ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ

https://doi.org/10.26565/1992-2337-2025-2-14
УДК 351.86:004

Дзюндзюк Вячеслав Борисович,
доктор наук з державного управління, професор,
завідувач кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: vbdzun@gmail.com https://orcid.org/0000-0003-0622-2600

Удовенко Олександр Валерійович,
кандидат юридичних наук, полковник ЗСУ,
командир частини, Сухопутні війська України,
майдан Свободи, 4, м. Харків, 61022, Україна
https://orcid.org/0009-0004-7845-0455

ПУБЛІЧНЕ УПРАВЛІННЯ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ІНСТИТУЦІЙНІ МЕХАНІЗМИ ТА ЦИФРОВІ ІНСТРУМЕНТИ

Анотація. У статті здійснено поглиблений науковий аналіз інституційних механізмів та цифрових інструментів публічного управління в умовах гібридної війни як принципово нового феномену сучасних геополітичних протистоянь, що кидає безпрецедентний виклик усталеним парадигмам державного управління, національної безпеки та міжнародної стабільності. Обґрунтовано, що гібридна агресія як стратегічна модель поведінки держав-ревізіоністів принципово трансформує ландшафт загроз, розмиваючи традиційні розмежування між станом війни та миром, між комбатантами та цивільним населенням, між внутрішніми та зовнішніми загрозами, між фізичним та інформаційним просторами ведення бойових дій, що вимагає відповідної трансформації не лише безпекових структур, а й усієї архітектури публічного управління.

Як цитувати: Дзюндзюк В. Б., Удовенко О. В. Публічне управління в умовах гібридної війни: інституційні механізми та цифрові інструменти. *Державне будівництво.* 2025. № 2 (38). С. 228–238. https://doi.org/10.26565/1992-2337-2025-2-14

In cites: Dziundziuk, V.B., Udovenko, O.V. (2025). Public governance under conditions of hybrid warfare: institutional mechanisms and digital tools. *State Formation, no. 2 (38), 228–238.* https://doi.org/10.26565/1992-2337-2025-2-14 [in Ukrainian].

На основі компаративного аналізу інституційних рішень провідних демократій – Сполучених Штатів, Великої Британії, Фінляндії, Естонії та країн ЄС – систематизовано організаційні форми та функціональні моделі спеціалізованих структур координації протидії гібридним загрозам, визначено конфігурацію їхніх мандатів, ресурсного забезпечення та механізмів взаємодії. Розкрито сутнісні характеристики принципу whole-of-government як концептуального фундаменту ефективного публічного управління в умовах гібридних конфліктів, що передбачає горизонтальну інтеграцію безпекових, оборонних, розвідувальних, правоохоронних та цивільних структур в єдину когерентну систему виявлення та нейтралізації загроз. Досліджено роль цифрових технологій – систем аналізу великих даних, технологій штучного інтелекту, платформ раннього попередження, інструментів атрибуції кібератак – у якісному розширенні спроможностей держави протистояти дезінформаційним кампаніям, кіберагресії та операціям гібридного впливу. Проаналізовано правові рамки регулювання дій держави у кіберпросторі та інформаційному середовищі з урахуванням необхідності балансування між ефективністю реагування та дотриманням принципів верховенства права. Висвітлено механізми залучення приватного сектору та інститутів громадянського суспільства до системи протидії гібридним загрозам через публічно-приватні партнерства та спільні платформи обміну розвідувальними даними. Узагальнено унікальний досвід України у формуванні адаптивної інституційної архітектури публічного управління в умовах повномасштабної збройної агресії та визначено перспективні напрями вдосконалення системи протидії гібридним загрозам.

Ключові слова: гібридна війна, публічне управління, національна безпека, інституційні механізми, інформаційні технології цифровізація, цифрові інструменти, кібербезпека, інформаційна безпека, інформаційні технології резильєнтність.

