, впровадження інновацій та підтримку наукових досліджень у сфері оборони. STO об'єднує понад 5000 вчених та інженерів із більш ніж 40 країн, які щорічно працюють над приблизно 350 науково-дослідними проектами. STO була створена у 2012 році через реорганізацію попередньої Організації НАТО з наукових досліджень і технологій (RTO), яка виникла в 1998 році в результаті злиття двох окремих груп: Консультативної групи аерокосмічних досліджень (AGARD) та Групи з оборонних досліджень (Defence Research Group, AC/243). Ця реорганізація була спрямована на підвищення ефективності науково-дослідної діяльності НАТО та оптимізацію використання ресурсів.

Серед основних напрямів діяльності організації визначають:

1) прикладні технології транспортних засобів — удосконалення військової техніки на суші, морі, у повітрі та космосі;
2) людські фактори та медицина — оптимізація здоров'я та працездатності військовослужбовців у польових умовах;
3) інформаційні системи та технології — розробка методів управління, зв'язку та штучного інтелекту, а також зміцнення кібербезпеки;
4) системний аналіз та дослідження — підтримка стратегічного планування та прийняття рішень у сфері оборони;
5) концепції та інтеграція систем — розробка новітніх військових технологій та їх інтеграція в системи НАТО;
6) сенсори та електронні технології — створення передових розвідувальних і спостережних систем.

Структурно STO складається з кількох основних компонентів, що будуть викладені далі. Головний офіс розташований у штаб-квартирі НАТО в Брюсселі та відповідає за стратегічне керівництво науково-технічною діяльністю Альянсу. Далі офіс підтримки співробітництва, який базується

в Парижі та відповідає за координацію та адміністративну підтримку наукових програм і проектів. Третій основний компонент Центр морських досліджень та експериментів (Centre for Maritime Research and Experimentation, CMRE), що розташований у Ла-Спеції, Італія, спеціалізується на дослідженнях і розробках у морській сфері для забезпечення оборонних потреб військово-морських сил Альянсу. Центр був створений у 1959 році під назвою SACLANTCEN і згодом відомий як Центр підводних досліджень НАТО (NATO Undersea Research Centre). Також серед форматів діяльності STO існують різноманітні науково-технічні заходи, які спрямовані на обмін знаннями та дослідницьким досвідом серед науковців. У переліку таких заходів є семінари та симпозіуми, зосереджені на обговоренні актуальних наукових питань і представленні новітніх досліджень, форуми та лекторії для дискусій та навчання, де експерти діляться своїми знаннями з учасниками. До всього вищесказаного додаються ще кооперативні демонстрації технологій (Cooperative Demonstration of Technology, CDT), як практичні покази нових технологічних рішень, що сприяють їх впровадженню та адаптації в рамках діяльності НАТО (*About the NATO science and technology organization (STO)*). STO відіграє критично важливу роль у підтримці наукового потенціалу НАТО, забезпечуючи його здатність реагувати на сучасні виклики безпеки та оборони.

Інша наукова діяльність, пов'язана з НАТО, зосереджена саме на комунікаційних стратегіях, це Центр передового досвіду НАТО з питань стратегічних комунікацій (*NATO StratCom COE*) і є міжнародною організацією, акредитованою НАТО, яка надає експертні знання та досвід у сфері стратегічних комунікацій, сприяючи підвищенню спроможностей Альянсу та його партнерів. Центр розпочав свою діяльність у січні 2014 року, а 1 липня того ж року сім держав-членів — Естонія, Німеччина, Італія, Латвія, Литва, Польща та Сполучене Королівство — підписали меморандуми про взаєморозуміння щодо його створення. 1 вересня 2014 року центр отримав акредитацію НАТО, і, як зазначено в Декларації саміту в Уельсі 2014 року, союзники привітали «...створення StratCom COE як значущий внесок у зусилля НАТО...» у сфері стратегічних комунікацій. Діяльність цього центру полягає в покращенні спроможностей НАТО, союзників і партнерів у сфері стратегічних комунікацій шляхом надання комплексного аналізу, своєчасних рекомендацій і практичної підтримки. Основна увага зосереджена на аналізі цифрового середовища, зокрема дослідженню новітніх технологій та штучного інтелекту, для створення повної та практичної бази знань для фахівців у галузі стратегічних комунікацій [14].

