

ЦИФРОВА ТРАНСФОРМАЦІЯ СФЕРИ БЕЗПЕКИ ТА ОБОРОНИ: СПІВПРАЦЯ ДЕРЖАВИ ТА СУСПІЛЬСТВА

Хома Н. М.,

*доктор політичних наук, професор,
професор кафедри політології та міжнародних відносин
Національного університету «Львівська політехніка»
ORCID ID: 0000-0002-2507-5741
nataliia.m.khoma@lpnu.ua*

У статті розглянуто особливості співпраці держави та суспільства щодо цифрової трансформації сфери безпеки й оборони. Метою дослідження визначено характеристику з позиції політичної науки взаємодії держави та суспільства щодо цифрової трансформації у сфері безпеки та оборони на основі вивчення вітчизняного та закордонного досвіду. Відзначено, що історично питання безпеки та оборони були прерогативою інституту держави, але нині недержавні актори відіграють щобільше активну роль. Наголошено на посиленні партнерського підходу держави, бізнесу та громадянського суспільства у сфері технологічних інновацій для сектора безпеки та оборони. Підкреслено, що цифрова трансформація включає не лише впровадження ІТ-рішень, проривних технологій і т. ін., а й активізацію взаємодії держави з бізнесом (ІТ-компанії, стартапи та ін.), освітянською та науковою спільнотами, неприбутковими організаціями, широкими колами суспільства. Зауважено, що сучасні технологічні рішення для сфери безпеки та оборони щораз активніше розробляються саме недержавними суб'єктами та завдяки їх капіталу. Відзначено, що завдяки цифровій трансформації формується нова модель співпраці держави та суспільства у сфері безпеки та оборони. Сформульована гіпотеза, що така модель співпраці буде розвиватися завдяки інституту публічно-приватного партнерства. Аргументовано, що цифрова трансформація сфери безпеки та оборони прискорюється не лише завдяки технологічному поступу, а й завдяки переосмисленню ролі суспільства у сфері безпеки та оборони, реалізації концепції належного врядування.

Ключові слова: цифровізація, цифрова трансформація, безпека, оборона, цифровізація безпекового та оборонного сектора, публічно-приватне партнерство.

Постановка проблеми. Тривалий час сфера безпеки та оборони уважалася прерогативою держави. Саме держава ухвалювала рішення щодо оборонної політики, безпекових стратегій, мобілізації ресурсів, технологічних інновацій і т. ін. Коло недержавних суб'єктів, долучених до безпекових та оборонних ініціатив, було доволі обмеженим. Лише з розвитком концепції демократичного цивільного контролю над сектором безпеки почало формуватися розуміння, що безпека та оборона є спільною справою держави та суспільства, а не лише державних інституцій. Російсько-українська війна розширила рамки співпраці з огляду на масштаби безпекових та інших викликів, які постали перед державою. Нині недержавні актори відіграють активну та багатовимірну роль у сфері безпеки й оборони України. Одним з найпомітніших напрямків співпраці в умовах високотехнологічних воєн є взаємодія держави та суспільства щодо цифрової трансформації сфери безпеки та оборони. Відтак потребують вивчення особливості цієї взаємодії.

Аналіз останніх досліджень і публікацій. Проблема співпраці держави та суспільства щодо цифрової трансформації у сфері безпеки та оборони наразі лише починає вивчатися. З висхідним інтересом досліджуються два окремі дослідницькі напрямки: 1) цифрова трансформація безпекової та оборонної сфери; 2) співпраця держави та суспільства у сфері безпеки та оборони. На перетині цих дослідницьких напрямків вивчаються взаємодії держави та суспільства у сфері цифрової трансформації сфери безпеки та оборони.

Найперше, відзначимо зростання дослідницького інтересу до багатогранної проблематики цифрової трансформації України, яка вивчається з позиції політичної, юридичної, економічної наук, безпекознавства, а також з позиції технічних та військових наук. Учені-юристи аналізують правове забезпечення цифрової трансформації в Україні, зокрема – у публічній сфері (Горінов & Сілаєв, 2025; Луценко & Пікуля, 2024; Хомишин, 2022; Khomenko et al., 2024). Досліджені цифрові технології в механізмі взаємодії громадянського суспільства та держави (Краснопольська & Милосердна, 2021). Проаналізована роль цифрової трансформації у забезпеченні національної безпеки (Kormych et al., 2024). Досліджені правовий, регуляторний аспекти трансформації взаємодії між урядом та інститутами громадянського суспільства в контексті війни (Khomenko et al., 2024). Учені зробили важливий висновок про зміцнення співпраці між цивільним і військовим секторами в контексті державної безпеки. Аргументовано, що посилення такої взаємодії має потенціал підвищити обороноздатність сучасних армій, й загалом – здатність протистояти викликам війни (Shchokin et al., 2023). Також відзначимо, що наявність численних вітчизняних досліджень у галузях технічних наук та військових наук, низки наукових