Постановка проблеми. Гібридна війна як стратегічний феномен постбіполярної геополітики здійснює принципову трансформацію самого поняття збройного конфлікту, руйнуючи усталені категоріальні розмежування між станом війни та миром, між комбатантами та цивільним населенням, між внутрішніми соціальними процесами та зовнішнім деструктивним впливом, між оборонними та безпековими секторами публічного управління. На відміну від класичних збройних зіткнень з чітко визначеними фронтами та ідентифікованими ворожими силами, гібридна агресія конструюється на стратегічній логіці навмисної амбівалентності, заперечуваності та поступової ескалації, що дозволяє агресору досягати стратегічних цілей, уникаючи формального визнання стану збройного конфлікту та супровідних правових і дипломатичних наслідків. Координоване застосування регулярних і нерегулярних збройних формувань, кібератак, масштабних дезінформаційних кампаній, економічного примусу та підтримки проксі-сил утворює синергетичну систему дестабілізаційного тиску, що руйнує суспільну згуртованість і підриває довіру до державних інституцій без перетинання юридично значущого порогу відкритої агресії.

Традиційні інститути публічного управління, сформовані відповідно до логіки класичного розподілу функцій між відомствами в умовах мирного часу, виявляються структурно неадаптованими до ефективного реагування на гібридні загрози. Відомча фрагментація генерує системні розриви у спроможності держави виявляти та нейтралізувати скоординовані багатовимірні атаки. Бюрократичні ієрархії перетворюються на джерело неефективної повільності в умо-

вах динамічних загроз, що вимагають швидких міжвідомчих рішень, тоді як інформаційні силоси перешкоджають формуванню комплексної розвідувальної картини, необхідної для антиципаторного управління.

Цифрові технології виступають водночас ключовим об'єктом гібридних атак та принципово новим інструментом протидії їм. Зростаюча залежність критичної інфраструктури від цифрових платформ управління генерує нові вектори атак для гібридних агресорів, здатних каскадно руйнувати взаємопов'язані системи. Натомість аналітика великих даних, штучний інтелект і блокчейн кардинально розширюють спроможності розвідки, кіберзахисту та інформаційної протидії. При цьому проблема формування ефективних інституційних механізмів набуває особливої гостроти для України, яка, перебуваючи в епіцентрі найбільш масштабної гібридної агресії сучасності, накопичила унікальний досвід інституційної адаптації та розробки цифрових інструментів протидії в умовах жорстких ресурсних обмежень.

Аналіз останніх досліджень і публікацій. Концептуалізація гібридної війни як самостійного теоретичного конструкту сягає фундаментальних досліджень Гофмана [6], який визначив гібридні загрози як синтез конвенційних та нерегулярних засобів збройної боротьби, терористичних тактик і кримінальних елементів в єдиний оперативний концепт. Відповідні доктринальні документи НАТО та ЄС концептуалізують гібридні загрози як широкий адаптивний комплекс засобів, що застосовуються гнучко та з максимальним ступенем заперечуваності [13]. Разом з тим семантична гнучкість поняття «гібридна війна» породжує концептуальні двозначності, що ускладнюють формування чітких критеріїв ідентифікації та атрибуції гібридної агресії в конкретних емпіричних контекстах.

Інституційний вимір протидії систематично аналізується у роботах Ренза та Сміта [13], які обґрунтовують необхідність координації на рівні всього уряду. Ланошка [10] досліджує логіку поступової ескалації у механізмах російської гібридної агресії. Фонтейн [4] розробляє теорію технологічного енактменту; Мергел, Едельманн та Хауг [11] пропонують концептуальне визначення цифрової трансформації, що виходить за межі технологічного редукціонізму; Клієвінк, Бароса та Тан [9] визначають передумови ефективного функціонування публічно-приватних інформаційних платформ.

У той же час, аналіз наукової літератури виявляє лакуну: відсутність досліджень, які органічно інтегрують інституційні механізми та цифрові інструменти в єдину аналітичну рамку, орієнтовану на специфіку гібридних конфліктів.

