Ефективність державного управління
Efficiency of public administration
https://doi.org/10.36930/508602
Article received: 12.09.2025, Article accepted: 05.12.2025
Article published: 28.01.2026
УДК 351.86:327:004.056:35.07
Correspondence author: V. O. Tkach Tkach.Vsevolod@nltu.lviv.ua
ISSN 2070-4011 (print)
ISSN 2786-6580 (online)

В. О. Ткач
Національний лісотехнічний університет України, м. Львів, Україна

ГЛОБАЛЬНЕ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ: ІНСТИТУЦІЇ УПРАВЛІННЯ ТА АДАПТАЦІЯ ДО СУЧАСНИХ ВИКЛИКІВ

Часті кіберінциденти, зафіксовані впродовж останніх років, чітко демонструють, що питання кібербезпеки зайняли важливе місце в міжнародному порядку денному. Декілька міжнародних організацій висунули ініціативи в галузі управління кіберпростором, зокрема, Організація Об'єднаних Націй та Європейський Союз. ООН та ЄС прагнуть відігравати провідну роль у сфері політики щодо забезпечення стійкості перед кіберзагрозами. Проте ці ініціативи досі не забезпечили створення належних регулятивних норм. У статті розглянуто фактори, що ускладнюють розвиток нормотворчості у кіберпросторі та управління кібербезпекою у міжнародному вимірі. Виявлено ключові тенденції розвитку глобального управління кібербезпекою, серед яких домінування неформальних інструментів співробітництва, поширення норм "відповідальної поведінки" держав у кіберпросторі та зростання ролі приватного сектору й громадянського суспільства у формуванні міжнародних стандартів. Встановлено, що ефективність наявних міжнародних інструментів стримування кіберзагроз залишається обмеженою через суперечності між державними інтересами, складність процедур атрибуції кібератак та високий рівень геополітичної конкуренції. З'ясовано, що розвиток нової моделі глобального управління кібербезпекою має ґрунтуватися на поєднанні державоцентричних та багатостейкхолдерних підходів, що відповідають принципам нового мультилатералізму. Також показано, що сьогоднішня тенденція полягає у спробах вирішення глобальних проблем кібербезпеки відповідно до наявних норм і в рамках вже створених структур міжнародного права, тоді як кіберпростір побудований на фундаментально інших законах і, отже, потребує створення нових правових норм та структур. Сучасні норми міжнародного права та забезпечення міжнародної безпеки, безумовно, можна застосовувати для забезпечення кібербезпеки, але ті з них, які не співвідносяться з унікальною природою відносин у кіберпросторі, потрібно замінити новими інструментами, побудованими на парадигмі нової багатосторонності (нового мультилатералізму), що передбачає активну участь недержавних акторів у побудові глобального ландшафту та екосистеми кібербезпеки, при напрямному, балансуючому та оптимізуючому впливі державних ("*nation-states*") суб'єктів.

Ключові слова: кібербезпека; кіберзагрози; недержавні актори (стейкхолдери); глобальний ландшафт кібербезпеки; публічне управління; глобальне управління; безпекові виклики для України.

Вступ

У XXI ст. розвиток суспільства, держави, права на всій планеті відбувається під впливом процесів цифрової трансформації, в основу яких покладено інформаційно-комунікаційні технології та створювані завдяки ним інформаційні мережі, системи, бази даних тощо. Світ вступив у цифрову епоху. Водночас, зміни у світі, породжувані цифровізацією, не завжди мають сприятливий характер. Нові можливості та переваги, породжувані широкомасштабним впровадженням цифрових технологій у всі сфери суспільних відносин, супроводжуються появою нових видів небезпек та злочинних посягань ("кібератаки", "кіберзагрози"), які фактично перетворилися на нову глобальну проблему для всього людства. Зокрема, штучний інтелект (ШІ) швидко перетворюється на серйозну, багатогранну загрозу глобальній безпеці, діючи як прискорювач наявних ризиків, так і "творець" абсолютно нових, складних, а іноді й автономних небезпек. Оскільки ШІ досягає можливостей експертного рівня, він змінює ландшафт загроз, даючи змогу здійснювати складніші, масштабніші атаки, одночасно знижуючи бар'єри для зловмисників [7].

