Received 04.03.2026 | Accepted 16.03.2026 | Published 30.03.2026

УДК 355.45:623 DOI: 10.63978/3083-6476.2026.1.4.01

Залужний Валерій Федорович
доктор філософії
Надзвичайний та Повноважний Посол України в Сполученому Королівстві Великої Британії і Північної Ірландії
ORCID: 0000-0002-1947-501X

ОБОРОННІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ ТА ТРАНСФОРМАЦІЇ МІЖНАРОДНОГО БЕЗПЕКОВОГО СЕРЕДОВИЩА

Анотація. *У статті розглянуто розвиток оборонних технологій в Україні на тлі повномасштабної війни з росією з 2022 року та їхній вплив на міжнародне безпекове середовище. Особливу увагу приділено трансформації українського оборонно-промислового комплексу: технологічним інноваціям (масове виробництво дронів, системи радіоелектронної боротьби, елементи штучного інтелекту, кіберзахист), інституційним змінам (від децентралізованої моделі до спроб централізації, державно-приватне партнерство, створення Міжвідомчої комісії при РНБО) та геополітичним наслідкам.*

На основі даних SIPRI (військові витрати України 64,7 млрд дол. США у 2024 р.), CFR, Atlantic Council та інших джерел проаналізовано зростання виробництва БПЛА (2,5–4 млн одиниць у 2025 р., план 7 млн у 2026 р.), інвестиції в defence-tech (понад 105 млн дол. у 2025 р.), перші експортні ліцензії та потенціал експорту на кілька мільярдів доларів щорічно за умови гармонізації з європейськими стандартами. Окремо висвітлено ризики: залежність від імпорту комплектуючих, дефіцит кваліфікованих фахівців, кіберзагрози (понад 2000 інцидентів у 2023 р. за даними CERT-UA та ENISA), бюрократичні бар'єри в НАТО та ЄС.

Запропоновано модель "Інтеграційна піраміда" з трьома рівнями: технологічна автономність (локалізація виробництва), регуляторна гармонізація (відповідність стандартам ЄС/НАТО), міжнародний вплив (експорт, спільні програми, внесок у колективну безпеку). Модель синтезує емпіричні дані та теоретичні концепції (RMA, "нові війни" Kaldor, роботи Horowitz та Scharre), але визнає власні обмеження: ефективна в асиметричних конфліктах середньої інтенсивності, менш універсальна в глобальних сценаріях.

Висновки підкреслюють роль України як реального випробувального полігону для Європи, де дешеві combat-proven рішення (наприклад, FPV-дрони) контрастують з провалами дорогих венчурних проєктів (Stark Defence). Рекомендації стосуються гармонізації стандартів, спільного виробництва (ППО, дрони, боєприпаси збільшеної дальності), збереження фронтового зворотного зв'язку, децентралізації критичної інфраструктури та регулярного SWOT-моніторингу ОПК.

Ключові слова: *оборонні технології, ОПК України, гібридна війна, дрони, радіоелектронна боротьба, кібербезпека, європейська безпека, НАТО, DIANA, інновації, експорт озброєнь.*

Valerii Zaluzhnyi
Doctor of Philosophy in Law
Extraordinary and Plenipotentiary Ambassador of Ukraine to the United Kingdom of Great Britain and Northern Ireland
ORCID: 0000-0002-1947-501X

DEFENSE TECHNOLOGIES AS A TOOL OF STATE MANAGEMENT OF NATIONAL SECURITY AND TRANSFORMATION OF THE INTERNATIONAL SECURITY ENVIRONMENT

Abstract. *The article examines the development of defense technologies in Ukraine amid the full-scale war with Russia since 2022 and their impact on the international security environment. Particular attention is given to the transformation of Ukraine's defense-industrial complex: technological innovations (mass drone production, electronic warfare systems, AI elements, cybersecurity), institutional changes (from decentralized model to attempts at centralization, public-private partnerships, establishment of the Interagency Commission under the National Security and Defense Council), and geopolitical implications.*

Drawing on data from SIPRI (Ukraine's military expenditure $64.7 billion in 2024), CFR, Atlantic Council and other sources, the study analyzes the growth of UAV production (2.5–4 million units in 2025, target 7 million in 2026), investments in defense-tech (over $105 million in 2025), first export licenses issued and export potential of several billion dollars annually subject to harmonization with EU standards. Specific risks are highlighted: dependence on imported components, shortage of qualified personnel, cyber threats (over 2000 incidents in 2023 according to CERT-UA and ENISA), bureaucratic barriers within NATO and the EU.

An "Integration Pyramid" model is proposed with three levels: technological autonomy (localization of production), regulatory harmonization (compliance with EU/NATO standards), international influence (export, joint programs, contribution to collective security). The model synthesizes empirical data and theoretical concepts (RMA, Kaldor's "new wars", works by Horowitz and Scharre), yet acknowledges its limitations: effective in asymmetric conflicts of medium intensity, less universal in global scenarios.

Conclusions emphasize Ukraine's role as a real testing ground for Europe, where low-cost combat-proven solutions (e.g., FPV drones) contrast with failures of expensive venture projects (Stark Defence). Recommendations focus on standards harmonization, joint production (air defense, drones, long-range munitions), preservation of frontline feedback loops, decentralization of critical infrastructure, and regular SWOT monitoring of the DIC.

Keywords: *defense technologies, Ukraine's DIC, hybrid warfare, drones, electronic warfare, cybersecurity, European security, NATO, DIANA, innovations, arms export.*

JEL Classification: O32, H56, L64, F52

Вступ

Повномасштабна збройна агресія російської федерації проти України, що розпочалася у лютому 2022 року, не лише спричинила глибоку гуманітарну кризу та фундаментальні геополітичні зрушення, але й стала потужним каталізатором для трансформації глобальних оборонних систем, військової організації та технологічних підходів до ведення сучасної війни. Цей воєнний конфлікт, що триває вже понад чотири роки, продемонстрував, як високотехнологічні інновації, інтегровані в реальні бойові умови, можуть радикально змінити динаміку протистоянь, переорієнтувавши акцент з традиційних обсягів матеріальних ресурсів на швидкість адаптації та ефективність цифрових рішень. Зокрема, війна виявила, що сучасні конфлікти все більше залежать від гібридних елементів, де кіберзагрози, автономні системи та інформаційні мережі відіграють ключову роль, доповнюючи кінетичні операції [1].

Актуальність теми посилюється останніми подіями в Ірані, де ескалація конфлікту з США та Ізраїлем, включаючи удари по лідерству (вбивство Верховного лідера Аятолли Алі Хаменеї) та військових об'єктах, призвела до асиметричної відповіді Ірану з використанням гіперзвукових ракет Fattah-2, кібератак на інфраструктуру та ударів по країнах Перської затоки. Це спричинило зростання цін на нафту через атаки на танкери в Ормузькій протоці та інтернет-блекаут в Ірані. Це переконливо ілюструє, як оборонні технології (гіперзвук, кібер, дрони) можуть швидко ескалувати регіональні кризи, загрожуючи глобальній енергетичній безпеці та європейській стабільності через потенційні потоки біженців і ланцюгові реакції [23-25].