Мета статті полягає у визначенні інституційних механізмів і цифрових інструментів публічного управління в умовах гібридної війни через компаративне дослідження міжнародного досвіду та обґрунтування науково-практичних рекомендацій щодо вдосконалення інституційної архітектури з урахуванням українського досвіду та кращих міжнародних практик резильєнтного врядування.

Застосована методологія і методи. Методологічну основу дослідження утворює міждисциплінарний синтез системного, інституційного та конструктивістського підходів, що дозволяє аналізувати публічне управління в умовах гібри-

дної війни як складну адаптивну систему. Компаративний аналіз проведено на матеріалі досвіду США, Великої Британії, Фінляндії, Естонії та провідних інституцій ЄС; відбір кейсів ґрунтується на варіації за рівнем зрілості інституційних систем та характером специфічних загроз безпековому середовищу. Метод кейс-дослідження застосовано для аналізу українського досвіду, що характеризується максимальною інтенсивністю загроз та мінімальними часовими горизонтами для реагування. Емпіричну базу складають стратегічні документи безпекового сектору, звіти міжнародних організацій та статистика кіберінцидентів.

Виклад основного матеріалу. Фундаментальна структурна проблема публічного управління в умовах гібридної агресії полягає у принциповій несумісності між мережевим характером загроз та вертикальною організацією державного апарату. Гібридна агресія конструюється саме так, щоб ця несумісність працювала на агресора: спецслужби бачать стратегічні наміри, але не мають інструментів дії у цивільному просторі; органи кібербезпеки фіксують технічні індикатори атак, але позбавлені розвідувальних даних для атрибуції; правоохоронці можуть переслідувати виконавців, але не мають позатериторіальних повноважень. Кожне відомство бачить частину картини. Жодне не бачить її цілком.

Відповіддю на цей виклик став принцип whole-of-government, що передбачає горизонтальну інтеграцію всіх інституційних спроможностей в єдину систему виявлення та нейтралізації загроз [4]. Слід підкреслити, що це не міжвідомча координація у звичному сенсі, тобто погодження вже прийнятих рішень. Це реконфігурація самих інформаційних потоків до моменту прийняття рішень. Різниця є принциповою.

Практичні реалізації цього принципу демонструють, що форма інституційного втілення має не менше значення, ніж сам принцип. Зокрема, США у 2018 році заснували CISA і розмістили її не в структурі профільного міністерства, а безпосередньо під Міністерством внутрішньої безпеки [2]. Це рішення, яке виглядає суто адміністративним, насправді є стратегічним: агентство з міжвідомчою місією не може бути підпорядковане одному з відомств, між якими воно покликане координувати. Велика Британія зробила аналогічний вибір, підпорядкувавши Команду з безпекових комунікацій безпосередньо Кабінету міністрів.

Фінська модель іде далі за обидві названі. Принцип whole-of-society інтегрує у систему захисту громадянське суспільство, медіа та освітні установи, охоплюючи 23 функції критичної важливості, розподілені між міністерствами та приватним сектором [3]. Показово, що не криза породила таку систему, а десятиліття свідомого будівництва. І саме тому вона функціонує ефективно.

Архітектура ЄС вирішує інше завдання, а саме завдання масштабу. Hybrid CoE у Гельсінкі, об’єднуючи понад 30 держав-учасниць, займається стратегічними дослідженнями та нарощуванням спроможностей, тоді як Гібридний центр злиття ЄС орієнтований на оперативний аналіз у реальному часі [13]. Поділ між стратегічним і оперативним рівнями є тут не адміністративною формальністю, а принциповим організаційним рішенням: структура, що думає про наступне десятиліття, не може водночас ефективно реагувати на атаку, яка відбувається прямо зараз.