Розташований у Ризі (Латвія), центр був заснований з метою надання реального внеску в розвиток стратегічних комунікаційних спроможностей НАТО, його союзників і партнерів. Експертиза центру сформована шляхом поєднання знань із різних секторів: військового, приватного, державного та академічного, що дозволяє ефективно застосовувати дослідження для виявлення та управління новими загрозами в інформаційному середовищі. Наразі команда центру складається з висококваліфікованих експертів із 17 країн, а його директором є латвієць Яніс Сартс. Фінансування та комплектування персоналом центру здійснюється за рахунок країн-учасниць та країн, що сприяють його діяльності. Початково заснований у 2014 році

сімома країнами, центр згодом розширився: Нідерланди та Фінляндія долучилися у 2016 році, Швеція — у 2017, Канада — у 2018, Словаччина — на початку 2019, Данія та США — у 2020, Угорщина — у 2021, Іспанія — у 2024 році. Франція та Австралія ініціювали процес приєднання. За перших дев'ять років повноцінної діяльності NATO StratCom COE зарекомендував себе як один із провідних дослідницьких та аналітичних центрів з питань стратегічних комунікацій, протидії дезінформації, аналізу тенденцій у цифровій безпеці та вивчення стратегій, тактик і методів ворожих акторів у євроатлантичному регіоні. Центр проводить дослідження у відповідь на потреби Альянсу та країн-учасниць, розробляє навчальні програми та допомагає розвитку військових спроможностей НАТО [20].

Загалом Альянс поширює свою діяльність не лише виключно на дослідницьку чи наукову сфери, а й також на *академічний кадровий та освітній напрями*. Прикладом цього є Оборонний коледж НАТО (NDC), що визнається академічною установою Альянсу, яка спеціалізується на стратегічних дослідженнях, вищій військовій освіті та підготовці керівного складу НАТО. Він займає важливу роль у формуванні стратегічного мислення та підтримці військово-політичного діалогу серед держав-членів Альянсу та його партнерів. NDC був заснований 19 листопада 1951 року в Парижі за ініціативою генерала Двайта Д. Ейзенхауера, який на той момент був на посаді Верховного головнокомандувача Об'єднаних збройних сил НАТО в Європі (SACEUR). Його бачення полягало у створенні навчального закладу, який би готував військових і цивільних лідерів до ефективного керівництва та стратегічного планування в умовах нової реальності безпеки після Другої світової війни. У 1966 році з причини виходу Франції з інтегрованої військової структури НАТО, коледж був перенесений до Риму, де й знаходиться на теперішній час. Місія та основні завдання NDC зосереджені на стратегічному рівні та орієнтовані на підготовку високопосадовців країн-членів НАТО, партнерських держав і міжнародних організацій. Серед основних напрямів його діяльності надання навчальних програм для військових і цивільних фахівців, які займають керівні посади в структурах НАТО, урядах союзників та партнерів. Також коледж проводить дослідження з питань міжнародної безпеки, оборони та стратегічного прогнозування, розвиває стратегічне мислення в плані формування єдиного розуміння глобальних викликів серед лідерів Альянсу. NDC орієнтований на підтримку взаємодії між членами НАТО та партнерами для зміцнення міжнародного співробітництва шляхом обміну знаннями, спеціалістами та доступом.

Коледж пропонує кілька ключових освітніх програм:

1) Старший курс (Senior Course) — основна освітня програма, розрахована на 5 місяців. Вона призначена для військових і цивільних фахівців, які готуються до керівних посад у НАТО.
2) Курс для генералів, флагманських офіцерів і послів (Generals, Flag Officers and Ambassadors' Course, GFOAC) — короткострокова програма, орієнтована на найвищий рівень керівництва в Альянсі.
3) Курс для регіональних партнерів (Regional Cooperation Course, RCC) — спеціалізована програма для країн Середземноморського регіону та Близького Сходу.

4) Модульний підхід до стратегічного лідерства (Modular Short Courses, MSC) — серія короткострокових курсів, що охоплюють актуальні питання оборони й безпеки [15].

