Received 05.02.2026 | Accepted 25.02.2026 | Published 30.03.2026

УДК: 355.865:355.021.2 DOI: 10.63978/3083-6476.2026.1.4.06

Романенко Євген Олександрович
доктор наук з державного управління, професор
начальник управління
Центральний науково-дослідний інститут Збройних Сил України
Київ, Україна
e-mail: poboss1978@gmail.com
ORCID: 0000-0003-2285-0543

Сокоринський Юрій Володимирович
доктор юридичних наук, доцент
співробітник Служби безпеки України
Служба безпеки України
Київ, Україна
e-mail: usokorinskiy@ukr.net
ORCID: 0000-0002-8907-9880

Жора Віктор Володимирович
військовослужбовець
Національна гвардія України
ORCID: 0000-0003-2679-3056

АНАЛІЗ ДИСПРОПОРЦІЇ МІЖ ДИНАМІКОЮ ГІБРИДНИХ (ДОПОРОГОВИХ) ЗАГРОЗ ТА ЧИННОЮ МОДЕЛЛЮ УПРАВЛІННЯ СЕКТОРОМ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Анотація. *У статті аналізується системна диспропорція між прискореною еволюцією гібридних (допорогових) загроз та консервативною вертикально-ієрархічною моделлю управління сектором безпеки і оборони України. На основі даних CSIS (2025), ENISA Threat Landscape 2025, RAND "From Policy to Victory" (2025), звіту NATO StratCom COE "The Collage of the Kremlin's Communication Strategy" (2025) та WEF Global Cybersecurity Outlook 2025 автор доводить, що традиційні відомчі «силоси» стали головною вразливістю держави. Агресор діє нелінійно та мережево, експлуатуючи "шви" між компетенціями РНБО, МО, СБУ, Держспецзв'язку та приватними операторами критичної інфраструктури (понад 80 % об'єктів).*

Чинна нормативна база (Закон "Про національну безпеку" 2018, Стратегія кібербезпеки 2021, Розпорядження Кабінету Міністрів України № 853-р 2025) не передбачає ефективних механізмів горизонтальної координації та оперативного обміну даними в реальному часі. Це призводить до хронічного інституційного лагу, коли розвідувальна інформація не встигає трансформуватися в превентивні дії.

Ключовим рішенням пропонується створення Об'єднаного аналітичного центру гібридних загроз (ОАЦГЗ) – компактного хаба (55–65 фахівців), підпорядкованого безпосередньо РНБО. Центр поєднує три блоки: прогнозний моніторинг на базі AI, юридично-атрибуційну оцінку та державно-приватний інтерфейс з Data Sharing Agreements. Реалізація вимагає точкових змін до Закону "Про національну безпеку" та оновлення Стратегії кібербезпеки з елементами Active Defense.

Практичне значення роботи полягає в обґрунтуванні переходу від реактивної до предиктивної моделі управління СБО та наданні конкретних рекомендацій щодо пілотного запуску ОАЦГЗ у 2027 році.

Ключові слова: *гібридні загрози, допорогова агресія, сектор безпеки і оборони, Об'єднаний аналітичний центр гібридних загроз, горизонтальна координація, приватно-державне партнерство, активна оборона, НАТО, стійкість критичної інфраструктури.*

Yevhen Romanenko
Doctor of Science in Public Administration Professor
Leading Researcher
Central Research Institute of the Armed Forces of Ukraine
Kyiv, Ukraine
e-mail: poboss1978@gmail.com
ORCID: 0000-0003-2285-0543

Yurii Sokorynskyi
Doctor of Juridical Sciences, Associate Professor
Security Service of Ukraine officer
Security Service of Ukraine
Kyiv, Ukraine
e-mail: usokorinskiy@ukr.net
ORCID: 0000-0002-8907-9880

Viktor Zhora
military personnel
National Guard of Ukraine
Kyiv, Ukraine
ORCID: 0000-0003-2679-3056

ANALYSIS OF THE DISPROPORTION BETWEEN THE DYNAMICS OF HYBRID (SUB-THRESHOLD) THREATS AND THE CURRENT MODEL OF MANAGEMENT OF UKRAINE'S SECURITY AND DEFENSE SECTOR

Abstract. *The article examines the systemic disproportion between the accelerated evolution of hybrid (sub-threshold) threats and the conservative vertical-hierarchical model of governance of Ukraine's security and defence sector (SDS). Drawing on CSIS data (2025), ENISA Threat Landscape 2025, RAND "From Policy to Victory" (2025), NATO StratCom COE "The Collage of the Kremlin's Communication Strategy" (2025), and WEF Global Cybersecurity Outlook 2025, the authors demonstrate that traditional inter-agency "silos" have become the primary vulnerability of the state. The aggressor operates non-linearly and networked, exploiting the "seams" between the RNBO, MoD, SBU, State Special Communications Service, and private critical infrastructure operators (over 80 % of objects).*

The existing normative framework (Law on National Security 2018, Cybersecurity Strategy 2021, CMU Order No. 853-r 2025) lacks effective mechanisms for horizontal coordination and real-time data exchange. This results in a chronic institutional lag, whereby intelligence information fails to translate into preventive action.