Від архітектурних рішень слід перейти до змісту того, чим ці структури мають займатися. І тут варто зафіксувати тезу, що нерідко губиться у дискусії про безпеку: гібридна агресія атакує насамперед не інфраструктуру, а свідомість. Мета полягає не в тому, щоб зруйнувати електростанцію, а в тому, щоб зруйнувати довіру до уряду, який її захищає [12]. Дезінформаційний наратив, успішно посіявши сумнів, не потребує підтримки, оскільки самовідтворюється через соціальні мережі та поляризоване медіасередовище. Реактивна модель спростувань програє за самою своєю логікою: вона надає наративу увагу, не знищуючи його коріння. Ефективна відповідь передбачає заповнення когнітивного простору до того, як туди проникне дезінформація, а не після. East StratCom Task Force ЄС рухається у цьому напрямку, однак залишається хронічно недофінансованим порівняно з ресурсами агресора. Це не деталь, а структурна проблема: виробництво дезінформації є суттєво дешевшим за протидію їй, і жодна технологія цю асиметрію не усуне.

З проблемою комунікацій нерозривно пов'язана атрибуція. Агресор, чия стратегія побудована на заперечуваності, найбільше втрачає саме тоді, коли його називають на ім'я, причому публічно, авторитетно та коаліційно [11]. Координована атрибуція NotPetya у 2018 році, де США, Велика Британія та союзники одночасно назвали відповідальних, стала прецедентом не технічним, а передусім політичним [1]. Показово також, що персоніфікація, тобто атрибуція до рівня конкретних офіцерів ГРУ, додає до репутаційного тиску особистий вимір: виконавці операцій починають усвідомлювати, що анонімність не є гарантованою.

Цифрові інструменти змінюють не кількість доступної інформації, а саму природу того, що можна побачити. Системи аналізу великих даних виявляють координовані дезінформаційні кампанії через аномалії у патернах поширення контенту, які принципово невидимі для людини, оскільки існують лише на рівні мільйонів одночасних взаємодій [8]. Алгоритми машинного навчання знаходять кореляції між подіями, що здаються непов'язаними, саме ті патерни, які аналітик пропускає під тиском кризового перевантаження [14]. Разом з тим тут важливо зупинитися на застереженні: алгоритм не приймає рішень, він готує матеріал для рішень. Людське судження у стратегічних питаннях є незамінним, а технологія лише підвищує його якість.

Системи раннього попередження реалізують логіку, що здається самоочевидною: виявити загрозу до атаки значно ефективніше, ніж реагувати після неї [5]. Однак практична складність полягає у відокремленні реального сигналу від шуму в умовах безперервного потоку даних. Ефективна система вирішує це через мультиджерельність: якщо сигнал підтверджується незалежно з відкритих цифрових просторів, технічної розвідки, дипломатичних каналів і фінансового моніторингу одночасно, ймовірність хибного спрацьовування різко знижується. Системи кризового управління, інтегровані з такими платформами, автоматично активують протоколи реагування, мінімізуючи часовий розрив між виявленням загрози і першими скоординованими діями [9].

Нормативно-правова рамка публічного управління стикається у контексті гібридної агресії з проблемою, що не має прецеденту у традиційному праві:

вона мусить регулювати явища, свідомо сконструйовані так, щоб не вписуватися у жодну наявну правову категорію [15]. Традиційні системи, побудовані на бінарному розрізненні між миром і збройним конфліктом, погано пристосовані до кібератак, дезінформаційних кампаній та економічного примусу, оскільки ці явища завдають реальної стратегічної шкоди, але не відповідають юридичним визначенням агресії. Варто підкреслити, що ця нормативна прогалина є не технічним недоліком правових систем, а свідомо використовуваним агресором ресурсом: залишаючись у «сірій зоні», гібридна агресія дозволяє уникати правових наслідків відкритого збройного нападу.