Сьогодні можна з упевненістю стверджувати, що забезпечення кібербезпеки (і, в ширшому контексті, інформаційної безпеки) є одним із найгостріших викликів, на які державам доведеться відповідати, діючи як індивідуально, так і спільно – у межах міжнародних організацій та інтеграційних об'єднань. Однак через складність та тривалість узгодження позицій держав на глобальному рівні (зокрема, в межах ООН) їхнє міжнародне співробітництво та інтеграція у сфері спільного забезпечення кібербезпеки наразі розвивається не надто успішно. Хоча деякі регіональні ініціативи (зокрема, зусилля Європейского Союзу зі створення регуляторного ландшафту безпеки, а також співпраця країн Альянсу "П'ять очей" (англ. *Five Eyes Alliance* (FVEY)) у сфері кібербезпеки для протидії загрозам зі сторони деяких держав, зокрема Китаю та Росії, а також для захисту критичної інфраструктури) продемонстрували певну

Ткач Всеволод Олегович, здобувач програми доктора філософії, кафедра публічного управління та адміністрування.
Email: Tkach.Vsevolod@nltu.lviv.ua; https://orcid.org/0009-0001-6582-0064

Цитування за ДСТУ: Ткач В. О. Глобальне управління кібербезпекою: інституції управління та адаптація до сучасних викликів. *Ефективність державного управління* : зб. наук. пр. Вип. 1(86). Львів: НЛТУ України, 2026. С. 17–27.
Citation APA: Tkach, V. O. (2026). Global cybersecurity governance: institutions and adaptation to modern challenges. *Efficiency of public administration, 1*(86), 17–27. https://doi.org/10.36930/508602

результативність, відсутність чітких глобальних параметрів управління кібербезпекою знижує їхню ефективність. Окрім того, більшість ініціатив у сфері кібербезпеки мають реактивний, а не проактивний характер і відстають за темпами розвитку від стрімкої еволюції новітніх кіберзагроз.

Водночас, у сучасному експертному та політичному дискурсах про майбутній світопорядок головний акцент, зазвичай, робиться на процесі дифузії сили в міжнародній системі, що відбувається на наших очах [25]. Основні дискусії розгорнулися навколо того, в якій саме конфігурації може бути досягнуто сталої рівноваги міжнародної системи. Різні варіанти взаємодії центрів сили у майбутній системі неминуче визначатимуть рівень стійкості світопорядку. Слабокерований світ в епоху ресурсних дефіцитів, стрімких змін клімату, безпрецедентних транскордонних міграційних потоків та безконтрольного розвитку нових технологій не може бути стабільним упродовж тривалого часу.

Без принципової зміни характеру відносин між усіма чи навіть між основними гравцями множення числа полюсів неминуче означає множення числа ризиків безпеки. Умовою відновлення загального світового порядку та запобігання некерованості та хаосу за умов збільшення числа активних учасників міжнародної взаємодії є випереджальне підвищення щільності сучасної мережі міжнародних угод, режимів та організацій [25]. Ця мережа створює нормативно-правову базу, інструменти контролю та горизонтальні зв'язки, що перешкоджають провалюванню світової політики в архаїку.

Тому в аналізі майбутніх моделей світового порядку, поряд із поняттями багатополярності та поліцентризму, важливо звернутися до поняття багатосторонності. Якщо багатополярність констатує наявність плюралізму у розподілі сили у міжнародній системі, де є три чи більше самостійних центрів прийняття рішень, то багатосторонність описує можливий варіант взаємодії цих центрів.

Феномен "нового мультилатералізму" – це реформований, інклюзивний та орієнтований на дії підхід до міжнародної співпраці, розроблений для вирішення криз XXI ст., таких як зміна клімату, нерівність та технологічні зміни. На відміну від традиційних, державоцентричних моделей, він наголошує на різноманітних партнерствах, що охоплюють громадянське суспільство, приватний сектор та регіональні організації, зосереджуючись на практичних, відчутних рішеннях.

Оскільки цифрові технології змінюють глобальну владу, правила, що їх регулюють, дедалі частіше обговорюють на багатосторонніх форумах. Але якщо ці органи прагнуть створити легітимні та перспективні рамки управління для Інтернету, штучного інтелекту, кібербезпеки та даних, їхні процеси повинні адаптуватися – розширюючи участь, охоплюючи ширше коло учасників, чий досвід є незамінним.