Дослідницький відділ коледжу активно займається аналітичними дослідженнями з питань безпеки, що мають стратегічне значення для Альянсу. Його експерти на регулярній основі публікують аналітичні звіти, статті та прогнози щодо сучасних геополітичних тенденцій. До основних видань можна віднести NDC Research Paper (глибокий аналіз актуальних проблем безпеки), NDC Policy Briefs (короткі огляди політичних рішень та рекомендацій), NDC Occasional Papers (дослідження, що висвітлюють ключові виклики для НАТО). Важливо також розглянути структуру Оборонного коледжу НАТО, яка складається з кількох ключових підрозділів, кожен з яких відповідальний за свою специфічну функцію. Департамент академічних операцій, відповідальний за освітню складову, а точніше за планування, координацію та реалізацію освітніх програм для коледжу. Науковою та дослідницькою діяльністю займається Дослідницький відділ NDC, який зосереджений проведенням наукової діяльності, публікацією аналітичних матеріалів та наданням експертних рекомендацій. За партнерства та співпрацю відповідальний департамент взаємодії, який також організовує конференції та семінари на важливі для НАТО теми. Оборонний коледж НАТО веде тісну співпрацю з військовими академіями держав-членів Альянсу, університетами, аналітичними центрами та міжнародними організаціями, що дозволяє розширювати академічну базу НАТО, залучати експертів та сприяти розробці інноваційних підходів у сфері міжнародної безпеки. Завдяки своїй багатогранній діяльності NDC відіграє ключову роль у формуванні стратегічного бачення НАТО, забезпечуючи високий рівень підготовки керівних кадрів і сприяючи єдності Альянсу перед сучасними викликами безпеки [3].

Однією з ключових складових глобальної стабільності у сучасному світі є морська безпека і саме тому НАТО приділяє особливу увагу дослідженням та розробкам у цій сфері. Для таких цілей було засновано вже згаданий раніше *Центр морських досліджень та експериментів НАТО* (CMRE), що базується в Італії. З 1959 року як науково-дослідний підрозділ НАТО Центр займається розробкою технологій для забезпечення морської безпеки і є частиною Науково-технологічної організації НАТО (STO) та працює над впровадженням інновацій у сфері морських досліджень, експериментальних технологій та ситуаційної обізнаності. Основною місією CMRE стала наукова підтримка військово-морських операцій НАТО шляхом досліджень, тестування новітніх технологій та розробки інтелектуальних систем для морських місій. Напрямки діяльності Центру досить широкі, до них входять літоральна розвідка, спостереження та рекогносцировка, використання безпілотних морських платформ для моніторингу акваторій та виявлення потенційних загроз, розробка та тестування заходів безпеки для критично важливої інфраструктури та транспортних шляхів, розширення ситуаційної обізнаності на морі разом зі створенням технологій для контролю морського простору та роботизована підготовка бойового простору із застосуванням безпілотних та інтелектуальних систем у військово-морських операціях. Варто згадати також технологічний

потенціал та флот центру, який використовується для проведення досліджень і тестувань технологій CMRE. NRV Alliance — 93-метрове судно, яке завдяки низькому рівню шуму є ідеальним для акустичних досліджень і протичовнової боротьби. CRV Leonardo — дещо менше за розмірами судно, яке використовується для експериментів у прибережних водах. Обидва кораблі оснащені передовими сенсорами та аналітичними системами, що дозволяють проводити найбільш точні дослідження морського середовища *(Centre for maritime research and experimentation).*

CMRE бере активну участь у міжнародних навчаннях, зокрема REPMUS (Robotic Experimentation and Prototyping with Maritime Unmanned System). Під час цих навчань тестуються автономні безпілотні апарати, які можуть використовуватись для боротьби з підводними човнами, розмінування акваторій та захисту підводної інфраструктури. У 2024 році до навчань REPMUS вперше долучилися Військово-морські сили України. Українська система DELTA успішно координувала роботу більш як 50 безпілотних морських апаратів, показуючи високу ефективність та перспективність використання подібних технологій у сучасних конфліктах. Одним з останніх напрямів досліджень CMRE є розробка нових технологій для захисту підводної інфраструктури. У центрі розробляються інструменти для підвищення ситуаційної обізнаності, що дозволить своєчасно виявляти загрози та оперативно реагувати на можливі атаки. Важливість цієї роботи в умовах гібридних загроз лише зростає через можливе використання підводних диверсійних засобів проти стратегічно важливих об'єктів, таких як газогони, телекомунікаційні кабелі та підводні системи зв'язку, що ми уже могли побачити у світлі недавньої історії. Центр морських досліджень та експериментів НАТО відіграє важливу роль у розробці передових морських технологій, що забезпечують обороноздатність Альянсу. Його дослідження, інновації та міжнародна співпраця сприяють зміцненню безпеки морського простору, адаптації до сучасних викликів і впровадженню новітніх технологій у військово-морські операції. Завдяки активному розвитку автономних систем, інтелектуального аналізу даних та захисту критичної морської інфраструктури CMRE залишається важливим центром морських досліджень, що формує майбутнє безпеки НАТО та його партнерів [5].