The central proposal is the establishment of a Joint Analytical Centre for Hybrid Threats (JACHT) – a compact hub (55–65 specialists) directly subordinated to the RNBO. The Centre integrates three functional blocks: AI-driven predictive monitoring, legal-attribution assessment, and a public-private interface based on Data Sharing Agreements. Implementation requires targeted amendments to Article 12 of the Law on National Security and updates to the Cybersecurity Strategy incorporating Active Defence elements.

The practical value of the study lies in substantiating the transition from a reactive to a predictive SDS governance model and providing concrete recommendations for the pilot launch of JACHT in 2027.

***Keywords**: hybrid threats, sub-threshold aggression, security and defence sector, Joint Analytical Centre for Hybrid Threats, horizontal coordination, public-private partnership, active defence, NATO, critical infrastructure resilience.*

JEL Classification: H56, H12, L86, O32, P43

Вступ

Еволюція засобів міждержавного протиборства станом на 2026 рік фактично розмила межу між конвенційною війною та миром. Сучасна конфліктність дедалі частіше відбувається в "сірій зоні", де гібридні впливи спрямовані на системну ерозію національної стійкості без формального оголошення війни. Для України, яка стала глобальною лабораторією першої повномасштабної інтегрованої війни, розв'язання цієї проблеми перетворилося на умову виживання.

Особливого експертного занепокоєння додають тенденції, задокументовані у звіті CSIS від 18 березня 2025 року: кількість російських актів саботажу в Європі майже потроїлася між 2023 та 2024 роками (з 12 до 34 атак), демонструючи чотирикратне зростання порівняно з 2022 роком. Основна відповідальність за ці операції лежить на ГРУ (гу гш зс рф), яке через агентурні мережі, безпілотні літальні апарати та "тіньовий флот" для підводних диверсій демонструє спроможність діяти поза класичним полем бою.

На цьому тлі чинна нормативно-правова база України, включно з фундаментом у вигляді Стратегії національної безпеки 2020 року, виявляє ознаки темпорального відставання, оскільки створювалася за умов зовсім іншої швидкості виникнення загроз.

Виникає критичний розрив: агресор діє нелінійно та мережево, тоді як вітчизняна модель управління сектором безпеки і оборони (далі – СБО) залишається заручником вертикальної бюрократії. Навіть враховуючи оновлення стратегії НАТО щодо гібридних загроз у січні 2026 року та запровадження посади Спеціального координатора, Україна ризикує залишити "вікна вразливості" відкритими через відсутність аналогічного горизонтального інтегратора. Як підкреслюється у дослідженні RAND "From policy to victory" (2025), український досвід інтеграції технологій може забезпечити перевагу лише за умови існування єдиної аналітичної платформи, інакше виявлена диспропорція управління лише посилюватиметься.

Огляд літератури

Наукове розуміння гібридних загроз пройшло довгий шлях. Спочатку вчені описували їх лише як набір тактичних прийомів кібератаки, пропаганду чи саботаж. Сьогодні ми говоримо про щось набагато глибше: "тотальну дифузію", коли агресор розмиває межі між війною і миром, поступово паралізуючи державні інститути.

Данилюк О. точно підмітив цю зміну: сучасні гібридні загрози – це вже не просто зовнішній тиск, а свідома експлуатація слабких місць демократії. Мета не знищити систему одним ударом, а виснажити її зсередини [15].

Український досвід став справжнім "лабораторією" таких конфліктів. Як зазначають у звітах RAND Corporation та в роботі Крапа А., саме Україна показала межі старих оборонних моделей. Традиційні ієрархічні структури, заточені під фізичне стримування, просто не встигають за атаками на когнітивну сферу та цифрову інфраструктуру [16].

Останні дослідження 2025 року тільки підтверджують цю тезу. У звіті НАТО Strategic Communications Centre of Excellence "The Collage of the Kremlin's Communication Strategy" автори детально розбирають, як Кремль поєднує цензуру, синтетичні медіа та пропаганду в єдину комунікаційну машину гібридної війни. Це вже не окремі операції – це цілісна стратегія впливу на свідомість [17].

World Economic Forum у "Global Cybersecurity Outlook 2025" іде ще далі. Звіт показує, як кіберзагрози в "Intelligent Age" переплітаються з дезінформацією. Атаки стають

конвергентними: один удар по інфраструктурі супроводжується інформаційною кампанією, яка підриває довіру суспільства. Традиційні підходи до захисту тут просто не працюють. [18].

Не менш важливий "Parliamentary Handbook on Disinformation, AI and Synthetic Media" від Commonwealth Parliamentary Association та Organization of American States. Автори прямо вказують: штучний інтелект робить фейки майже невловимими. Без швидкої атрибуції та нових законодавчих механізмів держави залишаються вразливими [19].

G7 у своєму аналітичному меморандумі (Policy Brief) "Strategy for Countering Russian Information Operations" (2025) фіксує ще одну тривожну тенденцію: кількість російських операцій FIMI в Європі майже потроїлася за рік [20]. При цьому Москва активно розширює діяльність на Індо-Тихоокеанський регіон, використовуючи локальні проксі-мережі. Це вже не європейська проблема – це глобальна мережа.