За даними Stockholm International Peace Research Institute (SIPRI), військові витрати України до 2024 року зросли і сягнули 64,7 млрд доларів США: це вже не просто зростання,

а один із найвищих показників військового навантаження на економіку (близько 34 % ВВП). Цей стрибок не лише підкреслив економічну напругу, але й стимулював перехід до гібридного характеру конфлікту, де технологічна якість – автономні дрони, системи радіоелектронної боротьби – дедалі більше доповнює традиційні фактори, включаючи логістику та артилерійську підтримку.

Наприклад, за оцінками Atlantic Council, значна частина втрат у початкових фазах війни були пов'язані з логістичними проблемами, але стабілізація постачань у 2024-2025 роках дозволила зосередитися на технологічних перевагах, таких як FPV-дрони з оптоволоконним керуванням, що підвищили ефективність на 30-40 % у зонах інтенсивних бойових дій [9; 10]. Водночас варто зауважити, що ці оцінки ефективності часто базуються на польових звітах і можуть бути суб'єктивними. Точна статистика втрат від дронів досі частково класифікована.

У міжнародному контексті трансформація українського оборонно-промислового комплексу (ОПК) розглядається як стратегічний фактор посилення безпекової архітектури Європи. Згідно з аналізом Council on Foreign Relations (CFR), саме українська оборонно-промислова база може стати одним із ключових елементів відновлення європейської обороноздатності, особливо з огляду на дефіцит виробничих потужностей у країнах ЄС [2].

Потенціал експорту українських оборонних технологій оцінюється орієнтовно в діапазоні кількох мільярдів доларів США щорічно за умови відповідності стандартам ЄС, це базується на прогнозі зростання ОПК та інтеграції з європейськими ланцюгами постачань (Reuters, лютий 2026). Інвестиції в deftech зросли стократно з 2023 року до понад 105 млн доларів у 2025 році [2]. Але чи стійке це зростання – питання відкрите: значна частина інвестицій залежить від зовнішніх партнерів, і в разі зміни політичної кон'юнктури (наприклад, зменшення допомоги) темпи можуть сповільнитися.

Проблематика дослідження полягає у необхідності розібратися у взаємозв'язку між технологічними інноваціями, інституційною перебудовою оборонної галузі та змінами в міжнародному безпековому середовищі. Російсько-українська війна виявила потребу в переосмисленні європейської безпеки, де традиційні моделі НАТО доповнюються новими ініціативами, такими як DIANA (Defence Innovation Accelerator for the North Atlantic) з бюджетом 1 млрд євро, спрямованими на прискорення інновацій [15]. Переговори про участь України в DIANA ведуться з грудня 2025 року – це може стати першим випадком залучення не-члена Альянсу як повноцінного партнера, але поки що статус не фіналізований.

Гіпотеза дослідження сформульована як модель з трьома незалежними змінними та одним залежним результатом: якщо рівень технологічної автономності (виражений як частка локалізованого виробництва в загальному обсязі ОПК, наприклад, 50 % за SIPRI) перевищує критичний поріг і поєднується з регуляторною інтеграцією (відповідність стандартам ЄС та НАТО, вимірювана кількістю спільних програм), тоді формується системний міжнародний вплив України на європейську безпеку.

Механізм впливу реалізується через три взаємопов'язані канали [2; 9]:

1) скорочення залежності від імпорту та прискорення циклу інновацій (від розробки до бойового застосування за тижні, як у випадку з дронами);

2) посилення експортної присутності та дипломатії;

3) внесок у колективну безпеку через спільні програми (наприклад, з Францією в рамках "Brave France" для тестування технологій).

Ця гіпотеза враховує емпіричні дані, такі як зростання виробництва дронів в Україні з 2,5-4 млн у 2025 році до планових 7 млн у 2026 році, що робить країну потенційною "дроновою столицею" світу. Однак без повної інституційної інтеграції, включаючи гармонізацію з європейськими регуляціями, вплив на глобальну безпеку залишається обмеженим, з ризиками фрагментації та залежності від зовнішньої допомоги. Події в Ірані, з їхньою асиметричною відповіддю (гіперзвукові удари, кіберінциденти), підкреслюють, як

подібні технології можуть швидко дестабілізувати регіони, впливаючи на європейську безпеку через енергетичні шоки та ескалацію.

Огляд літератури

Теоретична база осмислення технологічних змін у війні сформована задовго до подій 2022 року, зокрема концепцією "революції у військовій справі" (Revolution in Military Affairs, RMA), розробленою Andrew F. Krepinevich, яка акцентує роль інформаційних технологій у трансформації способів ведення війни [3]. Автор стверджує, що ця концепція, хоча й переконлива для великих держав з розвиненою промисловістю, недооцінює асиметричні адаптації в конфліктах на кшталт українсько-російського, де приватні ініціативи та швидкі ітерації технологій, такі як дешеві дрони та крилаті ракети, стають домінуючими.

Подальший розвиток ідеї RMA відображено у працях Williamson Murray та MacGregor Knox, де підкреслюється системний характер військових інновацій, що поєднує технології з організаційними змінами [4]. Сумнівно, чи така модель повною мірою застосовна до України, де цикл адаптації дронів та контрзаходів скоротився до 2-3 місяців у 2025 році – це перевищує темпи традиційних армій [3; 4; 10].

Lawrence Freedman у своїй фундаментальній праці "The Future of War" зазначає, що технологічні зміни не замінюють політичної природи війни, але суттєво змінюють її інструментарій, роблячи акцент на інформаційному домені [5]. Це твердження переконливо демонструє реальність українського фронту, де дрони не лише як засоби ураження, але й як елементи інформаційної інфраструктури, формують багаторівневу систему спостереження. Подібну позицію розвиває Mary Kaldor у концепції "нових воєн", акцентуючи на взаємодії державних і недержавних акторів у цифровізованому середовищі, що особливо актуально для України з її волонтерськими групами на кшталт Wild Hornets, які розробили контр-дрони STING для перехоплення російських Shahed [6]. Але чи буде така децентралізована модель стійкою в довгостроковій перспективі без інституційної підтримки та залежності від зовнішньої допомоги?

У контексті штучного інтелекту (ШІ) та автономних систем ключовими є роботи Paul Scharre та Michael C. Horowitz, які аналізують стратегічні наслідки впровадження алгоритмічних рішень у військову сферу [7; 8]. Horowitz доводить, що швидкість технологічного освоєння є ключовим фактором зміни балансу сил, але в українському випадку це працює з обмеженнями: за даними SIPRI, військові витрати України у 2024 році сягнули 64,7 млрд доларів, що дозволило масштабувати виробництво дронів, але з ризиками залежності від імпорту компонентів [9]. Це підкреслює необхідність локалізації, оскільки російські контрзаходи, такі як Supercam дрони з системами ухилення від перехоплювачів, вже перевершують українські в деяких аспектах. Аналітики Chatham House наголошують, що досвід України може слугувати джерелом інституційних уроків для НАТО, зокрема в ініціативах DIANA [10].