Регламент DORA 2022 року є показовим зразком нормативного реагування на цей виклик. Він встановлює вимоги до кіберрезилієнтності широкого кола фінансових установ, поширюючи безпекові стандарти на малих учасників ринку, чиї вразливості можуть слугувати точками входу до великих взаємопов'язаних систем. Принципово важливою є логіка цього рішення: не пряме регулювання загроз, а підвищення стійкості всієї системи через усунення її найслабших ланок. Директива про критичні суб'єкти відображає аналогічну еволюцію регуляторного мислення, а саме перехід від реактивного підходу до проактивного, від реагування на збої до проектування стійкості як вихідного принципу.

Залучення приватного сектору є структурно необхідним елементом системи, і причина цього є цілком прагматичною: переважна частина критичної інфраструктури та цифрових екосистем перебуває у приватній власності [9]. Компанії у сфері кібербезпеки, телекомунікацій та фінансового сектору мають перший доступ до операційних даних для виявлення аномалій гібридних атак, тоді як державні структури отримують цю інформацію із запізненням, коли вона вже частково втрачає оперативне значення. Структурний конфлікт інтересів при цьому є очевидним: держава потребує оперативних даних, тоді як компанії побоюються репутаційних збитків від розкриття власних вразливостей і можливого використання цих даних у регуляторних провадженнях. Спільні центри обміну та аналізу інформації (ISACs) вирішують цю суперечність через обмежений обмін з гарантіями конфіденційності та правовим захистом. Однак технічна платформа є лише необхідною умовою ефективної співпраці. Фундаментальним залишається формування культури взаємної довіри між секторами, що будується роками регулярної взаємодії та руйнується значно швидше, ніж будується.

У цьому контексті медіаграмотність та критичне мислення громадян набувають значення стратегічної інвестиції у суспільну резилієнтність, рентабельність якої вимірюється не роками, а десятиліттями [7]. Фінська модель, де медіаграмотність інтегрована в освітню програму від початкових класів, демонструє принциповий висновок: когнітивний імунітет до дезінформації значно ефективніше формується до повного занурення громадян у цифровий простір, ніж коригується після того, як некритичний спосіб споживання інформації вже став звичкою. Естонський досвід після кібератак 2007 року, що охоплював відкриття дублікатів урядових систем у цифрових посольствах за кордоном, посилення інфраструктури цифрової ідентичності X-Road та системне проведення

кіберчинь для різних категорій населення, демонструє здатність невеликої держави трансформуватися у глобального лідера кіберзахисту [3]. Ключовий урок полягає не у переліку конкретних технічних рішень, а у логіці системного підходу, що охоплює технологічний, організаційний, правовий та освітній виміри одночасно.

Захист критичної інфраструктури є першорядним завданням з огляду на фундаментальну властивість сучасних складних технічних систем, а саме системну взаємозалежність, де аварія однієї підсистеми автоматично генерує каскадні збої у суміжних [3]. Тут важливо зафіксувати суперечність, що не має простого вирішення: ефективна система є, як правило, мінімально надлишковою, тоді як стійка система потребує надлишковості як структурного принципу. Це фундаментальна напруга між операційною ефективністю та безпекою, яку неможливо усунути технічними засобами без управлінських рішень, готових свідомо жертвувати першою заради другої. Атака NotPetya у 2017 році завдала глобальних збитків понад десять мільярдів доларів, переконливо продемонструвавши транскордонний деструктивний потенціал кібератак без жодного фізичного військового компонента [1]. Концепція кіберрезилієнтності має, відповідно, передбачати не лише превентивний захист, а й спроможність швидкого відновлення функціональності через резервні системи та процедури ручного управління критичними процесами.

Захист виборчих процесів від гібридних атак є пріоритетним завданням з принципової причини: підрив довіри до виборів є стратегічною, а не інструментальною метою гібридної агресії [12]. Метою є не спотворення конкретних результатів, а руйнування самого принципу легітимного представницького управління. Досвід задокументованого втручання у вибори США 2016 року, де операції торкнулися реєстраційних систем виборців у двадцяти одному штаті, демонструє: ефект досягається не через технічне маніпулювання підрахунком голосів, а через поглиблення поляризації та підрив суспільної довіри до самого виборчого процесу. Президентські вибори в Румунії 2024 року, де Конституційний суд анулював результати першого туру на підставі доказів іноземного втручання, стали першим юридичним прецедентом, що підтвердив: гібридне втручання може набувати масштабів, достатніх для правового скасування результатів голосування.