видань (як-от: «Сучасні інформаційні технології у сфері безпеки та оборони», «Наука і оборона», «Наукоємні технології» та ін.), однак вони охоплюють тематику технічного, військового спрямування, а не проблематику соціальних наук.

Мета дослідження – схарактеризувати з позиції політичної науки взаємодію держави та суспільства щодо цифрової трансформації у сфері безпеки та оборони на основі вивчення вітчизняного та закордонного досвіду.

Виклад основного матеріалу дослідження. Цифрова трансформація у сфері безпеки та оборони є процесом впровадження цифрових технологій, інноваційних рішень та сучасних методів управління задля підвищення ефективності, гнучкості, адаптивності сил безпеки й оборони. У сучасних умовах гібридних загроз, кібервоєн та високотехнологічних збройних конфліктів, така трансформація стає не просто бажаною, а життєво необхідною. Цифрова трансформація включає не лише впровадження ІТ-рішень, а й зміну підходів до стратегічного управління, оперативного реагування, логістики, обміну інформацією, координації між підрозділами, а також взаємодії з бізнесом та громадянським суспільством. Це комплексна зміна культури, структури та технологічного базису сектора безпеки та оборони. Ключовими елементами цифрової трансформації сфери безпеки та оборони виступають інтеграція штучного інтелекту в системи аналізу розвідувальних даних та бойового управління, кібербезпека, Big Data та аналітика для прогнозування загроз і прийняття рішень, безпілотні літальні апарати, роботизовані системи в зоні бойових дій і т. ін.

Однак цифровізація у сфері безпеки та оборони – це не лише про нові технології, а й про трансформацію всієї системи національної безпеки та оборони, зміну моделі її функціонування. Цифрова трансформація задля зміцнення стійкості сфери безпеки та оборони за такого масштабу викликів, які наявні нині, потребує взаємодії держави з бізнесом (передусім – ІТ-спільнотою), освітянсько-науковою спільнотою, неприбутковими організаціями, широкими колами суспільства задля запобігання та протидії численним гібридним загрозам (кібератакам, дезінформації, ІТ-диверсії та ін.). Сучасні технологічні рішення для сфери безпеки та оборони щобільше розробляються недержавними акторами й практично впроваджуються мотивованими державними інститутами.

Відтак широкий спектр питань безпеки та оборони більше не є виключно у фокусі уваги держави. Бізнес, громадянське суспільство, волонтери, відіграють важливу роль у посиленні безпеки, обороні країни завдяки оборонним та безпековим інноваціям. Наявна активізація взаємодій держави та суспільства з питань цифрової трансформації сфери безпеки та оборони. В Україні ці процеси доволі чітко увиразнені. За надзвичайних безпекових викликів прискорено формується та функціонує (з досягненнями та проблемами) система партнерів процесу цифрової трансформації сфери безпеки та оборони. Вона включає:

1) державу (парламент, відповідні урядові інституції, найперше – Міністерство оборони України, Міністерство цифрової трансформації України) – формує політику, нормативну базу, інвестує в цифрову інфраструктуру безпеки та оборони, практично впроваджує технологічні рішення;

2) приватний сектор (ІТ-компанії, стартапи) – розробляє інноваційні рішення щодо кіберзахисту, системи зв'язку, аналітичні інструменти і т. ін.;

3) громадянське суспільство – розробка технологічних рішень, моніторинг закупівель ІТ-рішень та інших технологій, контроль, проведення тренінгів з кібергігієни, публічний тиск на владу щодо цифрової модернізації сектору оборони і т. ін.;

4) заклади освіти та науково-дослідні інститути – підготовка відповідних фахівців; проведення досліджень щодо відповідального штучного інтелекту, кібербезпеки та захисту цифрової інфраструктури, розробки роботизованих систем і т. ін.;

5) зацікавлені громадяни – протидія дезінформації, тестування нових цифрових рішень, долучення через волонтерські спільноти (InformNapalm та ін.) до проведення OSINT-аналізу (розвідка на основі відкритих джерел) і т. ін.