Агентство зв'язку та інформації НАТО (NCIA) є стратегічним підрозділом НАТО, який відіграє важливу роль у забезпеченні ефективного функціонування комунікаційних, інформаційних та кібернетичних систем Альянсу. Його діяльність спрямована на підтримку військових операцій, управління даними та забезпечення технологічних інновацій у сфері оборони. NCIA було створене 1 липня 2012 року, як наслідок об'єднання кількох організацій НАТО, що займалися інформаційними технологіями та зв'язком. Його коріння сягає понад 65 років назад, коли Альянс розпочав впровадження цифрових технологій для підвищення ефективності військового командування та координації операцій. Головний офіс NCIA розташований у Брюсселі, Бельгія. Крім цього, агентство також має оперативні центри в Монсі (Бельгія), Гаазі (Нідерланди) та Оейраші (Португалія), а також понад 30 регіональних представництв у Європі, Північній Америці та Азії. Це дозволяє забезпечити гнучке управління інформаційними мере-

жами та оперативний контроль за даними НАТО, які потрібно убезпечувати. NCIA відповідає за розвиток, впровадження та експлуатацію цифрових технологій у НАТО. Серед його діяльності такі ключові сфери: 1) комунікаційні системи: розгортання, підтримка та покращення мереж зв'язку НАТО, що забезпечують координацію між штабами, союзниками та військовими контингентами; 2) технології C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) — управління, зв'язок, комп'ютерні технології, розвідка, спостереження та рекогносцировка, що забезпечують оперативне командування військами; 3) кібербезпека та цифровий захист: безперервний моніторинг кіберпростору НАТО, виявлення загроз і розробка механізмів реагування на кібератаки; 4) протиракетна оборона: аналіз даних, стратегічне планування та інтеграція технологій для запобігання повітряним і ракетним загрозам; 5) великі дані (Big Data) та штучний інтелект: використання передових технологій для аналізу інформації, прогнозування загроз та прийняття рішень у реальному часі [1].

NCIA відіграє важливу роль у підтримці військових операцій Альянсу. Комунікаційні мережі підрозділу використовуються під час навчань, місій і стратегічних операцій, забезпечуючи надійний зв'язок між військовими контингентами. Окрім цього, агентство активно співпрацює з національними урядами, приватним сектором та науковими установами, що дозволяє інтегрувати інноваційні рішення у військову сферу. Одним із ключових аспектів цієї співпраці є розвиток кібербезпеки та протидія новітнім загрозам у цифровому середовищі. Серед пріоритетів діяльності NCIA впровадження інноваційних технологій для адаптації НАТО до сучасних викликів. Агентство розробляє та впроваджує рішення у таких сферах: 1) розвитку штучного інтелекту та алгоритмів машинного навчання для аналізу розвідданих і управління критичними системами; 2) хмарні технології: безпечне зберігання, обробка та передача даних між країнами-членами НАТО; 3) розвиток 5G-інфраструктури: забезпечення високошвидкісного зв'язку та його інтеграція у військові комунікаційні системи. Завдяки діяльності NCIA НАТО посилює свої можливості у сфері інформаційної безпеки, цифрових технологій та стратегічного планування, що є критично важливим для підтримання обороноздатності Альянсу в сучасному глобальному середовищі [1].

Розташований у Таллінні (Естонія) Центр передового досвіду з кооперативної кібероборони НАТО [17] є багатонаціональним та міждисциплінарним центром, який займається дослідженнями, навчанням та підготовкою з кібероборони. Він був заснований 14 травня 2008 року. У жовтні того ж року центр отримав повну акредитацію НАТО та статус міжнародної військової організації. Його місія полягає в наданні експертної підтримки країнам-членам НАТО шляхом проведення досліджень, розробки стратегій, організації навчань та створення аналітичних матеріалів щодо кібербезпеки. Беручи до уваги швидкий розвиток інформаційних технологій та кіберзагроз, діяльність центру охоплює чотири основні напрями: технології, стратегію, операції та право. CCDCOE проводить численні дослідження та розробляє аналітичні матеріали, які допомагають НАТО та країнам-союзникам бути готовими до нових викликів у сфері кібероборони.