Євроатлантичне партнерство також реагує. Десятий прогрес-репорт НАТО-ЄС (2025) показує реальний прогрес: нові структуровані діалоги щодо сталості, кіберзахисту та оборонної промисловості. Але дослідники прямо пишуть: координація ще недостатня, щоб випереджати агресора [21].

Українські дослідники Сальнікова О., Сівоха І., Іващенко А. [22], а також Юськів Б., Карпчук Н. та Пелех О. (2024) [23] підкреслюють, що стратегічні комунікації в гібридній війні – це інструмент рефлексивного управління та випередження. Усі джерела сходяться в одному: ієрархічна модель програє мережевим атакам. Майбутнє – за горизонтальною взаємодією, інтеграцією приватного сектору та швидким обміном даними.

Мета та завдання статті

Мета статті – виявити причини структурної невідповідності чинної моделі управління СБО динаміці сучасних гібридних загроз. Завдання полягає в локалізації точок розриву між відомствами та обґрунтуванні створення Об'єднаного аналітичного центру гібридних загроз (ОАЦГЗ) як інструменту переходу від реактивної до предиктивної моделі.

Методи

Методологія ґрунтується на системному аналізі нормативних актів і компаративістиці організаційних структур СБО України та країн НАТО. Структури розглядаються не як статичні об'єкти, а як динамічні цикли прийняття рішень. Основу становить OSINT-аналіз верифікованих звітів CSIS та ENISA 2024–2025 років. Модель превентивно-реактивних дій (Preventive-Response Options) НАТО (2026) слугує базисом, який, однак, потребує адаптації до українських реалій, де співпраця з приватним сектором досі має декларативний характер.

Окремо враховано аналітику RAND Corporation (2025) щодо еволюції гібридних інструментів у бік підвищення їхньої летальності, що змушує відмовитися від суто описових підходів на користь предиктивного моделювання.

Результати

Традиційні ієрархічні системи безпеки втрачають ефективність, коли агресор діє нелінійно, одночасно в кількох доменах і з високою швидкістю. Гібридні (допорогові) загрози являють собою синхронізоване поєднання невійськових інструментів від кібероперацій до саботажу з метою системного виснаження суверенітету без переходу до відкритої фази конфлікту. Об'єктом впливу стає не територія, а функціональна спроможність інститутів і стійкість критичної інфраструктури.

Ключові характеристики таких загроз: допороговість, конвергентність і атрибутивна неоднозначність. У 2026 році вони перетворилися на алгоритмізовану агресію. Дані CSIS

(2025) свідчать, що понад 21 % російських підривних операцій у Європі спрямовані на енергетику та логістичні ланцюги.

НАТО реагує на ці виклики через комплексний підхід (Comprehensive Approach), подвоюючи кількість багатонаціональних бойових груп та закладаючи рекордні витрати на оборону до 5 % ВВП до 2035 року. Однак для України ситуація ускладнюється внутрішньою фрагментацією. Розпорядження Кабінету Міністрів України № 853-р від 13 серпня 2025 року визнає наявність нормативних документів, які не мають єдиної візії та належної координації. Така ситуація при реальній відсутності надвідомчого аналітичного хаба створює умови, за яких держава залишається в стані постійної реактивності. Відтак, перебудова моделі управління СБО на основі мережевої синергії розвідки, держорганів та приватного сектору розглядається як спосіб збереження керованості в умовах "тотальної гібридності".

Технічний аналіз та відомчі обмеження

Яскравим прикладом стала синхронізована атака на енергосистему Польщі (грудень 2025), де агресор поєднав вразливості FortiGate з вайпером DynoWiper [6], вивівши з ладу понад 30 об'єктів генерації. В українському контексті протидія таким атакам натикається на жорстку відомчу сегментацію. Закон "Про національну безпеку" (2018) чітко розмежовує повноваження, але не передбачає механізмів швидкої взаємодії в "сірій зоні".

Відповідно до Закону "Про національну безпеку України" [7], сектор безпеки має чітку, але надто ізольовану структуру. Повноваження Міністерства оборони, згідно зі Стратегією воєнної безпеки [8], сфокусовані на відсічі збройній агресії, що фактично паралізує залучення військового ресурсу (включно з де-юре відсутніми кіберсилами) до інцидентів у "сірій зоні", які формально не класифікуються як акт війни.

Своєю чергою, Служба безпеки України, виконуючи функції контррозвідки, часто вступає у функціональний конфлікт із Кіберполіцією та Держспецзв'язку. Останній, спираючись на Стратегію кібербезпеки [9], забезпечує захист державних інформаційних ресурсів, проте критична інфраструктура, що перебуває у приватній власності, залишається в зоні «невизначеної відповідальності». Це створює ідеальні умови для агресора: атака на приватного обленерго-провайдера юридично не є атакою на державу, хоча її соціальні наслідки ідентичні.