Відтак наявний широкий спектр напрямків взаємодій держави та суспільства щодо цифровізації у сфері безпеки та оборони, серед яких: 1) розвиток ІТ-рішень стартапами, технологічними компаніями; 2) громадський контроль і прозорість, як-от створення цифрових платформ для моніторингу державних закупівель у сфері оборони; 3) волонтерські ініціативи у напрямку кібероборони на зразок хактивістів, які підтримують національну кібербезпеку, об'єднуються в «кібервійська»; 4) інформаційна безпека та протидія дезінформації, моніторинг інформаційного простору з метою виявлення фейків і протидії пропаганді. Зростає роль громадськості у виявленні фейків, протидії пропаганді, підтримці інформаційного фронту.

Одним із перших проєктів цифровізації, ініційованим на волонтерському рівні, була система ситуаційної обізнаності та координації військ «Delta». Цей проєкт був розпочатий ще у 2015 році волонтерами команди «Аеророзвідка». Ця громадська організація сприяла створенню та впровадженню мережецентричних і роботизованих військових спроможностей для Сил безпеки й оборони України. У межах «Аеророзвідки» українське громадянське суспільство стало учасником боротьби проти російської агресії. Згодом волонтери «Аеророзвідки» підписали контракт із ЗСУ (Центр впровадження та супроводження автоматизованих систем оперативного (бойового) управління, Центр інновацій та розвитку оборонних технологій Міністерства оборони України). Була реалізована велика кількість

оборонних проєктів, які ґрунтуються на цифрових технологіях. Цей кейс увиразнює, як нині великий державний проєкт виріс з громадської ініціативи.

У 2023 році в Україні з ініціативи уряду було запущено кластер з розвитку оборонних технологій BREVE1. Проєкт позиційований як єдине вікно співпраці держави з компаніями з оборонних технологій, військовими, інвесторами, волонтерськими фондами, медіа, зацікавленими закладами освіти (як державних, так і приватних) та інших зацікавлених у розробці й застосуванні передових технологій для сфери оборони та безпеки держави. Створені можливості для отримання грантів на реалізацію важливого для безпеки чи оборони технологічного проєкту.

Завдяки бізнесу та громадським ініціативам під час війни створюються унікальні стартапи, результатів яких нині потребує найперше Україна, а надалі можливий вихід на експорт у країни, які зацікавлені в таких технологічних рішеннях. До прикладу, продуктом українського стартапу Swarmer, що входить до кластера оборонних інновацій Brave1, є програма Clarity. Вона автоматизує аналіз аерофотознімків і за хвилини виявляє підозрілі ворожі об'єкти; раніше це вимагало багатогодинної ручної обробки. Програма Clarity шукає військову та цивільну техніку, замасковані об'єкти, а також сліди, які можуть вказувати та перебування поряд ворожої позиції.

Уважаємо, що співпраця держави та суспільства щодо цифрової трансформації сфери безпеки та оборони посилює стійкість обох сторін до викликів російсько-української війни. Держава отримує партнера, сильно мотивованого у результативні тих чи інших безпеково і оборонних проєктів. Суспільство, своєю чергою, відчуває свою значущість, створюючи своїми ініціативами можливості долучитися до стратегічно важливих безпеково-оборонних питань. Досвід періоду російсько-української війни показує, що об'єднання державою та суспільством ресурсів, знань, технології дає змогу: швидше розробляти та впроваджувати інноваційні рішення; адаптуватися до змін на фронті та в інформаційному просторі; вчасно реагувати на нові загрози (кібератаки, дезінформація тощо).

Відтак, російсько-українська війна активізувала бізнес і громадськість у частині розробки й подальшого практичного впровадження сучасних рішень для ведення «розумної війни» (Öz & Ünal, 2024). Активізувалися сотні українських компаній в галузі defense tech, які розробляють сучасні рішення. У них зацікавлена держава, армія та ін. з огляду на швидкість продукування рішень з ефективним застосуванням цифрових технологій. Ці рішення посилюють оборонну здатність країни, зберігають життя захисників та цивільних і ефективно використовують ресурси завдяки технологічним інноваціям. Співпраця державного та недержавного секторів в Україні стала критично важливою для оборони та безпеки держави. Така співпраця поєднує ресурси та легітимність держави з гнучкістю, ініціативністю та мобільністю неурядових структур.