Однак занадто часто багатосторонність та участь великої кількості стейкхолдерів розглядають як конкуруючі моделі легітимності: держави проти зацікавлених сторін. Насправді ці два поняття можуть і повинні доповнювати одне одного. Доцільно розглядати це через два шляхи інтеграції:

1) Відкриття, що керується державою (вертикальна інтеграція), де погляди зацікавлених сторін враховуються урядом – через національні консультації, дорадчі органи або включення до офіційних делегацій. Це робить відкритість частиною цифрової зовнішньої політики країни.
2) Інституційне відкриття (горизонтальна інтеграція), у якому зацікавлені сторони незалежно взаємодіють із багатосторонніми інститутами через структуровані канали участі, створені самими інститутами.

Обидва напрями вже існують практично, але застосовуються нерівномірно. Пошук способів побудови нового, ефективного і гнучкого середовища багатостороннього співробітництва для протидії загрозам кібербезпеки, що виникають, є вкрай актуальним науковим завданням.

Методи дослідження. Дослідження базується на інструментарії інтегративного огляду з використанням інструменту оцінки змішаних методів (MMAT). Підхід інструментарію MMAT представлено на рис. 1. Етапи дослідницького процесу наведено в табл. 1.

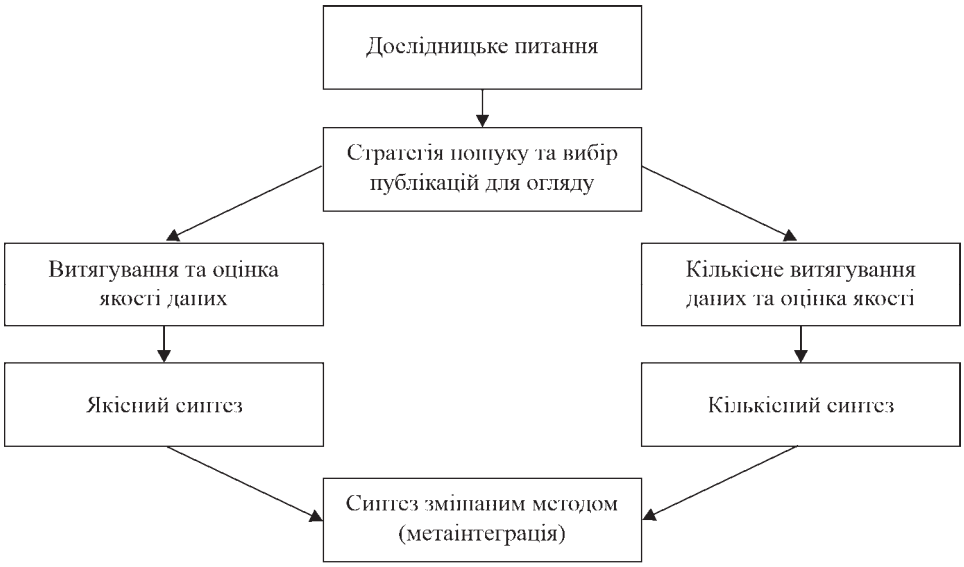

Рис. 1. Концептуальна діаграма MMAT для потреб цього дослідження

Джерело: авторська розробка.

Табл. 1. Хід дослідження: презентація процесів

Етап	Зміст етапу
Пошук літератури	Визначення баз даних для пошуку (MDPI, ScienceDirect, JSTOR, Springer, ResearchGate) та пошукові терміни. Узагальнена вибірка для подальшого скринінгу (137 елементів). Ключові слова для пошуку (англійською та українською мовами): *новий мультилатералізм, міжнародне співробітництво в сфері кібербезпеки, глобальне управління в сфері кібербезпеки, недержавні суб'єкти глобальної кібербезпеки.*
Аналіз даних	Системний, порівняльний, історико-генетичний та функціональний методи.
Оцінка даних	Застосування фреймворку MMAT. Формування фінальної вибірки для проведення інтегративного огляду (40 елементів).
Презентація результатів	Формування тематичних розділів огляду відповідно до результатів аналізу даних.

Джерело: авторська розробка.

Методологічний апарат дослідження, застосований після завершення процедури формування вибірки, базувався на інтеграції системного, порівняльного, історико-генетичного та функціонального методів, що забезпечує комплексне вивчення глобального управління кібербезпекою.