Рада національної безпеки і оборони України, попри свій статус координаційного органу [2], залишається структурою стратегічного планування. Процес скликання засідань та підготовки Указів Президента України створює часовий лаг, який у 2026 році вимірюється годинами, тоді як автоматизовані атаки розвиваються за мілісекунди. Як зазначають експерти RAND у звіті 2025 року, основні суб'єкти кібербезпеки можуть володіти індикаторами компрометації (IoC) ще до початку атаки, проте складні протоколи передачі таємної інформації цивільним відомствам, таким як Міненерго, блокують можливість превентивного реагування [4].

Генезис безпекових викликів та еволюція гібридного інструментарію

Трансформація безпекового середовища навколо України, що набула критичної фази у 2025–2026 роках, не є випадковим сплеском активності, а результатом послідовного генезису доктрини "постійного конфлікту". Витоки нинішнього розриву в управлінні слід шукати в переході від спорадичних дезінформаційних кампаній до системної, алгоритмізованої агресії. Як зазначають дослідники RAND Corporation (2025), сучасна модель гібридної війни рф остаточно оформилася як стратегія "керованого хаосу", де основний акцент зміщено з прямого воєнного зіткнення на дестабілізацію через некінетичні методи [5].

Статистичні дані CSIS підтверджують цей еволюційний злам. Якщо у 2022 році було зафіксовано лише 3 масштабні акти саботажу в Європі, то у 2023-му їхня кількість зросла до 12, а у 2024-му – до 34 [1]. Такий темп (майже трикратне зростання щороку) вказує на

те, що агресор перейшов до етапу “виснаження інфраструктурної стійкості”. Генезис цих викликів демонструє перехід від вузькопрофільних кібератак до конвергентних операцій, де злам цифрового контуру є лише підготовчим етапом для фізичного руйнування об’єктів енергетики чи логістики.

Згідно зі звітом ENISA Threat Landscape 2025, загальна кількість верифікованих інцидентів у Європейському регіоні сягнула 4875, причому 77 % з них становили DDoS-атаки нового покоління, що використовуються як “шумова завіса” для глибшого проникнення в мережі [6].

Для України цей генезис має ще складніший характер. Ми спостерігаємо зрощення кримінальних мереж, проксі-груп та спецслужб рф. НАТО у своїх оновлених оцінках 2026 року визнає, що швидкість, з якою гібридні загрози адаптуються до контрзаходів, перевищує можливості будь-якої закритої ієрархічної системи [3]. Таким чином, генезис викликів випереджає генезис інституцій, створюючи той самий розрив, який ми пропонуємо подолати через мережеву трансформацію СБО.

Інституційний аналіз сектору безпеки і оборони в контексті гібридного протиборства

Проведений інституційний аналіз чинної архітектури СБО України вказує на її детермінованість принципами жорсткої вертикалі, що закладалися ще у 2018 році при ухваленні профільного Закону “Про національну безпеку” [7]. Ця модель виходить із презумпції чіткого розподілу ролей: Міноборони – відсіч агресії, СБУ – контррозвідка, МВС – громадський порядок. Проте в умовах 2026 року, коли межі між цими доменами стерті зусиллями агресора, така спеціалізація перетворюється на певну інституційну пастку.

Ключовим вузлом координації залишається Рада національної безпеки і оборони (РНБО). Згідно зі Стратегією національної безпеки 2020 року, саме цей орган має забезпечувати системну єдність [2]. Проте на практиці РНБО функціонує як орган стратегічного координатора, а не оперативного управління. Між ухваленням рішення на рівні РНБО та його імплементацією конкретним відомством утворюється “інституційний лаг”, який є критично неприпустимим при нейтралізації швидких гібридних інцидентів.

Особливого аналізу потребує роль Держспецзв’язку у світлі Стратегії кібербезпеки 2021 року [9]. Попри розширення повноважень, цей інститут залишається обмеженим державним сектором. Як підкреслюють експерти RAND Corporation (2025), сучасна стійкість (resilience) неможлива без інтеграції комерційних технологій та приватних операторів критичної інфраструктури [4]. В українській інституційній моделі приватний сектор досі розглядається не як повноправний суб’єкт СБО, а як об’єкт регулювання або захисту.

Розвідувальна спільнота (ГУР МО, СЗРУ), чия діяльність регулюється Законом “Про розвідку”, володіє найвищим рівнем обізнаності щодо намірів ворога, проте інституційні бар’єри (режим секретності, відсутність спільних дата-платформ) перешкоджають миттєвій передачі цих даних цивільним міністерствам. Як результат, виникає парадоксальна ситуація: держава має інформацію про загрозу, але не має гнучкого механізму її реалізації без задіяння громіздкої бюрократичної машини.

Порівняння з оновленими протоколами НАТО 2026 року свідчить, що успішні системи сьогодні будуються на принципі “горизонтальної довіри”, де обмін даними відбувається в реальному часі без постійної апеляції до вищого керівництва [3]. В Україні ж інституційна культура залишається орієнтованою на “звіт вгору”, що автоматично робить систему реактивною. Отже, інституційна “криза” СБО полягає не у відсутності органів, а в їхній певній закритості, ізольованості та нездатності до мережевої синергії, що прямо підтверджується накопиченням стратегічних документів [10].