Досвід України щодо співпраці державного та недержавного секторів у сфері цифрової трансформації безпеки та оборони є новаторським, однак маємо звернути увагу на наявність схожого й у інших держав. Наведемо два приклади:

1) Ізраїль одним з перших стратегічно визнав кіберпростір як новий вимір конфлікту. Створено унікальну синергетичну модель співпраці між державою, військовими, приватним сектором та академічними колами (Olech, 2025). Колишні члени підрозділу 8200 Управління військової розвідки («Аман») заснували такі компанії, як Check Point, CyberArk, Clarity, CyCognito та Palo Alto Networks. Вони підтримують національну безпеку та слугують інструментами кіберм'якої сили Ізраїлю за кордоном;

2) американський Підрозділ оборонних інновацій (Defense Innovation Unit, U.S. War Department) має завданням прискорювати впровадження передових комерційних технологій для американської армії, розширювати базу інноваційних рішень у сфері національної безпеки завдяки укладенню контрактів з компаніями (з США та держав-союзників). Контракти стосуються рішень, які є відповіддю на нові виклики національній безпеці, що пропонують рішення для викликів національній безпеці в різних технологічних галузях (кібербезпека, геоінформаційні технології, аналітика Великих даних, технології ведення електронної війни та ін.). Наприклад, американський оборонний та аерокосмічний tech-стартап Shield AI, який уже відомий й в Україні, працює для захисту військовослужбовців та цивільного населення за допомогою інтелектуальних систем. Завданням Shield AI є створити найкращого у світі пілота зі штучним інтелектом.

Постає питання: як можуть співпрацювати держави та суспільство щодо реформування сектора безпеки та оборони України завдяки цифровій трансформації на повоєнному етапі? Уважаємо, що на етапі повоєнного відновлення Україна постане перед викликом не лише відбудови країни, а й конструювання сучасної, ефективної та стійкої системи, здатної запобігати новим загрозам. У цьому процесі цифрова трансформація стане важливим інструментом, а співпраця держави і суспільства щодо нових цифрових рішень – критично необхідною умовою. Цифрова трансформація формує нову модель співпраці держави та суспільства, де громадяни – не лише об'єкти захисту, а активні суб'єкти творення більш безпечного майбутнього. Важливу роль у цьому процесі може відіграти інститут публічно-приватного партнерства.

Власне Закон України «Про публічно-приватне партнерство» (чинний з 30.10.2025 р.) унормував механізм, який уможливить залучення державою ресурсів приватного сектора для створення та реалізації інфраструктурних проєктів, надання суспільно значущих послуг. Ст. 4 вказаного нормативно-

правового акту визначає, що механізм публічно-приватного партнерства може застосовуватися в секторах безпеки та оборони, електронних комунікацій, цифрової інфраструктури, інформаційних технологій та кібербезпеки (Про публічно-приватне партнерство, 2025). Публічно-приватне партнерство може набути стратегічної важливості щодо цифрової трансформації сфери оборони та безпеки. Підставою для такого припущення є те, що ще від 2014 року в Україні спостерігається зростання ролі недержавних суб'єктів у безпекових, оборонних проєктах. Передусім, це різні IT-рішення для фронту (аналітика, геоінформаційні системи, програмне забезпечення для управління вогнем і т. ін.). Низка неприбуткових організацій стали партнерами держави. Фактично ще до закріплення у 2025 році інституту публічно-приватного партнерства в Україні формувалася його модель, адаптована під потреби війни. Відбулося розширення традиційних меж взаємодії між державою і суспільством зокрема – завдяки сферам безпеки та оборони. За новим Законом України «Про публічно-приватне партнерство» такими партнерами для держави можуть виступати недержавні суб'єкти зі статусом юридичної особи, зокрема й ті громадські об'єднання, що зареєстровані зі статусом юридичної особи.

Висновки та перспективи подальших досліджень. Цифрова трансформація сфери безпеки та оборони є результатом як технологічного поступу у сфері безпеки та оборони, так й переосмислення ролі суспільства у посиленні стійкості держави. Цифровізація та пов'язані з нею процеси змінюють і переосмислюють традиційні уявлення про належне врядування, залучаючи нових учасників до сфери безпеки та оборони. За нашою оцінкою, результат як цифрової трансформації, так і багатьох інших процесів у сфері безпеки та оборони, узалежнений не лише від технологічного прогресу, а й від якості співпраці держави та суспільства, рівня довіри, відкритості, мотивованості спільно реагувати на безпекові та оборонні виклики. Велика перспектива в цьому напрямку вбачається нами у функціонуванні інституту публічно-приватного партнерства.