Штучний інтелект трансформує ландшафт гібридних конфліктів симетрично і двосторонньо, що унеможливлює просту оптимістичну оцінку [1]. Технології генеративного ШІ якісно розширюють можливості дезінформаційних операцій: масштабне виробництво deepfake-відео та синтетичних текстів підвищує переконливість кампаній при зниженні їх вартості, посилюючи вже наявну асиметрію між витратами на виробництво дезінформації та витратами на протидію їй. Ті самі алгоритми дозволяють автоматизувати моніторинг загроз, однак гонка між атакуючим та захисним застосуванням ШІ не є симетричною: витрати на захист систематично перевищують витрати на атаку. Регуляторні рамки у безпековому секторі мають вирішити принципову дилему між операти-

вністю реагування та підзвітністю, з огляду на те, що автоматизовані системи прийняття рішень у критичних контекстах потребують механізмів нагляду, здатних виявляти та виправляти помилки до їх незворотних наслідків [15].

Міжнародне співробітництво набуває структурно необхідного характеру, оскільки гібридна агресія є принципово транскордонним явищем і свідомо спрямована на розколювання альянсів [10]. НАТО здійснило значний прогрес через заснування Центру передового досвіду з кооперативного кіберзахисту у Таллінні, розробку Таллінського посібника та рішення 2019 року про те, що кібератака відповідного масштабу може активувати Статтю 5, принципово важливого саме своєю прецедентністю. Скоординована атрибуція та узгоджені санкційні відповіді є найефективнішим інструментарієм колективного накладення витрат на агресора [2]. Реальна ефективність колективного стримування залишається дискусійною з огляду на складність верифікації зобов'язань та різні оцінки загроз серед союзників, однак наявні дані свідчать: навіть часткова коаліційна атрибуція є значно ефективнішою стримуючою мірою, ніж найрішучіша одностороння реакція.

Досвід України у побудові системи публічного управління, здатної функціонувати в умовах повномасштабної збройної агресії, поєднаної з масованими кібератаками і дезінформаційними операціями, являє собою унікальний природний експеримент, що не має аналогів у сучасній демократичній практиці [12]. Унікальність полягає не лише в безпрецедентній інтенсивності загроз, а й у тому, що Україна мусила здійснювати інституційну адаптацію в режимі реального часу, без можливості завершити реформи до гострої фази конфлікту та без права на системні помилки.

Серед принципових особливостей українського досвіду передусім слід відзначити системну інтеграцію волонтерських ініціатив та IT-сектору в офіційні структури. IT Army of Ukraine та OSINT-спільноти функціонують у гібридному просторі між громадянським суспільством і державою без чіткого правового статусу, але з реальним оперативним значенням. Це явище не вкладається у жодну з існуючих теоретичних моделей публічно-приватного партнерства і потребує окремої концептуалізації. Показовою є також оперативна розробка цифрових інструментів, від додатку «Дія» як платформи мобільного урядування до систем верифікації розвідувальних даних, в умовах жорстких ресурсних обмежень. Це демонструє, що обмеження можуть стимулювати інноваційність, а не лише гальмувати розвиток. Нарешті, збереження функціональності ключових органів управління навіть під масованими ракетними ударами є практичним підтвердженням цінності принципів кіберрезилієнтності, що розроблялися переважно у теоретичних контекстах.

Водночас аналіз виявляє системні обмеження, осмислення яких є не меншою науковою цінністю, ніж позитивні уроки. Надмірна централізація окремих функцій ставить під загрозу принципи децентралізації: децентралізована система при ураженні центрального вузла є значно стійкішою. Дефіцит кваліфікованих кадрів, загострений мобілізацією, обмежує нарощування цифрових спро-

можностей у момент найвищого попиту на них. Культура ситуативного реагування, що є природним наслідком необхідності вирішувати невідкладні проблеми тут і зараз, ризикує витіснити системне стратегічне планування, без якого неможливе довгострокове інституційне будівництво.