Компаративний аналіз моделей стійкості: досвід країн НАТО та українські реалії

Усвідомлення глибини управлінського розриву в Україні потребує детального зіставлення з моделями "тотальної оборони» та «всеосяжної безпеки", які де-факто стали стандартом для країн НАТО, що межують із агресором. На відміну від української моделі, де координація часто зводиться до бюрократичного листування, досвід Фінляндії та Естонії демонструє життєздатність горизонтальних екосистем.

Модель Фінляндії: Комітет безпеки та концепція "Society-Wide Resilience"

Фінська модель базується на функціонуванні Комітету безпеки (Turvallisuuskomitea), який, попри зовнішню схожість із апаратом РНБО, має принципово іншу операційну природу. Згідно з фінською Стратегією безпеки суспільства (Yhteiskunnan turvallisuusstrategia), безпека не є прерогативою силових відомств, а розподіленою відповідальністю між державними органами, бізнесом та неурядовими організаціями [3; 8].

Ключова відмінність від українських реалій полягає у функціонуванні Національного оперативного центру (НОЦ), який у режимі 24/7 інтегрує дані від цивільних операторів інфраструктури та розвідки. В Україні ж, як зазначалося раніше, дані розвідки (ГУР МО, СЗРУ) часто "застрягають" на рівні вищого політичного керівництва, не потрапляючи до кінцевих розпорядників критичних об'єктів [4]. Фінський досвід доводить: ефективність предиктивного аналізу залежить від довіри, де приватний сектор є не об'єктом контролю, а повноправним учасником обміну розвідданими про загрози.

Естонський досвід: Центри передового досвіду та цифрова інтегрованість

Естонія, яка пережила першу масштабну гібридну атаку ще у 2007 році, вибудувала одну з найбільш адаптивних систем кіберзахисту у світі. Особливого значення набуває діяльність Об'єднаного центру передового досвіду з кібероборони НАТО (CCDCOE) у Таллінні. Проте для нашого аналізу важливішим є внутрішній естонський протокол взаємодії в межах Кабінету безпеки.

Згідно зі звітом ENISA 2025, Естонія реалізувала принцип "цифрової безшовності" в управлінні інцидентами [6]. Коли виникає гібридна загроза (наприклад, GPS-спуфінг у Балтійському морі, зафіксований у 2024–2025 рр.), реакція відбувається не через скликання комісій, а через автоматизовану платформу обміну інформацією між Департаментом інформаційних систем (RIA) та силами Кайтселійту (Союзу оборони). В Україні ж аналогічні процеси вимагають узгоджень між Держспецзв'язку, СБУ та профільними міністерствами, що створює той самий "часовий лаг", який агресор успішно експлуатує [10].

Адаптація протоколів НАТО 2026: від реакції до превенції

Оновлені протоколи НАТО, ухвалені на початку 2026 року, запроваджують концепцію Preventive-Response Options (PROs), яка передбачає активацію контрзаходів ще до того, як гібридна атака спричинить фізичні руйнування [3]. Це вимагає такого рівня атрибуції загроз, який наразі в Україні технічно розпорошений.

Порівняльний аналіз висвітлює ключову системну помилку української моделі: ми намагаємося регулювати безпеку через збільшення кількості стратегічних документів (понад 330 одиниць [10]), тоді як країни НАТО йдуть шляхом спрощення процедур та створення спільних ситуаційних центрів. Як підкреслюють аналітики RAND у 2025 році, українська система досі функціонує за принципом "потрібно знати" (need to know), що обмежує доступ до інформації, тоді як сучасні виклики вимагають принципу "потрібно поділитися" (need to share) [4].

Звичайно інтеграція західного досвіду в українські реалії не може бути механічним копіюванням. Вона вимагає подолання "культурного розриву" всередині СБО і переходу від закритої відомчої ієрархії до відкритої, але захищеної мережі взаємодії. Це порівняння слугує остаточним аргументом на користь створення Об'єднаного аналітичного центру

гібридних загроз (ОАЦГЗ), який має стати українською відповіддю на мережеві виклики, трансформуючи наш унікальний бойовий досвід у сучасну інституційну форму.

Синергія між суб'єктами СБО та приватним сектором як чинник стійкості

Досвід останніх років показує, що забезпечення національної стійкості в умовах тотальної гібридизації конфліктів 2025–2026 років неможливе без радикального переосмислення ролі приватного сектору. Традиційна модель, де держава є монопольним гарантом безпеки, остаточно вичерпала себе, оскільки понад 80 % об'єктів критичної інфраструктури (енергетика, телекомунікації, хмарні сервіси) перебувають поза межами прямого державного управління. Як зазначають аналітики RAND у роботі "From policy to victory" (2025), ключем до переваги є не нарощування власних потужностей держави, а її здатність до швидкої інтеграції з комерційними технологічними гігантами [4].

В українському контексті створення реальної синергії блокується застарілою регуляторною логікою. Відповідно до статті 12 Закону "Про національну безпеку" сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки [7]. Чинна Стратегія кібербезпеки 2021 року [9] розглядають приватний сектор переважно як об'єкт для перевірок або надання обов'язкових до виконання вказівок. Проте дані ENISA Threat Landscape 2025 свідчать, що швидкість ідентифікації нових загроз у приватному секторі на 40–60 % вища, ніж у державних структурах, завдяки використанню глобальних масивів даних [6].