Серед найважливіших проєктів центру — створення «Талліннського посібника», який є найповнішим науково-правовим дослідженням щодо застосування міжнародного права до кібероперацій. Окрім цього, центр підтримує інтерактивний кіберправовий інструментарій, що дозволяє фахівцям з права аналізувати кіберзагрози з точки зору міжнародного права. Важливим інформаційним ресурсом є також база даних INCYDER, яка містить ключові документи з кібербезпеки від основних міжнародних організацій та аналітичні матеріали експертів CCDCOE. Центр регулярно проводить аналіз стратегій та механізмів кібероборони країн-членів НАТО, оцінюючи рівень їхньої готовності до кіберзагроз та ефективність політики в цій сфері. Важливу роль у діяльності CCDCOE відіграє міжнародна співпраця. Наразі до центру входять 32 країни-члени НАТО, які беруть участь у його діяльності, а також 7 держав-партнерів, що не входять до Альянсу, проте активно співпрацюють із організацією. У березні 2022 року до центру приєдналася Україна, розширивши таким чином його міжнародне представництво. Співпраця з різними державами дозволяє CCDCOE отримувати широку експертизу у сфері кібербезпеки, розробляти найкращі практики та сприяти обміну інформацією між країнами. Окрім дослідницької діяльності, центр також організовує масштабні навчання та міжнародні заходи. Найвідомішим з них є "Locked Shields-— найбільше у світі кібернавчання, що імітує реальні кіберконфлікти та дає змогу фахівцям відпрацьовувати вміння реагування на складні атаки в умовах реального часу. Навчання залучає експертів з усього світу, включаючи представників державного сектору, приватних компаній та наукових установ. Також CCDCOE проводить щорічну конференцію "CyCon яка збирає провідних спеціалістів у галузі кібербезпеки для обговорення сучасних викликів, обміну досвідом і представлення нових досліджень. Діяльність CCDCOE допомагає зміцненню кібербезпеки та посиленню співпраці між країнами НАТО та їхніми партнерами. Завдяки напрацюванням центру Альянс має можливість вдосконалювати свою стратегію у сфері кібероборони, готуватися до ймовірних загроз та оперативно реагувати на нові виклики в кіберпросторі. Інноваційний підхід, глибокі дослідження та практичні навчання роблять цей центр одним із основних елементів кіберзахисту НАТО, що забезпечує стабільність та безпеку цифрового середовища, як для країн-членів, так і для міжнародної спільноти загалом [17].

4 Висновки

У ході дослідження встановлено, що НАТО активно трансформує підходи до безпеки, інтегруючи наукові дослідження та інновації як ключовий інструмент у протидії сучасним загрозам. Програма «Наука заради миру і безпеки» (SPS) доводить ефективність міждисциплінарної співпраці, об'єднуючи науковців, політиків і безпекові структури задля розробки рішень у сфері кіберзахисту, боротьби з тероризмом, реагування на технологічні та природні катастрофи.

Сучасні концепції та стратегії розвитку НАТО передбачають передусім підтримку науки передових технологій: автономні системи, розробки з кібербезпеки, штучного інтелекту, аналіз великих даних, автомати-

зація ухвалення рішень та ін. Однак огляд центрів і тематик доводить, що науково-дослідна робота під егідою Альянсу охоплює й складний комплекс соціально-поведінкових, комунікаційних, політико-правових, психологічних, культурологічних досліджень. Адже розв'язання конфліктів та відновлення миру у світі потребує не лише високотехнологічних рішень, але й сучасних гуманістичних підходів до міжлюдських взаємин, суспільного договору, міжкультурних зв'язків, глобальної політики тощо.

Важливо, що для досягнення поставлених дослідницьких завдань в широких рамках НАТО, недостатньо самого лише внутрішнього ресурсу, тому співпраця Альянсу з незалежними академічними осередками, НУО та комерційним сектором склала суттєвий виклик і водночас нові можливості для розвитку науково-дослідних перспектив військово-політичного союзу.

Значну роль у реалізації цих цілей відіграють міжнародні наукові центри, зокрема Центр морських досліджень НАТО (CMRE), Центр передового аналізу (NATO STO — Science and Technology Organization), а також співпраця з провідними академічними інституціями країн-членів Альянсу. Водночас виклики, пов'язані зі стрімкими технологічними змінами та зростанням гібридних загроз, вимагають подальшого вдосконалення взаємодії між наукою і політикою безпеки. Стаття засвідчує, що лише через поглиблення науково-дослідницької співпраці та інституційну гнучкість Альянс зможе зберігати стратегічну стійкість у складному геополітичному середовищі.