Вітчизняні дослідники Гурковський В., Романенко Є., Коваль В., Ільницький С. в своїй праці "Форсайт-дослідження як інструмент зміцнення резильєнтності до загроз БПЛА з оптоволоконникм управлінням" розглядають західні та українські розробки засобів протидії оптоволоконним БПЛА, зокрема лазерні сисеми, радари та ШІ-базовані детектори [20]. Зазначені автори пропонують стратегічний підхід до відбору пріоритетних технологічних напрямів у сфері оборони, орієнтований на довгострокові сценарії військово-технічного розвитку.

Водночас література містить застереження щодо ризиків надмірної венчуризації оборонного сектору. Приклад компанії Stark Defence, проаналізований у DroneXL (2025), демонструє, що не всі інноваційні проєкти ШІ витримують перевірку реальними умовами [12]. Коли ударні безпілотники на базі ШІ не влучили у ціль під час чотирьох окремих спроб, це викрило неприємну правду: мільярди венчурного капіталу та спритний маркетинг

не змінюють жорсткого зворотного зв'язку реального бою. Українські FPV дрони вартістю 400 доларів щодня знищують російську бронетехніку зі швидкістю розгортання тисяч одиниць на день – це контраст, який важко ігнорувати.

Для України, де відбувається масштабне тестування нових видів озброєння в умовах реального бойового застосування, європейська безпека дедалі більше залежить від такого "лабораторного осередку" перевірки технологій у реальних умовах.

Для посилення аналізу загроз безпеки розглянемо роботу про кіберзагрози в російсько-українській війні 2022-2023, яка підкреслює зростання загроз з кіберпростору, з понад 2000 інцидентами в Україні за ENISA, що еволюціонували від DDoS до цільових атак на енергетику [21]. Це підтверджується створенням Cyber Force та Space Force в Україні до кінця 2025 року, як оголошено парламентом, що сигналізує про стратегічний зсув до незалежних кібер- та космічних команд. Але чи буде це достатньо без ресурсів рівня США, нажаль, сумнівно, оскільки росія нарощує дронові операції через Rubicon Center, виробляючи до тисяч Shahed на місяць.

Окрім того, останні дані про використання "Шахедів" свідчать, що вони перетворилися з простих камікадзе-дронів у мережеві, багатофункціональні платформи зі впровадженням елементів ШІ та роєвої логіки. Все частіше вони використовуються як носії FPV-дронів – вони наближаються до лінії фронту або території України, а потім скидають дрібні FPV, які далі ведуть точкові атаки з короткої дистанції.

Незважаючи на значну кількість аналітичних матеріалів, комплексного дослідження, що інтегрує стратегічну теорію, інституційний аналіз та практику українського ОПК, наразі бракує. Акцент Horowitz на дифузії влади корисний, але не враховує локальні фактори, такі як дефіцит embedded-розробників, що обмежує масштабування. Додаткові EU звіти, як McKinsey's European defense by the numbers, прогнозують витрати ЄС до 800 млрд євро до 2030 року, додаючи економічний вимір [30]. Сумнівно, чи Європа зможе досягти оборонної автономії без української швидкості інновацій.

Мета та завдання статті

Метою дослідження є виявлення та оцінка механізмів, через які розвиток оборонних технологій в Україні в умовах російсько-української війни трансформує національний оборонно-промисловий комплекс і впливає на європейську безпекову архітектуру, зокрема в процесі інтеграції з НАТО та ЄС, з формулюванням моделі такого впливу.

Методи

Методологічна основа базується на поєднанні системного аналізу, інституційного підходу та порівняльної методології. Такий гібридний метод видається найбільш адекватним для вивчення українського ОПК в умовах триваючого конфлікту високої інтенсивності, оскільки дозволяє розглядати технологічні інновації не ізольовано, а як частину взаємопов'язаної екосистеми, де технічні рішення, організаційні структури та міжнародні кооперацийні механізми формують єдину модель.

Системний аналіз застосовується для оцінки оборонних технологій як динамічної системи з елементами зворотного зв'язку: бойовий досвід безпосередньо впливає на ітерації розробки, що скорочує цикл від концепції до застосування до кількох тижнів або місяців – на відміну від традиційних 5-10 років у великих державах НАТО. Це поки переконливо демонструє перевагу асиметричної адаптації в Україні.

Інституційний підхід фокусується на трансформації управлінських структур, підвищенні ролі професійних асоціацій, державно-приватного партнерства та нових органів, таких як Міжвідомча комісія з питань військово-промислової політики та оборонних технологій при РНБО (утвореної рішенням РНБО від 22 листопада 2025 року, введеним в дію 12 лютого 2026 року указом Президента України №116/2026) [18]. Цей

підхід дозволяє оцінити, як інституційна централізація балансує між децентралізованою венчурною моделлю (понад 450 компаній лише в дроновому секторі) та державним контролем. Саме інституційна перебудова є визначальним чинником для переходу від "виживання в умовах довготриваючої війни" до "системного зростання", але ризики бюрократії проявилися в затримках з експортними ліцензіями, зокрема в сегменті озброєння та БПЛА на початку 2026 року.

Порівняльна методологія дає змогу зіставити український досвід з практиками держав НАТО, зокрема в рамках DIANA. У 2026 році програма розширилася до найбільшої когорти – 150 інноваторів з 24 країн НАТО, з фокусом на дуальні технології (UAV, AI, кіберзахист) [15]. Україна, як потенційний перший не-член НАТО партнер у DIANA (переговори ведуться з грудня 2025 року), отримує доступ до інфраструктури та фінансування, що створює унікальну можливість для інтеграції.

Порівняння з традиційними моделями НАТО (де цикл інновацій часто перевищує 5 років) підкреслює українську перевагу в швидкості, але бюрократичні бар'єри Альянсу можуть не дозволити повноцінно інтегрувати українські рішення без значних компромісів щодо стандартів [29].

Джерельна база обмежується переважно верифікованими інституційними та академічними матеріалами: звіти SIPRI (Trends in World Military Expenditure 2024, де витрати України сягнули 64,7 млрд дол. США у 2024 році з подальшим зростанням), ENISA Threat Landscape, EDA Defence Data, NATO офіційні документи, CFR та Atlantic Council аналізи, а також peer-reviewed публікації з ResearchGate (2023–2026) щодо кіберзагроз та національної стійкості [15; 28; 9]. Публіцистичні та експертні оцінки (наприклад, з DOU чи IT Arena) використовуються як ілюстративні, а не як основа кількісних висновків, щоб уникнути ризику переоцінки прогнозів [16; 19].