Аналіз літературних джерел. Ще у 2015 р. V. Greiman [10], щоб краще зрозуміти проблеми розроблення єдиної системи глобального кіберуправління, провів порівняльний аналіз національних стратегій та структур кібербезпеки у 10 країнах та Європейському Союзі з різних регіонів як розвинених, так і країн, що розвиваються. На основі емпіричних досліджень та аналізу національних і міжнародних стратегій і політик кібербезпеки, у його статті досліджувалися проблеми та переваги створення глобальної правової та політичної бази для кібердіяльності, яка б сприяла досягненню цілей національної розвідки та технологічних інновацій, одночасно підвищуючи довіру та покращуючи правову визначеність на світовому електронному ринку.

Висновки S. Sundari та ін. [27] показують, що відсутність співпраці між країнами та низький рівень розуміння громадськістю політики захисту даних, (такої як Закон про захист даних в Індонезії, як наведено у прикладі в статті), є основними перешкодами у створенні ефективної системи безпеки даних. У дослідженні пропонують комплексний метод, який поєднує правові, технологічні та політичні елементи для вирішення питань безпеки даних загалом та конкретних питань, пов'язаних з екологічними даними. Спираючись на передовий досвід, такий як лідерство Малайзії в кібербезпеці, S. Sundari та ін. [27] пропонують практичні рекомендації для підтримки безпечної та сталої глобальної цифрової екосистеми.

M. Vandendriessche [31] висвітлює дуже неоднорідний, динамічний та фрагментований ландшафт, для якого часто характерне поєднання різноманітних, гібридних інституцій. Її робота аналізує складний, багатосторонній характер цієї сфери, підкреслюючи, що управління кібербезпекою частково визначається "ознакою неоднорідності".

M. Raymond та J. Sherman [18] вказують на ще одну ключову проблемну сферу. Вони стверджують, що хоча багатосторонність вважається конститутивною рисою сучасного ліберального міжнародного порядку та асоціюється з ліберальними цінностями, протягом двадцяти п'яти років авторитарні держави виступали за розширення багатосторонніх методів управління питаннями кібербезпеки, тоді як великі консолідовані демократії часто виступали проти них.

C. Cai та R. Zhang [5] попереджають про проблему фрагментації глобального управління кібербезпекою. Вони стверджують, що за останні роки особливо помітним стало протиріччя між необхідністю спільного глобального управління кібербезпекою та фрагментацією системи управління кібербезпекою. Виходячи з припущення, що міжнародна кібербезпека є квазісуспільним благом, у цій статті зроблено спробу проаналізувати фрагментацію управління кібербезпекою та її причини з погляду постачання та споживання продуктів кібербезпеки, спираючись на теорії про квазісуспільні блага та використовуючи порівняльний аналіз і тематичні дослідження.

M. Natorski [15] досліджує, як міжнародний мультилатералізм стосується питання появи універсальної технології штучного інтелекту. Детальніше автор аналізує дві ключові особливості ШІ-мультилатералізму: його узагальнені принципи та координацію державних відносин у сфері ШІ. По-перше, у статті розрізняються узагальнені принципи багатостороннього підходу до ІІ: епохальні зміни, детермінізм та діалектичне розуміння. По-друге, адаптація багатостороннього підходу до ШІ призвела до інтеграції питань ШІ до порядку денного наявних рамок співробітництва та створення нових спеціальних рамок, орієнтованих виключно на питання ШІ. В обох випадках багатосторонній підхід до ШІ розвивається "в тіні" державної ієрархії у взаєминах з іншими стейкхолдерами у сфері ШІ. Автор наголошує, що, хоча мультилатералізм ШІ є багатостороннім, а ієрархія між державними та недержавними суб'єктами може здаватися розмитою, держави зберігають компетенцію як вирішальні особи, що приймають рішення у визначенні порядку денного, переговорах та виконанні міжнародних зобов'язань щодо "м'якого права".

Штучний інтелект став темою численних міжнародних ініціатив у рамках сучасних міжнародних організацій та інституціоналізації нових структур. В академічних роботах ці міжнародні ініціативи розглядають в рамках широкого поняття (глобального) управління; однак, воно не завжди чітко концептуалізується з самого початку. Відповідно до підходу глобального управління, дослідники запропонували різні категорії для відображення швидкозмінного ландшафту глобального управління ШІ. Наприклад, J. Butcher та I. Beridze [4] надали огляд ранніх ініціатив. Вони вирізнили їх за різними рівнями залучення приватного сектору, державного сектору, неурядових організацій, дослідницьких установ, багатосторонніх організацій та ООН. L. Schmitt [23] класифікував нові ініціативи щодо управління ШІ на основі розмежування між ініціативами в рамках наявних структур управління та новостворюваними структурами, специфічними для ШІ, а також лідерством, що виходить від держав та інших (недержавних) суб'єктів, таких як бюрократія міжнародних організацій або при-