Перспективи подальших досліджень могли би охопити основні напрямки співпраці Україна-НАТО саме у науково-дослідній частині, варто переосмислити і наявні приклади такого співробітництва, і можливі шляхи його розвитку.

References

[1] About NCIA The NATO Communications and Information Agency (NCIA) is NATO's technology and cyber hub (n. d.). NATO OTAN. https://www.ncia.nato.int/about-us (Accessed: 1.05.2025).

[2] About the NATO science and technology organization (STO) (n. d.). Science and Technology Organization. https://www.sto.nato.int/Pages/default.aspx (Accessed: 1.05.2025).

[3] About the research division (n. d.). NATO DEFENSE COLLEGE. https://www.ndc.nato.int/education/courses.php?icode=0 (Accessed: 1.05.2025).

[4] Bielawski, R. 2022. Development of security technologies by NATO: Current status and development prospects. *Security and Defence Quarterly.* 37(3), 49–62. https://doi.org/10.37105/sd.170

[5] Centre for maritime research and experimentation. (n. d.a). Eurofleets – An alliance of European marine research infrastructure to meet the evolving needs of the research and industrial communities. https://www.eurofleets.eu/partner/centre-for-maritime-research-and-experimentation/ (Accessed: 1.05.2025).

[6] Centre for maritime research and experimentation. (n. d.b). NATO OTAN. https://www.cmre.nato.int/ (Accessed: 1.05.2025).

[7] Charotte D., Colli, F. & Reykers Y. 2024. From policy to practice: How NATO joined forces with NGOs for the protection of civilians. Cooperation and Conflict. https://doi.org/10.1177/00108367241288082

[8] Dowd A. M., Pezard S., Flanagan S. J. & de Lataillade C. 2024. Sustaining the Transatlantic Alliance: 75 years of RAND insights on NATO—Annex with annotated bibliography (RAND Research Report No. RRA3235-2). RAND Corporation. URL: https://www.rand.org/pubs/research_reports/RRA3235-1.html (Accessed: 1.05.2025).

[9] Ertan A., Floyd K., Pernik P. & Stevens T. 2020. Cyber threats and NATO 2030: Horizon scanning and analysis. . NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf (Accessed: 1.05.2025).

[10] Keenan J. M., Trump B. D. & Linkov I. 2024. The role of science in resilience planning for military-civilian domains in the U.S. and NATO. *The RUSI Journal*. Advance online publication. https://doi.org/10.1080/14702436.2024.2365218.

[11] Kunertova D. & Herzog S. 2024. NATO and emerging technologies — the alliance's shifting approach to military innovation. Naval War College Review, 77(22). https://digital-commons.usnwc.edu/nwc-review/vol77/iss2/5/ (Accessed: 1.05.2025).

[12] Lucarelli S., Marrone A. & Moro F. N. (Ed.). 2021. Nato decision-making in the age of big data and artificial intelligence. Università Di Bologna Istituto Affari Internazionali. https://www.iai.it/sites/default/files/9781955445000.pdf (Accessed: 1.05.2025).

[13] NATO 2022 strategic concept. (2023, 3 March). NATO OTAN. http://nato.int/cps/en/natohq/topics_210907.htm (Accessed: 1.05.2025).

[14] NATO centres of excellence — NATO strategic communications centre of excellence. (2023, 24 July). NATO OTAN. https://www.act.nato.int/article/nato-stratcom-coe/ (Accessed: 1.05.2025).

[15] Organization. (n. d.). NATO Defense College. https://www.ndc.nato.int/education/courses.php?icode=0 (Accessed: 1.05.2025).

[16] Patel, P. 2016. NATO's science program funds materials research. MRS Bulletin, 41(3), 183–184. https://doi.org/10.1557/mrs.2016.38

[17] Research. (n. d.). CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. https://ccdcoe.org/research/ (Accessed: 1.05.2025).

[18] Science for peace and security programme. (2023, 17 April). NATO OTAN. https://www.nato.int/cps/en/natohq/topics_85373.htm (Accessed: 1.05.2025).

[19] Soare S. R. 2021. Innovation as adaptation: NATO and emerging technologies. German Marshall Fund of the United States. https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies (Accessed: 1.05.2025).

[20] StratCom | NATO strategic communications centre of excellence Riga, Latvia. (n. d.). StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia. https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5 (Accessed: 1.05.2025).