Обмеження методології полягають у доступності даних: повна статистика виробництва та втрат залишається класифікованою, а війна вносить динаміку, що ускладнює довгострокові прогнози. Це змушує покладатися на непрямі індикатори (зростання інвестицій у deftech до понад 105 млн дол. у 2025 році, експортні центри в Європі з 2026 року), але підкреслює необхідність постійної емпіричної верифікації. Порівняльний вимір з іншими конфліктами (наприклад, ізраїльські інновації в Iron Dome чи турецькі Bayraktar) свідчить, що український кейс унікальний за масштабом децентралізації та швидкістю, але ризикує втратити темп без стабільного фінансування та інтеграції з ЄС/НАТО.

Результати

Технологічна трансформація: системний вимір

Технологічні зміни в українському оборонному секторі після 2022 року не обмежуються ізольованими інноваціями, а формують мережеву інтеграцію безпілотних платформ, сенсорних систем, алгоритмів обробки даних, засобів радіоелектронної боротьби та цифрових комунікацій. Згідно з Keir Giles у публікації Chatham House "NATO can learn from Ukraine's military innovation" (2023), ключовою особливістю українського підходу є швидка інтеграція комерційних технологій в оперативну практику, що скорочує цикл від розробки до бойового застосування до тижнів [11].

Це ілюструє перевагу асиметричної війни, де Україна виробляє від 2,5 до 4 млн дронів у 2025 році з планами на 7 млн у 2026, роблячи країну "дрономовою столицею" світу [10]. Однак чи така швидкість буде стійкою без стабільного фінансування з урахуванням ризиків залежності від імпорту компонентів [11].

У цьому контексті БПЛА виконують не лише функцію засобів ураження, а й елементів інформаційної інфраструктури, поєднуючись із супутниковим зв'язком, цифровими картографічними сервісами та алгоритмічними системами аналізу. Подібна

конфігурація змінює традиційні уявлення про глибину оборони та наступу, інтегруючи розвідку і вогневе ураження у спільний цифровий контур, як описано в Council on Foreign Relations “Securing Ukraine’s Future in Europe” [2].

Звіт CFR є цінним через стратегічний аналіз, але оцінка потенціалу експорту (кілька млрд доларів) потребує уточнення через регуляторні бар’єри ЄС, оскільки зростання виробництва дронів з fiber-optic FPV технологіями вимагає сертифікації для спільних проєктів з Францією чи Німеччиною [10]. Водночас зростає значення засобів радіоелектронної боротьби (РЕБ), які нівелюють переваги високотехнологічних систем шляхом придушення сигналів або перехоплення управління. Така динамічна конкуренція створює технологічний паритет, але в умовах високої інтенсивності брак GPS змушує переходити до альтернатив, таких як радіомаяки, що може генерувати нові вразливості без кіберзаходів [2; 10].

Інституційна перебудова та інтеграція з НАТО та ЄС

Трансформація технологічного середовища супроводжується інституційними змінами, де мережа професійних об’єднань відіграє роль посередника між державою, бізнесом та міжнародними партнерами [13]. Формування таких структур сприяє інституціоналізації сектору, раніше фрагментованого, з кількістю виробників понад 500 за SIPRI [9]. Звіт SIPRI є надійним завдяки глобальним даним, але недооцінює роль приватного сектору, де зростання інвестицій у deftech сягнуло 105 млн доларів у 2025 році [2]. Створення Міжвідомчої комісії з питань військово-промислової політики та оборонних технологій при РНБО України у 2026 році вказує на централізацію, але ризики бюрократії можуть уповільнити експорт.

Виклики технологічної конкуренції змушують НАТО переглядати інноваційну політику, як у ініціативах DIANA. Український досвід демонструє гнучкість, але традиційні моделі НАТО ускладнюють адаптацію [11]. Це створює структурний виклик: стандартизація повинна поєднуватися з українським темпом, як у передачі Saab 340 AEW&C у 2026 році. Звіт GLOBSEC “Seven Security Scenarios on Russian War in Ukraine for 2025–2026” є корисним для сценаріїв, але прогнози ескалації не завжди враховують AI-інтеграцію.

Кібербезпека та багатодоменні операції

Кібербезпека та багатодоменні операції становлять один із критичних аспектів сучасного оборонного середовища. Згідно з ENISA Threat Landscape 2023, у Європі спостерігається стійке зростання кіберзагроз, зокрема в секторах критичної інфраструктури та енергетики; для України цей тренд посилюється через геополітичний тиск [14]. Peer-reviewed стаття “The 2022-2023 Russia-Ukraine War and Cyberspace Threats” (Lagvilava, 2023) детально описує еволюцію кіберзагроз: від масових DDoS-атак на початку вторгнення до більш цілеспрямованих операцій проти енергетичної інфраструктури, транспортних систем та урядових мереж [21]. Така еволюція суттєво посилює ризик ескалації конфлікту, перетворюючи кіберпростір на повноцінний оперативний домен. Ефективність превентивних заходів залишається обмеженою без переходу до децентралізованої архітектури мереж та підвищення стійкості на рівні мікромереж і локальних енергетичних вузлів.

Економічні аспекти трансформації ОПК України визначаються як потенціалом зростання, так і структурними обмеженнями. За оцінками CFR (2025), потенціал експорту може сягати кількох мільярдів доларів США щорічно за умови гармонізації з європейськими стандартами [2].

Звіт McKinsey “European defense by the numbers” (2026) прогнозує зростання загальних витрат європейських країн НАТО на оборону до 800 млрд євро до 2030 року, що створює сприятливе середовище для інтеграції українського ОПК як постачальника інноваційних рішень [30]. Звіти European Defence Agency (EDA) свідчать, що витрати ЄС

на оборону у 2024 році сягнули 343 млрд євро зі зростанням на 19 %, що створює можливості для спільних проєктів з Україною [29;30].

Геополітичні імплікації трансформації українського ОПК полягають у потенціалі посилення колективної оборони через інтеграцію швидких інноваційних практик України в європейські структури. Згідно з публікацією Atlantic Council (2026), Європа потребує саме української моделі – швидкості адаптації, децентралізації розробок і тісного зворотного зв'язку з фронтом – для подолання власної бюрократичної інерції [10].

Така інтеграція може стати каталізатором змін у НАТО та ЄС, перетворюючи Україну з отримувача допомоги на ключового постачальника технологій і тактичних рішень. Водночас фрагментація європейського оборонного ринку створює інвестиційний та фінансовий дефіцит, оцінюваний у сотні мільярдів євро за наступне десятиліття; цей розрив ускладнює швидке нарощування спроможностей і робить Європу вразливою до зовнішніх постачальників.

Розвиток ОПК України

Важливість розвитку власної оборонної промисловості важко переоцінити, оскільки технологічна перевага завжди відіграє ключову роль у військових конфліктах і російсько-українська війна лише підтверджує цей факт.