ватні суб'єкти. J. Tallberg та ін. [28] зіставили ініціативи ШІ навколо не взаємовиключних категорій сфери регулювання (горизонтальна проти вертикальної), повноважень (централізовані проти децентралізованих), зобов'язань (м'яке право проти жорсткого права), походження (приватне проти державного) та предмета (військово-безпекові проти невійськових). Нарешті, M. Vaele та ін. [32] виділили такі шість модальностей зобов'язань в області глобального управління ШІ: етичні кодекси та ради (державні та приватні), галузеве самоврядування, контракти та ліцензування, стандарти, міжнародні угоди та екстериторіальні внутрішні правила.

Окрім цих ранніх спроб категоризації емпіричного аналізу, нова архітектура глобального управління ШІ вивчалася переважно з нормативного погляду, із зосередженням на бажаних інституційних рамках. Учені пропонували закріпити основу для дискусій та регулювання щодо ШІ, що відображають різні міжнародні структури, такі як Міжнародна група експертів зі зміни клімату, Міжнародне агентство з атомної енергії або ЦЕРН, щоб створити, наприклад, Міжурядову групу експертів зі ШІ, Міжнародну організацію ШІ, Агентство ООН з контролю за ШІ або Науково-дослідну організацію ООН зі ШІ. M. Maas та J. Villalobos [14] склали карту 47 пропозицій щодо інституцій глобального управління ШІ за сімома вимірами можливих організацій, зосереджуючись на формуванні наукового консенсусу, формуванні політичного консенсусу та нормотворчості, координації політики та регулювання, забезпеченні дотримання стандартів або обмежень, стабілізації та реагуванні на надзвичайні ситуації, міжнародних спільних дослідженнях, а також розподілі переваг та доступу.

Наведені вище приклади картування міжнародних ініціатив у сфері штучного інтелекту вказують на безліч наявних та нових відповідних структур і напрямів для досліджень у рамках широкого концептуального поняття глобального управління. Ця нечітко визначена концепція висвітлює регуляторні процеси, що включають багатьох учасників, розмиваючи межу між державною владою та приватною ініціативою.

Українські науковці В. Ободяк та Є. Котух [17] наголошують, що слабко захищені комп'ютерні мережі певних юрисдикцій, які можуть використати зловмисники, створюють ризик не тільки для їхніх власників, а й для інших мереж. Слабка кібербезпека з цієї перспективи є настільки ж серйозною суспільною проблемою, як викиди вуглекислого газу чи вирубування лісів. Водночас, управління кібербезпекою, на думку авторів, залишається новою та методологічно складною областю досліджень. Через обмежений обсяг емпіричних даних усі висновки наразі мають попередній характер і до них варто підходити з максимальною обережністю. Урахувуючи ці обмеження, автори вважають, що кібербезпека за своїми базовими властивостями меншою мірою сприяє міжнародному співробітництву порівняно з іншими глобальними проблемами. Це, водночас, може загострити різноманітні аспекти співпраці на міжнародному рівні.

Черниш Р. [40] підкреслює, що останнім часом глобальний кіберпростір щоразу об'єктивніше оцінює світова спільнота як один із найважливіших пріоритетів безпеки, оскільки його функціонування є вагомим чинником розвитку економіки, військового, соціального, безпекового та інших секторів. Своєю чергою, С. Стежко та Т. Шевченко [39] розглядають зміст та ключові аспекти Стратегії кібербезпеки США та конкретизують засади спільної діяльності американо-українських відносин у сфері забезпечення кібербезпеки.

Вівчар І. та ін. [37] досліджують кібербезпеку як ключовий компонент міжнародного співробітництва за умов глобальної безпекової кризи. У статті розглядають перетворення кіберзагроз у чинник стратегічної нестабільності, а також акцентують увагу на нагальній потребі створення глобальної системи кібербезпеки. Окремо висвітлено особливості участі України в міжнародних інструментах кібербезпеки, підкреслено потребу в уніфікації нормативних підходів, зміцненні кіберспроможностей та координації дій між державами. Цікаво, що кібербезпеку трактують ці автори як глобальне публічне благо, що потребує багаторівневого управління та політичної солідарності.