Висновки і перспективи подальших досліджень. Здійснений системний аналіз переконливо демонструє, що публічне управління в умовах гібридної війни вимагає фундаментальної трансформації інституційної архітектури, що виходить за межі часткового реформування і передбачає перегляд базових принципів організації публічного управління, механізмів міжвідомчої координації та підходів до залучення позадержавних акторів. Ключовим концептуальним фундаментом є принцип whole-of-government, що передбачає системну горизонтальну інтеграцію різнорідних інституційних спроможностей і подолання відомчого партикуляризму. Резилієнтність інституцій як динамічна здатність до адаптації та відновлення функціональності виступає другим ключовим принципом, що вимагає проектування систем управління з урахуванням неминучості збоїв та їх наслідків.

Цифрові інструменти, серед яких системи аналізу великих даних, технології штучного інтелекту, платформи автоматизованого моніторингу та системи раннього попередження, являють собою потужні, але не самодостатні засоби підвищення ефективності. Їхній реальний внесок залежить від якості інституційної рамки, наявності кваліфікованих кадрів та нормативного регулювання, що забезпечує підзвітність і захист прав громадян. Правова рамка потребує систематичної розробки для усунення нормативних прогалин у «сірій зоні» гібридної агресії при збереженні принципів верховенства права.

Узагальнення результатів дослідження дозволяє сформулювати висновок, що публічне управління в умовах гібридної війни не може бути зведене ані до суто безпекової проблематики, ані до питань цифрової трансформації окремо – воно вимагає їх органічного синтезу в єдиній інституційній логіці. Компаративний аналіз свідчить: найбільш резилієнтними виявляються не ті системи, що мають найдосконаліші технології, а ті, що досягли узгодженості між інституційною архітектурою, нормативною базою, кадровим потенціалом і суспільною готовністю. Саме ця узгодженість є тим, що неможливо імпортувати або впровадити швидко – і саме її відсутність є найбільш поширеною причиною інституційних провалів у відповідь на гібридні загрози.

Перспективи подальших досліджень охоплюють розробку методологічно строгих підходів до емпіричної оцінки ефективності моделей міжвідомчої координації, аналіз впливу технологій штучного інтелекту на системи раннього попередження з урахуванням швидкої еволюції атакуючих і захисних застосувань, дослідження умов ефективного залучення громадянського суспільства до систем резилієнтності, а також розробку системи індикаторів оцінки інституційної готовності держави до протидії гібридним загрозам. Систематизація унікального українського досвіду публічного управління в умовах гібридної та відкритої агресії залишається найбільш нагальним завданням для дослідників у цій сфері,

здатним збагатити як практику відновлення державних інституцій України, так і глобальне знання про механізми резилієнтного демократичного врядування.

Конфлікт інтересів.
Автори заявляють, що конфлікту інтересів щодо публікації цього рукопису немає.

Стаття надійшла до редакції 28.08.2025 р.
Стаття рекомендована до друку 03.10.2025 р.

Dziundziuk V. B.,
Doctor of Science in Public Administration, Full Professor,
Head the Public Policy Department,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: vbdzun@gmail.com https://orcid.org/0000-0003-0622-2600

Udovenko O. V.,
Candidate of Science in Law, Colonel of the Armed Forces of Ukraine,
Unit Commander, Land Forces of Ukraine
https://orcid.org/0009-0004-7845-0455