Ще до початку широкомасштабної російської агресії було визначено *критичні чинники*, які суттєво впливали на розвиток ОПК України, а саме:

відсутність дієвих механізмів переходу від виробництва одиночних і малосерійних виробів до *серійного виробництва* новітніх зразків ОВТ, залучення інвестицій у галузь;

недостатня концентрація ресурсів для реалізації пріоритетних напрямів створення ОВТ нових поколінь;

повна відсутність державної підтримки та фінансування *розвитку критичних технологій* у сфері ОПК України та проведення фундаментальних досліджень в інтересах Сил безпекиі оборони України;

низький рівень узгодженості військово-технічної та військово-промислової політики під час розроблення новітніх зразків ОВТ;

низький рівень військово-технічного співробітництва для залучення міжнародних компаній до інвестування в підприємства ОПК.

За останні роки вітчизняна оборонна промисловість демонструє значний розвиток та налагодила виробництво широкого спектру озброєнь, насамперед артилерійські системи, міномети, бронетехніку, FPV-дрони, водні дрони, ракети, боєприпаси радянських калібрів. У той же час забезпечення потреб Сил безпеки і оборони України залишається на недосяжному рівні і на даний час складає близько 40%, що в свою чергу вимагає значних фінансових витрат з державного бюджету на імпорт озброєння та боєприпасів і призводить до критичної залежності від міжнародної військової допомоги.

Одним із основних факторів, що гальмують розвиток ОПК України, є *безпека інфраструктури*, оскільки багато підприємств залишаються в зоні підвищеного ризику через бойові дії, що ускладнює виробництво та призводить до потреби релокації підприємств. Не менш важливим фактором є *критична залежність від імпортних комплектуючих та сировини*, зокрема вибухових речовин, які держава не виробляє у достатніх обсягах.

Також негативно впливає на розвиток оборонної промисловості *відсутність належного механізму державної фінансової підтримки* для відновлення пошкоджених або знищених виробничих потужностей, що суттєво ускладнює виконання оборонних замовлень.

Тому ОПК України сьогодні потребує *системної трансформації*, тобто не просто формування сукупності оборонних підприємтсв, а створення динамічної екосистеми, у якій обєднані державні та приватні підприємсства, де організована тісна взаємодія з міжнародними корпораціями.

З цією метою було проведено оцінювання здатності ОПК України щодо подальшого розвитку за допомогою SWOT-аналізу. Вага кожного фактору була обґрунтована їх прямим впливом на здатність ОПК зберігати конкурентну перевагу в умовах асиметричного конфлікту та переходити до системної інтеграції з європейською безпековою архітектурою:

Сильні сторони ОПК України: швидка адаптація технологій; значна кількість виробників (близько 500); потужний приватний сектор, що забезпечує інноваційну гнучкість.

Слабкі сторони: фрагментація сектору; гострий дефіцит кваліфікованих фахівців (embedded-розробників, інженерів РЕБ, спеціалістів з кібербезпеки), що обмежує масштабування виробництва.

Можливості ОПК України: інтеграція в програми НАТО (зокрема DIANA); потенціал експорту інноваційних рішень на європейський ринок.

Загрози: зростаюча кількість багатодоменних кіберзагроз; залежність від зовнішньої допомоги, яка може бути нестабільною в довгостроковій перспективі.

Результати проведеного SWOT-аналізу обумовлюють доцільність розроблення довгострокової стратегії розвитку (модернізації) ОПК України. Ключовими цілями і пріоритетами зазначеної стратегії повинні стати:

у *короткостроковій перспективі* (*під час війни*) – підвищення спроможності забезпечувати потреби Сили безпеки і оборони України в ОВТ та боєприпасах;

у *довгостроковій перспективі* (*післявоєнний період*) – повне забезпечення потреб Сил безпеки і оборони України, створення відповідних запасів та збільшення експортного потенціалу; інтеграція в оборонні стандарти та виробничі ланцюги НАТО та ЄС.

При цьому *основними напрямками подальшого розвитку* ОПК України вважається:

масштабування виробництва ОВТ та боєприпасів;

підтримка наукових розробок та інноваційних рішень (FPV-дрони, морські дрони, автономні роботизовані платформи, високоточна зброя, штучний інтелект);

розвиток спільних проєктів з іноземними партнерами, залучення інвестицій, створення спільних підприємств;

створення прозорої системи захисту інтелектуальної власності та нормативно-правове врегулювання (впровадження механізмів надання державної допомоги для відновлення пошкоджених або знищених виробничих потужностей).

Важливим напрямком подальшого розвитку ОПК повинно стати *державно-приватне партнерство*. Це дозволить збільшити інвестиції за рахунок залучення приватного капіталу, підвищити якість внаслідок збільшення конкуренції в приватному секторі, швидше реагувати на потреби Сил безпеки і оборони України та зменшити навантаження на бюджет.

Ще одним із важливих напрямків розвитку оборонної промисловості має стати формування експортного потенціалу оборонної продукції. З цією метою доцільно використати конкурентні переваги:

по-перше – приваблива ціна, оскільки практично будь-яке українське озброєння в 1,5-2 рази дешевше, ніж іноземні аналоги;

по-друге – ефективність та інноваційність, у тому числі завдяки постійній комунікації між виробником, винахідником і споживачем (безпосереднє застосування на полі бою).

Необхідно також здійснити *перегляд експортної політики* товарів військового призначення та подвійного використання. Мова йде не про зняття заборони на експорт озброєння, а впровадження жорстких правил та принципів:

під час війни – експорт деяких видів озброєнь, які є у профіциті (морські дрони, протитанкові засоби та інше);

у післявоєнний період – поступове зняття заборони на експорт, з урахуванням забезпечення поточних потреб Сил безпеки і оборони України та створення відповідних запасів.

На *короткострокову перспективу* ОПК повинен стати фундаментом безпеки та інноваційним кластером економіки України, а на *довгострокову перспективу* його роль слід розглядати в розрізі елементу нової архітектури національної економіки.

Авторська модель впливу ОПК на міжнародну безпеку: "Інтеграційна піраміда ОПК України"

Потрібно відзначити, що розроблена модель "Інтеграційна піраміда ОПК України" – це конструкція для оцінювання впливу ОПК України на міжнародне безпекове середовище.

Вона базується на синтезі емпіричних даних із джерел, таких як звіти SIPRI [9], ENISA Threat Landscape 2023 [14], Council on Foreign Relations (CFR) [2] та інші, і покликана пояснити, як внутрішні трансформації ОПК України можуть переростати в глобальні ефекти.

Модель структурована як піраміда з трьома рівнями, де кожен наступний залежить від попереднього (рис.).

Рис. Інтеграційна піраміда ОПК України

Базовий рівень – це *технологічна автономність*, фундаментом якої є частка локалізованого виробництва, скорочення циклу інновацій (від тижнів до місяців), адаптація комерційних технологій до військових потреб. Наприклад, зростання виробництва дронів щорічно ілюструє, як автономність дозволяє швидко реагувати на нові виклики [10]. Без міцного базису неможлива стійка інтеграція з міжнародними структурами, оскільки залежність від зовнішніх постачальників робить систему вразливою.