Справжня синергія вимагає переходу до моделі Data Sharing Agreements (угод про спільне використання даних), що вже є нормою в оновлених протоколах НАТО 2026 року [3]. Це передбачає створення безпечного інформаційного периметра, де розвідувальні індикатори компрометації (IoC) від ГУР МО чи СБУ автоматично синхронізуються з системами захисту приватних провайдерів без бюрократичних погоджень. Більше того, досвід відсічі кібер-фізичним атакам 2025 року підкреслює необхідність залучення приватних груп швидкого реагування до державних планів кризисного менеджменту.

Однак, як демонструє аналіз Пайє П., створення такої екосистеми в Україні впирається у проблему довіри та відсутність юридичних гарантій захисту комерційної таємниці при взаємодії з силовиками [4]. Без внесення змін до законодавства, які б легалізували статус приватних технологічних компаній як суб'єктів забезпечення безпеки з відповідним рівнем доступу до даних, синергія залишатиметься на рівні декларативного волонтерства. У 2026 році такий розрив є не просто організаційним дефектом, а прямою загрозою національній стійкості, оскільки ворог атакує найбільш вразливу, тобто найменш інтегровану ланку системи. Для подолання цієї диспропорції необхідно впроваджувати механізми горизонтальної координації, де держава виступає не як контролер, а як модератор спільних зусиль [10].

Подолання цього розриву неможлива без експертної ревізії нормативно-правового поля, яке станом на 2026 рік залишається занадто консервативним. Автори пропонують розглянути можливість внесення змін до ключових законів для офіційного закріплення мережевої моделі управління в законодавстві.

1. Зміни до Закону "Про розвідку" [10]:

Критичним є перегляд механізмів передачі розвідувальної інформації. Наразі цей Закон (ст. 1) обмежує коло споживачів розвідінформації передусім вищими посадовими особами держави. Для ефективності ОАЦГЗ необхідно легалізувати передачу деперсоніфікованих технічних даних (threat intelligence) безпосередньо технічним підрозділам суб'єктів критичної інфраструктури. Це дозволить реалізувати концепцію "розвідки для захисту", а не лише для інформування "визначених Президентом України інших складових сектору безпеки і оборони України".

2. Реформа Стратегії кібербезпеки України [9]:

Потрібен перехід від “захисту периметра” до моделі Активної оборони (Active Defense). Це передбачає внесення правок, що дозволяють визначеним суб’єктам СБО проводити превентивні операції з нейтралізації інфраструктури агресора (С2-серверів) за межами національного сегменту мережі. Як зазначається у рекомендаціях RAND Corporation (2025), пасивний захист у 2026 році є апріорі програшним [4].

3. Впровадження інституту “Цифрового офіцера зв’язку” на стратегічних приватних компаніях:

Законодавче закріплення присутності представників Служби безпеки України та Держспецзв’язку у визначених стратегічних приватних компаніях. Це не контроль, а створення прямого каналу зв’язку, що відповідає практиці Фінляндії та Естонії. Звичайно впровадження інституту “Цифрового офіцера зв’язку” вимагає чіткого визначення критеріїв, за якими такі компанії обираються. Необхідно встановити, зокрема, критерії стратегічної значущості для національної безпеки, належність до критичних секторів інфраструктури (енергетика, транспорт, телекомунікації тощо), масштаб їхнього впливу на оборонно-промисловий комплекс тощо. Також доцільно встановити механізм періодичного перегляду переліку таких компаній з урахуванням змін у ризиковому ландшафті та стратегічних пріоритетах держави.

Ця правова трансформація має супроводжуватися скасуванням або суттєвим спрощенням застарілих відомчих інструкцій, які не повною мірою відповідають характеру сучасних гібридних (допорогових) загроз.

Пропонована архітектура моделі управління: перехід до мережецентричності

Для подолання виявленої структурної диспропорції між динамікою гібридних загроз і чинною вертикальною моделлю управління сектором безпеки і оборони України пропонується здійснити фундаментальну трансформацію. Центральним елементом трансформації може стати Об’єднаний аналітичний центр гібридних загроз (ОАЦГЗ) – компактний високошвидкісний хаб, підпорядкований безпосередньо РНБО. Штатна чисельність на етапі пілоту – 55-65 фахівців.

Структура центру включає три блоки:

– Групу прогнозного моніторингу (AI-аналіз відкритих джерел, розвідданих і логів приватних операторів);

– Групу юридично-атрибуційної оцінки (підготовка доказової бази);

– Інтерфейс державно-приватної взаємодії (автоматизований обмін IoC через Data Sharing Agreements).

Пілотний запуск рекомендується здійснити на початку 2027 року на обмеженій групі об’єктів (енергетика, зв’язок, транспорт).

Результати пілоту протягом року дозволять прийняти обґрунтоване рішення щодо масштабування моделі.