Khoma N. Digital Transformation of Security and Defence: Cooperation Between the State and Society. This article examines the specific features of the cooperation between the state and society in the digital transformation of the security and defence sector. From a political science perspective, the study aims to characterise the interaction between the state and society in this digital transformation, based on an analysis of domestic and foreign experience. Historically, security and defence issues have been the responsibility of the state, but non-state actors are now playing an increasingly active role. The article emphasises the importance of strengthening the partnership approach between the state, businesses, and civil society in the field of technological innovation for the security and defence sector. The article stresses that digital transformation encompasses not only the adoption of IT solutions and cutting-edge technologies, but also the intensification of interaction between the state, businesses (IT companies and start-ups), educational and scientific communities, non-profit organisations, and broader societal groups. It was noted that modern technological solutions for the security and defence sector are increasingly being developed by non-state actors thanks to their capital. Digital transformation is shaping a new model of cooperation between the state and society in the field of security and defence. It is hypothesised that such a model of cooperation will develop through the establishment of public–private partnership partnerships. It is argued that the digital transformation of the security and defence sector is accelerating due to technological progress and a rethinking of society's role in security and defence, as well as the implementation of good governance concepts.

Keywords: digitalisation, digital transformation, security, defence, the digitalisation of the security and defence sector, public–private partnership partnerships.

Література:

1. Горінов, П., & Сілаєв, В. (2025). Політика цифрової трансформації України в умовах євроінтеграції. Наукові праці Міжрегіональної академії управління персоналом. Серія: Політичні науки та публічне управління, 1 (77), 50–57. DOI: 10.32689/2523-4625-2025-1(77)-8
2. Краснопольська, Т., & Милосердна, І. (2021). Цифрові технології в механізмі взаємодії громадянського суспільства та держави. Актуальні проблеми політики, 67, 68–74. DOI: <https://doi.org/10.32837/app.v0i67.1152>
3. Луценко, В., & Пікуля, Т. (2024). Правове забезпечення цифрової трансформації в Україні. Науковий вісник Ужгородського національного університету. Серія: Право, 81 (1), 61–67. DOI: 10.24144/2307-3322.2024.81.1.9
4. Про публічно-приватне партнерство: Закон України (2025). Голос України, 31 липня, № 149.
5. Хомишин, І. (2022). Напрями цифрової трансформації у публічній сфері: правові основи. Вісник Національного університету «Львівська політехніка». Серія «Юридичні науки», 3 (35), 233–239. DOI: 10.23939/law2022.35.233
6. Bouhafs, H. (2025). Cybersecurity in the Digital Era: Between Digital Transformation and Protection Challenges. Law and World, 11 (35), 111–125. DOI: 10.36475/11.3.8

7. Khomenko, O., Shyian, O., Kravchuk, P., Movchan, O., & Morgun, S. (2024). Transformation of Interaction Between the Government and Civil Society Institutions in the Context of War: Legal and Regulatory Aspect. *Social & Legal Studies*, 7 (2), 86–95. DOI: 10.32518/sals2.2024.86
8. Kormych, L., Krasnopol'ska, T., & Zavhorodnia, Yu. (2024). Digital Transformation and National Security Ensuring. *Evropsky Politicky a Pravni Diskurz*, 11 (1), 29–37. DOI: 10.46340/eppd.2024.11.1.4
9. Olech, A. (2025). Cyber Forces: Israel. *Defence24*. https://defence24.com/geopolitics/cyber-forces-israel?utm_source
10. Öz O., & Ünal, A. (2024). The Concept of Smartwar: A Theoretical Framework. *Nosyon: International Journal of Society and Culture Studies*, 13, 35–57.
11. Shchokin, R., Soloviov, O., & Tantsiura, I. (2023). Strengthening Cooperation between the Civilian and Military Sectors In the Context of State Security: Benefits and Challenges. *Revista de cercetare și intervenție socială*, 83, 155–170. DOI: 10.33788/rcis.83.11

Стаття надійшла до редакції 14.10.2025

Стаття рекомендована до друку 24.10.2025