Середній рівень – це *регуляторна гармонізація*, перехідний етап, де технологічна автономність інтегрується з міжнародними стандартами ЄС та НАТО. Вона вимірюється ступенем відповідності нормам (технічні регламенти, сертифікація, кількість спільних програм). Без цього рівня автономні розробки залишаються ізольованими: українські FPV-дрони з оптоволоконним керуванням чи системи РЕБ не можуть вийти на експортні ринки чи інтегруватися в альянсні структури. Гармонізація з європейськими нормами дозволяє уникнути бар'єрів і перетворити локальні інновації на спільні проєкти [31].

Вершина – це міжнародний вплив, кінцевий результат, вимірюваний експортним обсягом (кілька млрд дол. США), кількістю спільних програм з НАТО, стійкістю до кіберзагроз та внеском у колективну безпеку. Вплив проявляється через механізми скорочення залежності (від імпорту до експорту), прискорення інновацій, дипломатію технологій (внесок у колективну оборону) та ін.

Розроблена модель має *певні межі* – без повної інституційної інтеграції (членство в НАТО чи ЄС) вплив обмежується асиметричними конфліктами [27].

У цілому, "Інтеграційна піраміда ОПК України" – це інструмент для стратегічної оцінки, що синтезує дані для прогнозування. Вона не є статичною і адаптується до змін (зростання інвестицій, нові загрози тощо).

Висновки

Проведений аналіз дозволяє модифікувати первинну гіпотезу: технологічна автономність, поєднана з регуляторною інтеграцією до стандартів ЄС та НАТО, формує системний міжнародний вплив України на європейську безпеку, але цей ефект залишається обмеженим без глибокої інституційної трансформації.

Досвід російсько-української війни надає Україні конкурентну перевагу в асиметричних високотехнологічних рішеннях, зокрема в автономних системах, засобах радіоелектронної боротьби та низьковартісних безпілотних платформах, інтегрованих у цифрові мережі управління.

Європейська та міжнародна безпека дедалі більше залежать від українського досвіду як від реального випробувального полігону оборонних технологій у умовах hybrid warfare. Провал дороговартісних стартапів контрастує з масовою ефективністю дешевих FPV-систем. Реальна бойова валідація в Україні стає ключовим критерієм для масштабування оборонних інновацій у Європі, мінімізуючи інвестиційні ризики та визначаючи стандарти ефективності в міжнародному безпековому середовищі.

Реалізація потенціалу ОПК України вимагає посиленої кооперації з Європейським Союзом та Північноатлантичним альянсом. Потенціал експорту може становити кілька мільярдів доларів за умови відповідності західним стандартам. Стратегічно розвиток українського оборонного сектору виступає інвестицією у стійкість Європи, але для повної реалізації необхідна адаптація інституційних механізмів НАТО до більш гнучкої моделі інноваційного управління. Очевидним є те, що розвиток української оборонної бази пов'язаний з європейською обороноздатністю. Така залежність означає і взаємний ризик.

Модель "Інтеграційна піраміда ОПК України" підтверджує ієрархічну залежність факторів, де технологічна автономність слугує базисом для регуляторної гармонізації, а та – для міжнародного впливу. Ця конструкція є аналітичним внеском, що базується на синтезі емпірики, але визнає свої межі: в асиметричних конфліктах середнього масштабу вона ефективна. Проте в глобальних сценаріях вимагає доповнення факторами відновлення після війни.

Загалом, трансформація ОПК України не тільки відповідає на виклики російсько-української війни, але й переосмислює європейську безпеку, роблячи акцент на гібридності технологій та інституцій.

Рекомендації

Для максимальної реалізації потенціалу ОПК України в контексті міжнародної безпеки першочергово варто продовжити гармонізацію стандартів виробництва з нормами Європейського Союзу та Північноатлантичного альянсу, зокрема через ініціативи на кшталт Defence Innovation Accelerator for the North Atlantic (DIANA), де бюджет у 1 млрд євро дозволяє прискорити спільні розробки.

Розширення програм спільного виробництва з державами-членами ЄС, з фокусом на ППО та дрони, стане логічним кроком, оскільки ППО, дрони та боєприпаси збільшеної дальності є ключовими оборонними пріоритетами України у 2026 році. Спрощення регуляторних процедур без послаблення експортного контролю дозволить підвищити конкурентоспроможність, хоча це вимагає балансу між швидкістю інновацій та безпековими стандартами, аби уникнути ризиків, подібних до невдач Stark Defence.

Збереження механізму бойового зворотного зв'язку як ключового інструменту ітерацій інновацій є критичним, оскільки саме зворотний зв'язок з фронту забезпечує адаптацію, роблячи український досвід уроком для НАТО.

Інвестування в модернізацію критичної інфраструктури як складової оборонної стратегії, з децентралізацією за рекомендаціями IEA "World Energy Outlook 2023", має стати пріоритетом для протидії кіберзагрозам і ескалації, інтегруючи це з НАТО для спільного моніторингу.

Посилення фокусу на ППО та дронах повинно супроводжуватися розвитком ракетних програм через державно-приватне партнерство. Розробка стратегій кіберзахисту, яка базується на ENISA "Threat Landscape 2023", з тренінгами для персоналу та інтеграцією штучного інтелекту з етичними стандартами, забезпечить превентивні заходи проти зростання інцидентів.

Проведення щорічного SWOT-аналізу ОПК України з моніторингом загроз дозволить адаптивно реагувати на динаміку, перетворюючи рекомендації на стратегічну рамку для довгострокового розвитку.

Список використаних джерел

1. Залужний В. Про зміну характеру війни. *Українська правда.* 2026. URL: https://www.pravda.com.ua/columns/2026/02/23/8022301/ (дата звернення: 27.02.2026).
2. Sestanovich S. Securing Ukraine's Future in Europe: Ukraine's Defense Industrial Base as an Anchor for Economic Renewal and European Security. *Council on Foreign Relations.* 2025. URL: https://www.cfr.org/articles/securing-ukraines-future-in-europe-ukraines-defense-industrial-base-an-anchor-for-economic-renewal-and-european-security (дата звернення: 27.02.2026).
3. Krepinevich A. Cavalry to Computer: The Pattern of Military Revolutions. *The National Interest.* 1994. № 37. С. 30–42. URL: https://www.jstor.org/stable/42896863.
4. Murray W., Knox M. The Dynamics of Military Revolution 1300–2050. Cambridge : Cambridge University Press, 2001.
5. Freedman L. The Future of War: A History. London : Allen Lane, 2017.
6. Kaldor M. New and Old Wars: Organized Violence in a Global Era. Stanford : Stanford University Press, 2012.
7. Scharre P. Army of None: Autonomous Weapons and the Future of War. New York : W.W. Norton & Company, 2018.
8. Horowitz M. C. The Diffusion of Military Power: Causes and Consequences for International Politics. Princeton : Princeton University Press, 2010.
9. Trends in world military expenditure, 2023. *Stockholm International Peace Research Institute.* URL: https://www.sipri.org/publications/2023/sipri-fact-sheet/trends-world-military-expenditure-2023 (дата звернення: 27.02.2026). (Оновлено: дані 2024 в SIPRI Trends 2024).
10. Dickinson P., Kostyuk N. Ukrainian defense tech companies must prepare for export opportunities. *Atlantic Council.* 2025. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-defense-tech-companies-must-prepare-for-export-opportunities/ (дата звернення: 27.02.2026).
11. Giles K. NATO can learn from Ukraine's military innovation. *Chatham House.* 2023. URL: https://www.chathamhouse.org/publications/the-world-today/2023-02/nato-can-learn-ukraines-military-innovation (дата звернення: 27.02.2026).
12. DroneXL. Peter Thiel-backed Stark Defence fails all four strikes. 2025. URL: https://dronexl.co/2025/10/31/peter-thiel-backed-stark-defence-fails-all-four-strikes/ (дата звернення: 27.02.2026).
13. Ukrainian Defence Associations Overview. *Security Assistance Hub.* 2024. URL: https://sahasec.org/policy-briefs/ukrainian-defence-associations-overview/ (дата звернення: 27.02.2026).
14. European Union Agency for Cybersecurity. *ENISA Threat Landscape* 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 27.02.2026).