Повномасштабна реалізація цієї архітектури вимагатиме внесення відповідних змін до Закону “Про національну безпеку України” [7], Закону “Про Державну службу спеціального зв’язку та захисту інформації”. Крім того, Стратегія кібербезпеки має бути доповнена протоколами Active Defense (активної оборони), які б дозволяли визначеним суб’єктам СБО нейтралізувати загрози в зародку, а не лише фіксувати збитки [9].

Висновки

Проведений аналіз підтверджує існування фундаментального розриву між швидкістю еволюції гібридних (допорогових) загроз і консервативною вертикальною моделлю управління сектором безпеки і оборони України. Ця диспропорція закладена в чинному законодавстві та проявляється в хронічній затримці між отриманням розвідданих і оперативними діями.

На думку авторів статті, косметична модернізація існуючих органів уже недостатня. Структурним рішенням є створення Об'єднаного аналітичного центру гібридних загроз як оперативного інтегратора. Його пілотний запуск у 2027 році на обмеженій групі об'єктів дозволить перевірити ефективність моделі в реальних умовах.

Автори не претендують на істину в останній інстанції. Запропоновані положення мають характер попередньої наукової гіпотези. Деякі висновки можуть сприйматися як загальні, що пояснюється обмеженим доступом до закритої інформації. Окремі твердження потребують подальшої верифікації та критичного обговорення.

Водночас автори вважають, що порушені проблеми управління сектором безпеки і оборони в умовах гібридних (допрогових) загроз є надто важливими, щоб залишатися лише предметом внутрішньовідомчих дискусій. Стаття спрямована на ініціювання відкритого наукового діалогу та внесок у спільний пошук ефективних інституційних рішень. Автори з повагою ставляться до будь-яких конструктивних зауважень і критики з боку наукової спільноти та читачів і розглядають їх як необхідний етап удосконалення запропонованих ідей.

Список використаних джерел

1. Center for Strategic and International Studies (CSIS). Russian Sabotage Operations in Europe: Data Analysis and Strategic Implications. CSIS Special Report. March 18, 2025.
2. ENISA Threat Landscape 2025: From Cyber Espionage to Physical Sabotage. *European Union Agency for Cybersecurity (ENISA).* URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
3. Countering Hybrid Threats: Updated Protocols on Horizontal Coordination and Resilience. *North Atlantic Treaty Organization (NATO).* 2026. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm.
4. Paillé P. others. From Policy to Victory: Recommendations to Ukraine for Harnessing Defence Technology. *RAND Europe.* 2025.
5. Microsoft Digital Defense Report 2024: The Evolution of Hybrid Conflicts. *Microsoft.* Microsoft Security Response Center. 2024.
6. Google Cloud / Mandiant. APT44: 2024 Retrospective. A Close Look at Sandworm's Evolving Cyber-Physical Tactics. 2024.
7. Wang H., Zakheim B. China's Lessons from the Russia-Ukraine War: Perceived New Strategic Opportunities and an Emerging Model of Hybrid Warfare. RAND Corporation, 2025.
8. The Finnish Security and Defence Committee. The Strategy for Society's Resilience: Comprehensive Security Model. Helsinki, Ministry of Defence, 2024.
9. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
10. Про розвідку : Закон України від 17 вересня 2020 року № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20.
11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року : Указ Президента України № 392/2020 "Про Стратегію національної безпеки України".
12. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року : Указ Президента України № 121/2021 "Про Стратегію воєнної безпеки України".
13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року : Указ Президента України № 447/2021 "Про Стратегію кібербезпеки України".
14. Про затвердження плану заходів щодо синхронізації стратегічного планування у сфері національної безпеки : Розпорядження Кабінету Міністрів України від 15 серпня 2025 року № 853-р.
15. Danylyuk O. Total Diffusion: The New Reality of Hybrid Aggression against Democratic Institutions. London: Royal United Services Institute (RUSI), 2024.
16. Lysenko S., Marukhovskyi O., Krap A., Illiuschenko S., Pochapska O. The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War. *Studies in Media and Communication.* 2023. № 11 (7). P. 150–158. URL: https://redfame.com/journal/index.php/smc/article/view/6414; https://doi.org/10.11114/smc.v11i7.6414.
17. NATO Strategic Communications Centre of Excellence. The Collage of the Kremlin's Communication Strategy. Riga: NATO StratCom COE, 2025.
18. World Economic Forum. Global Cybersecurity Outlook 2025 (In collaboration with Accenture). Geneva: WEF, 2025.

19. Commonwealth Parliamentary Association & Organization of American States. Parliamentary Handbook on Disinformation, AI and Synthetic Media. London/Washington, D.C., 2023.
20. Swanström N., Logan T. J. G7 Strategy for Countering Russian Information Operations in the Indo-Pacific Region: A Framework for Enhanced Multilateral Coordination and Response. *Institute for Security & Development Policy*. 2025. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.isdp.eu/wp-content/uploads/2025/06/Policy-Brief-FIMI.pdf.
21. European Union & North Atlantic Treaty Organization. Tenth progress report on the implementation of the common set of proposals (June 2024 – May 2025). Brussels. 2025.
22. Юськів Б., Карпчук Н., Пелех О. Зміни стратегічних комунікацій України в час російсько-української війни (2022–2024 рр.). *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2024. № 3 (20). С. 99-112. URL: https://doi.org/10.29038/2524-2679-2024-03-99-112.
23. Сальнікова О., Сівоха І., Іващенко А. Стратегічні комунікації в сучасних війнах гібридного типу. *Social Development & Security*. 2019. № 9 (5). С. 133–142. URL: http://doi.org/10.33445/sds.2019.9.5.9.