PUBLIC GOVERNANCE UNDER CONDITIONS OF HYBRID WARFARE: INSTITUTIONAL MECHANISMS AND DIGITAL TOOLS

Abstract. The article presents an in-depth scientific analysis of institutional mechanisms and digital tools for public governance under hybrid warfare conditions as a fundamentally novel phenomenon of contemporary geopolitical confrontations, posing unprecedented challenges to established paradigms of state administration, national security, and international stability. The study substantiates that hybrid aggression as a strategic behavioral model of revisionist states fundamentally transforms the threat landscape by blurring traditional distinctions between war and peace, combatants and civilians, domestic and external threats, physical and informational battlespaces – thus demanding a corresponding transformation not only of security structures but of the entire architecture of public governance. Through comparative analysis of institutional solutions adopted by leading democracies – the United States, Great Britain, Finland, Estonia, and EU institutions – the article systematizes the organizational forms and functional models of specialized structures for coordinating responses to hybrid threats, defining the configuration of their mandates, resource provisioning, and interaction mechanisms. The essential characteristics of the whole-of-government principle are revealed as the conceptual foundation of effective public governance under hybrid conflicts, encompassing horizontal integration of security, defense, intelligence, law enforcement, and civilian structures into a single coherent system of threat detection and neutralization. The role of digital technologies in qualitatively expanding state capacity to withstand disinformation campaigns, cyber aggression, and hybrid influence operations is investigated. The legal frameworks for regulating state actions in cyberspace and the information environment are analyzed in light of the necessity to balance response effectiveness with adherence to the rule of law. Mechanisms for engaging the private sector and civil society institutions in the hybrid threat response system through public-private partnerships and shared intelligence exchange platforms are highlighted. Ukraine's unique experience in forming an adaptive institutional architecture for public governance under conditions of full-scale armed aggression is summarized, and prospective directions for improving the system of countering hybrid threats are identified.

Keywords: hybrid warfare, public administration, national security, institutional mechanisms, information technology digitalization, digital tools, cybersecurity, information security, information technology resilience.

REFERENCES

1. Buchanan, B. (2020). The AI Triad and What It Means for National Security Strategy. Washington: Center for Security and Emerging Technology.
2. Coaffee, J., & Lee, P. (2016). Urban resilience: Planning for risk, crisis and uncertainty. London: Palgrave Macmillan.
3. Dunn Cavelty, M. (2018). Cybersecurity in Switzerland. Zurich: Springer International Publishing.
4. Fountain, J.E. (2001). Building the virtual state: Information technology and institutional change. Washington: Brookings Institution Press.
5. Gil-Garcia, J.R., Dawes, S. ., & Pardo, T.A. (2018). Digital government and public management research: Finding the crossroads. *Public Management Review*, 20(5), 633–646. https://doi.org/10.1080/14719037.2017.1327181
6. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies.
7. Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. https://doi.org/https://doi.org/10.1016/j.giq.2015.07.001
8. Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly*, 33(3), 371–377. https://doi.org/10.1016/j.giq.2016.08.011
9. Klievink, B., Bharosa, N., & Tan, Y. H. (2016). The collaborative realization of public values and business goals: Governance and infrastructure of public–private information platforms. *Government Information Quarterly*, 33(1), 67–79. https://doi.org/10.1016/j.giq.2015.12.002
10. Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*, 92(1), 175–195. https://doi.org/10.1111/1468-2346.12509
11. Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. https://doi.org/10.1016/j.giq.2019.06.002
12. Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Washington: Brookings Institution.
13. Renz, B., & Smith, H. (2016). Russia and hybrid warfare: Going beyond the label. Helsinki: Aleksanteri Institute.
14. Shim, J.P., Warkentin, M., Courtney, J.F., Power, D.J., Sharda, R., & Carlsson, C. (2002). Past, present, and future of decision support technology. *Decision Support Systems*, 33(2), 111–126.
15. Veale, M., Van Kleek, M., & Binns, R. (2018). Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making. *In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–14).

Conflict of interest.
The authors declare that there is no conflict of interest regarding the publication of this manuscript.

The article was received by the editors 28.08.2025.
The article is recommended for printing 03.10.2025.
Published 30.12.2025.