15. Defence Innovation Accelerator for the North Atlantic (DIANA). *NATO*. 2023. URL: https://www.nato.int/cps/en/natohq/topics_185166.htm (дата звернення: 27.02.2026).
16. "Очікую прориву в українській ракетній програмі". Прогнози українського deftech на 2026. *DOU.* 2026. URL: https://dou.ua/lenta/articles/deftech-forecasts-for-2026/ (дата звернення: 27.02.2026).
17. ППО, дрони та боєприпаси збільшеної дальності – названі ключові оборонні пріоритети України у 2026 році. *ArmyInform.* 2026. URL: https://armyinform.com.ua/2026/01/26/protypovitryana-oborona-drony-ta-boyeprypasy-zbilshenoyi-dalnosti-nazvani-klyuchovi-oboronni-priorytety-ukrayiny-u-2026-roczi/ (дата звернення: 27.02.2026).
18. Указ Президента України "Про Рішення Ради національної безпеки і оборони України від 22 листопада 2025 року "Про Міжвідомчу комісію з питань військово-промислової політики та оборонних технологій". *Офіційне інтернет-представництво Президента України*. 2026. Указ № 116/2026. URL: https://www.president.gov.ua/documents/1162026-58317 (дата звернення: 02.03.2026).
19. Технології фронту: найперспективніші інвестиційні напрями у 2026. *IT Arena*. 2026. URL: https://itarena.ua/ua/tehnologi%d1%97-frontu-najperspektivnishi-investiczijni-napryami-u-2026/ (дата звернення: 27.02.2026).
20. Гурковський В., Романенко Є., Коваль В., Ільницький С. Форсайт-дослідження як інструмент зміцнення резильєнтності до загроз БПЛА з оптоволоконним управлінням. *Національні інтереси України*. 2025. №7 (12). URL: https://perpectives.pp.ua /index.php/niu/view/26219. DOI: https://doi.org /10.52058/3041-1793-2025-7(12)-88-101 (дата звернення: 02.03.2026).
21. The 2022-2023 Russia-Ukraine War and Cyberspace Threats. *ResearchGate*. 2023. URL: https://www.researchgate.net/publication/373855591_The_2022-2023_Russia-Ukraine_War_and_ Cyberspace_Threats (дата звернення: 27.02.2026).
22. Modern cyber threats to critical infrastructure in Ukraine and the world. *ResearchGate.* 2025. URL: https://www.researchgate.net/publication/390394323_MODERN_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_IN_UKRAINE_AND_THE_WORLD (дата звернення: 27.02.2026).
23. EU policymakers expect no immediate oil security impact from Iran conflict, email shows. *Reuters.* March 2, 2026. URL: https://www.reuters.com/business/energy/eu-policymakers-expect-no-immediate-oil-security-impact-iran-conflict-email-2026-03-02 (дата звернення: 02.03.2026).
24. The Regional Reverberations of the U.S. and Israeli Strikes on Iran. *CSIS.* March 1, 2026. URL: https://www.csis.org/analysis/regional-reverberations-us-and-israeli-strikes-iran (дата звернення: 02.03.2026).
25. IAEA Director General's Introductory Statement to the Extraordinary Board of Governors. *IAEA.* March 2, 2026. URL: https://www.iaea.org/newscenter/statements/iaea-director-generals-introductory-statement-to-the-board-of-governors-2-march-2026 (дата звернення: 02.03.2026).
26. Countering cyber threats to Ukraine's national security: institutional and preventive capability. *ResearchGate*. 2026. URL: https://www.researchgate.net/publication/400373357_Countering_ cyber_threats_to_Ukraine's_national_security_institutional_and_preventive_capability (дата звернення: 27.02.2026).
27. National Resilience of Ukraine: Content and Security Strategy in the Context of a War and Post-war Recovery. *ResearchGate*. 2025. URL: https://www.researchgate.net/publication/393564415_ National_Resilience_of_Ukraine_Content_and_Security_Strategy_in_the_Context_of_a_War_and_Post-war_Recovery (дата звернення: 27.02.2026).
28. World Energy Outlook 2023. *IEA.* URL: https://www.iea.org/reports/world-energy-outlook-2023 (дата звернення: 27.02.2026).
29. Defence Data 2023-2024. *European Defence Agency.* 2024. URL: https://eda.europa.eu/docs/default-source/brochures/eda-defence-data-2023.pdf (дата звернення: 27.02.2026).
30. European defense by the numbers. *McKinsey.* 2026. URL: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-by-the-numbers (дата звернення: 27.02.2026).
31. EU Defence Industry Transformation Roadmap. *EU Commission.* 2025. URL: https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf (дата звернення: 27.02.2026).

References

1. Zaluzhnyi, V. (2026). Pro zminu kharakteru viiny [On the changing nature of war]. *Ukrainska pravda.* Retrieved from: https://www.pravda.com.ua/columns/2026/02/23/8022301/ (accessed 27.02.2026) [in Ukrainian].
2. Sestanovich, S. (2025). Securing Ukraine's Future in Europe: Ukraine's Defense Industrial Base as an Anchor for Economic Renewal and European Security. *Council on Foreign Relations*. Retrieved from:

https://www.cfr.org/articles/securing-ukraines-future-in-europe-ukraines-defense-industrial-base-an-anchor-for-economic-renewal-and-european-security (accessed 27.02.2026).
3. Krepinevich, A. (1994). Cavalry to Computer: The Pattern of Military Revolutions. *The National Interest*, 37, 30–42. Retrieved from: https://www.jstor.org/stable/42896863.
4. Murray, W., & Knox, M. (2001). The Dynamics of Military Revolution 1300–2050. Cambridge: Cambridge University Press.
5. Freedman, L. (2017). The Future of War: A History. London: Allen Lane.
6. Kaldor, M. (2012). New and Old Wars: Organized Violence in a Global Era. Stanford: Stanford University Press
7. Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. New York: W.W. Norton & Company.
8. Horowitz, M. C. (2010). The Diffusion of Military Power: Causes and Consequences for International Politics. Princeton : Princeton University Press.
9. Trends in world military expenditure. (2023). *Stockholm International Peace Research Institute*. Retrieved from: https://www.sipri.org/publications/2023/sipri-fact-sheet/trends-world-military-expenditure-2023 (accessed 27.02.2026).
10. Dickinson, P., & Kostyuk, N. (2025). Ukrainian defense tech companies must prepare for export opportunities. *Atlantic Council.* Retrieved from: https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-defense-tech-companies-must-prepare-for-export-opportunities/ (accessed 27.02.2026).
11. Giles, K. (2023). NATO can learn from Ukraine's military innovation. *Chatham House*. Retrieved from: https://www.chathamhouse.org/publications/the-world-today/2023-02/nato-can-learn-ukraines-military-innovation (accessed 27.02.2026).
12. DroneXL. (2025). Peter Thiel-backed Stark Defence fails all four strikes. Retrieved from: https://dronexl.co/2025/10/31/peter-thiel-backed-stark-defence-fails-all-four-strikes/ (accessed 27.02.2026).
13. Ukrainian Defence Associations Overview. (2024). *Security Assistance Hub.* Retrieved from: https://sahasec.org/policy-briefs/ukrainian-defence-associations-overview/ (accessed 27.02.2026).
14. European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape.* Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed 27.02.2026).
15. Defence Innovation Accelerator for the North Atlantic (DIANA). (2023). *NATO*. Retrieved from: https://www.nato.int/cps/en/natohq/topics_185166.htm (accessed 27.02.2026).
16. "Ochikuiu proryvu v ukrainskii raketnii prohrami". Prohnozy ukrainskoho deftech na 2026 ["I expect a breakthrough in the Ukrainian missile program." Ukrainian deftech forecasts for 2026]. (2026). *DOU*. Retrieved from: https://dou.ua/lenta/articles/deftech-forecasts-for-2026/ (accessed 27.02.2026) [in Ukrainian].
17. PPO, drony ta boieprypasy zbilshenoi dalnosti – nazvani kliuchovi oboronni priorytety Ukrainy u 2026 rotsi [Air defense, drones and extended-range ammunition – Ukraine's key defense priorities in 2026 named]. (2026). *ArmyInform.* Retrieved from: https://armyinform.com.ua/2026/01/26/protypovitryana-oborona-drony-ta-boyeprypasy-zbilshenoyi-dalnosti-nazvani-klyuchovi-oboronni-priorytety-ukrayiny-u-2026-roczi/ (accessed 27.02.2026) [in Ukrainian].
18. Ukaz Prezydenta Ukrainy "Pro Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 22 lystopada 2025 roku "Pro Mizhvidomchu komisiiu z pytan viiskovo-promyslovoi polityky ta oboronnykh tekhnolohii" [Decree of the President of Ukraine "On the Decision of the National Security and Defense Council of Ukraine dated November 22, 2025 "On the Interdepartmental Commission on Military-Industrial Policy and Defense Technologies"]. (2026). *Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy*. Ukaz № 116/2026. Retrieved from: https://www.president.gov.ua/documents/1162026-58317 (accessed 02.03.2026) [in Ukrainian].
19. Tekhnolohii frontu: naiperspektyvnishi investytsiini napriamy u 2026 [Front-end technologies: the most promising investment directions in 2026]. (2026). *IT Arena*. Retrieved from: https://itarena.ua/ua/tehnologi%d1%97-frontu-najperspektivnishi-investiczijni-napryami-u-2026/ (accessed 27.02.2026) [in Ukrainian].
20. Hurkovskyi, V., Romanenko, Ye., Koval, V., & Ilnytskyi, S. (2025). Forsait-doslidzhennia yak instrument zmitsnennia rezylientnosti do zahroz BPLA z optovolokonnym upravlinniam [Foresight research as a tool for strengthening resilience to fiber-optic-controlled UAV threats]. *Natsionalni interesy Ukrainy*, 7 (12), 88-101. Retrieved from: https://perpectives.pp.ua /index.php/niu/view/26219. DOI: https://doi.org /10.52058/3041-1793-2025-7(12)-88-101 (accessed 02.03.2026) [in Ukrainian].
21. The 2022-2023 Russia-Ukraine War and Cyberspace Threats. (2023). *ResearchGate*. Retrieved from: https://www.researchgate.net/publication/373855591_The_2022-2023_Russia-Ukraine_War_and_Cyberspace_Threats (accessed 27.02.2026).
22. Modern cyber threats to critical infrastructure in Ukraine and the world. (2025). *ResearchGate.* Retrieved from:

https://www.researchgate.net/publication/390394323_MODERN_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_IN_UKRAINE_AND_THE_WORLD (accessed 27.02.2026).
23. EU policymakers expect no immediate oil security impact from Iran conflict, email shows. (March 2, 2026). *Reuters.* Retrieved from: https://www.reuters.com/business/energy/eu-policymakers-expect-no-immediate-oil-security-impact-iran-conflict-email-2026-03-02 (accessed 02.03.2026).
24. The Regional Reverberations of the U.S. and Israeli Strikes on Iran. (March 1, 2026). *CSIS*. Retrieved from: https://www.csis.org/analysis/regional-reverberations-us-and-israeli-strikes-iran (accessed 02.03.2026).
25. IAEA Director General's Introductory Statement to the Extraordinary Board of Governors. (March 2, 2026). *IAEA.* Retrieved from: https://www.iaea.org/newscenter/statements/iaea-director-generals-introductory-statement-to-the-board-of-governors-2-march-2026 (accessed 02.03.2026).
26. Countering cyber threats to Ukraine's national security: institutional and preventive capability. (2026). *ResearchGate*. Retrieved from: https://www.researchgate.net/publication/400373357_Countering_cyber_threats_to_Ukraine's_national_security_institutional_and_preventive_capability (accessed 27.02.2026).
27. National Resilience of Ukraine: Content and Security Strategy in the Context of a War and Post-war Recovery. (2025). *ResearchGate*. Retrieved from: https://www.researchgate.net/publication/393564415_National_Resilience_of_Ukraine_Content_and_Security_Strategy_in_the_Context_of_a_War_and_Post-war_Recovery (accessed 27.02.2026).
28. World Energy Outlook 2023. *IEA.* Retrieved from: https://www.iea.org/reports/world-energy-outlook-2023 (accessed 27.02.2026).
29. Defence Data 2023-2024. (2024). *European Defence Agency*. Retrieved from: https://eda.europa.eu/docs/default-source/brochures/eda-defence-data-2023.pdf (accessed 27.02.2026).
30. European defense by the numbers. (2026). *McKinsey*. Retrieved from: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-by-the-numbers (accessed 27.02.2026).
31. EU Defence Industry Transformation Roadmap. (2025). *EU Commission.* Retrieved from: https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf (accessed 27.02.2026).