References

1. Center for Strategic and International Studies (CSIS). (2025). Russian Sabotage Operations in Europe: Data Analysis and Strategic Implications. CSIS Special Report. March 18, 2025.
2. European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025: From Cyber Espionage to Physical Sabotage. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
3. North Atlantic Treaty Organization (NATO). (2026). Countering Hybrid Threats: Updated Protocols on Horizontal Coordination and Resilience. Retrieved from: https://www.nato.int/cps/en/natohq/topics_156338.htm.
4. Paillé, P., & others. (2025). From Policy to Victory: Recommendations to Ukraine for Harnessing Defence Technology. RAND Europe.
5. Microsoft. (2024). Microsoft Digital Defense Report 2024: The Evolution of Hybrid Conflicts. Microsoft Security Response Center.
6. Google Cloud / Mandiant. (2024). APT44: 2024 Retrospective. A Close Look at Sandworm's Evolving Cyber-Physical Tactics.
7. Wang, H., & Zakheim, B. (2025). China's Lessons from the Russia-Ukraine War: Perceived New Strategic Opportunities and an Emerging Model of Hybrid Warfare. RAND Corporation.
8. The Finnish Security and Defence Committee. (2024). The Strategy for Society's Resilience: Comprehensive Security Model. Helsinki, Ministry of Defence.
9. Zakon Ukrainy. (2018). Pro natsionalnu bezpeku Ukrainy [On national security of Ukraine] (No. 2469-VIII). Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19 [in Ukrainian].
10. Zakon Ukrainy. (2020). Pro rozvidku [On intelligence] (No. 912-IX). Retrieved from: https://zakon.rada.gov.ua/laws/show/912-20 [in Ukrainian].
11. President of Ukraine. (2020). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine"] (Decree No. 392/2020) [in Ukrainian].
12. President of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku "Pro Stratehiiu voiennoi bezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine of March 25, 2021 "On the Military Security Strategy of Ukraine"] (Decree No. 121/2021) [in Ukrainian].
13. President of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"] (Decree No. 447/2021) [in Ukrainian].
14. Kabinet Ministriv Ukrainy. (2025). Pro zatverdzhennia planu zakhodiv shchodo synkhronizatsii stratehichnoho planuvannia u sferi natsionalnoi bezpeky [On approval of the action plan for the synchronization of strategic planning in the field of national security] (Order No. 853-r) [in Ukrainian].
15. Danylyuk, O. (2024). Total Diffusion: The New Reality of Hybrid Aggression against Democratic Institutions. London: Royal United Services Institute (RUSI).
16. Lysenko, S., Marukhovskyi, O., Krap, A., Illiuschenko, S., & Pochapska, O. (2023). The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War. *Studies in Media and Communication,* 11 (7), 150–158. Retrieved from: https://redfame.com/journal/index.php/smc/article/view/6414; https://doi.org/10.11114/smc.v11i7.6414.

17. NATO Strategic Communications Centre of Excellence. (2025). The Collage of the Kremlin's Communication Strategy. Riga: NATO StratCom COE.
18. World Economic Forum. (2025). Global Cybersecurity Outlook 2025 (In collaboration with Accenture). Geneva: WEF.
19. Commonwealth Parliamentary Association & Organization of American States. (2023). Parliamentary Handbook on Disinformation, AI and Synthetic Media. London/Washington, D.C.
20. Swanström, N., & Logan, T. J. (2025). G7 Strategy for Countering Russian Information Operations in the Indo-Pacific Region: A Framework for Enhanced Multilateral Coordination and Response. *Institute for Security & Development Policy*. Retrieved from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.isdp.eu/wp-content/uploads/2025/06/Policy-Brief-FIMI.pdf.
21. European Union & North Atlantic Treaty Organization. (2025). Tenth progress report on the implementation of the common set of proposals (June 2024 – May 2025). Brussels.
22. Yuskiv, B., Karpchuk, N., & Pelekh, O. (2024). Zminy stratehichnykh komunikatsii Ukrainy v chas rosiisko-ukrainskoi viiny (2022–2024 rr.) [Changes in Ukraine's strategic communications during the Russian-Ukrainian war (2022–2024)]. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii*, 3 (20), 99-112. Retrieved from: https://doi.org/10.29038/2524-2679-2024-03-99-112 [in Ukrainian].
23. Salnikova, O., Sivokha, I., & Ivashchenko, A. (2019). Stratehichni komunikatsii v suchasnykh viinakh hibrydnoho typu [Strategic Communications in Modern Hybrid Wars]. *Social Development & Security*, 9 (5), 133–142. Retrieved from: http://doi.org/10.33445/sds.2019.9.5.9 [in Ukrainian].