Тим часом, як справедливо стверджує Urgessa [30], хоча міжнародна співпраця в галузі кібербезпеки була ускладнена через розбіжні визначення та концептуалізації предмета, які є очевидними в міжнародній системі, проблема переросла в глухий кут, оскільки ця розбіжність ґрунтується на несумісності методів організації політичних систем великих кібердержав у своїх країнах. Отже, стверджується, що роль багатосторонньої системи у досягненні будь-якого значного прогресу в управлінні кібербезпекою є дуже обмеженою.

Дійсно, загальноприйнята думка стверджує, що жодна з головних глобальних викликів XXI ст., чи то зміна клімату, ядерна зброя чи кібербезпека, не може бути належно вирішена без належної міжнародної співпраці. Однак багатостороння співпраця в багатьох проблематичних сферах, включаючи кібербезпеку, перебуває в глухому куті. Водночас, питання ефективності та тим більше проактивності глобального управління кібербезпекою не отримали належної уваги в науковому дискурсі.

Результати дослідження

Багатостороння співпраця в кібер- та інформаційній сферах потрібна як ніколи, особливо тоді, коли геополітичні конфлікти загрожують вийти з-під контролю. Цивільному сектору та збройним силам країн потрібно співпрацювати, щоб узгодити оперативні межі останніх та якнайкраще обмінюватися інформацією та відповідально поводитися в кібер- та інформаційній сферах.

Глобальне управління кібербезпекою охоплює ініціативи ООН (GGE, OEWG), форуми (GFCE) та технічні альянси, спрямовані на створення норм відповідальної поведінки держав у кіберпросторі. Вони об'єднують уряди, бізнес та громадянське суспільство для запобігання конфліктам, обміну досвідом та захисту критичної інфраструктури. Ключові інструменти та пов'язані з ними проблеми та тенденції наведно в табл. 2.

Останніми роками національні держави вирішували проблему кібербезпеки, активно впроваджуючи ініціативи в різних міжурядових організаціях, будь то універсальні організації (такі як Організація Об'єднаних Націй або МСЕ), або регіональні чи закриті організації, такі як Європейський Союз, Рада Європи, ОБСЄ, ОЕСР, Африканський Союз, Шанхайська організація співробітництва, НАТО, АСЕАН, G7 або G20. Ці ініціативи також розробляють в рамках спеціальних структур з кібербезпеки, де держави ініціюють вражаючу кількість

конференцій, таких як Глобальна конференція з кіберпростору (GCCS), яка запустила Глобальний форум з кіберекспертизи (GFCE) – і це не враховуючи академічних ініціатив, таких як процес, що призвів до прийняття Талліннських посібників 1 та 2, або створення аналітичних центрів, таких як Глобальна комісія зі стабільності кіберпростору під головуванням Марини Кальюранд (колишнього міністра закордонних справ Естонії).

Табл. 2. Інструменти забезпечення кібербезпеки

Інструменти та ініціативи у сфері кібербезпеки	
Робоча група відкритого складу (OEWG) ООН:	Діючий інструменти під егідою ООН, що включає всі держави-члени для обговорення безпеки у сфері ІКТ
Група урядових експертів (GGE) ООН:	Розробляє норми відповідальної поведінки держав, рекомендації щодо заходів зміцнення довіри та застосування міжнародного права у кіберпросторі
Глобальний форум з кіберекспертизи (GFCE):	Платформа для міжнародного співробітництва, обміну знаннями та зміцнення потенціалу кібербезпеки, особливо для країн, що розвиваються.
Технічна спільнота та ініціативи:	Координація здійснюється через форуми, такі як ICANN (управління інтернетом) та FIRST (реагування на інциденти).
Проблеми та тенденції	
Фрагментація:	Національно-орієнтовані підходи створюють ризики «клаптевого» управління.
Розбіжності:	Відмінності між країнами у розумінні суверенітету у мережі ускладнюють прийняття обов'язкових конвенцій.
Фокус:	Основна увага приділяється захисту даних, мереж та запобіганню атакам.

Джерело: авторська розробка на основі [5, 39].

Альянс "П'ять очей" також виходить за межі свого безпосереднього членства, вирішуючи ширші проблеми безпеки, що впливають на міжнародну спільноту. Завдяки ранньому попередженню про конфлікти, розвідці про геополітичні ризики та скоординованим реагуванням на шпигунство та кіберзагрози, альянс функціонує як стабілізаційна сила у глобальній безпеці. Невід'ємною частиною стратегії кібербезпеки альянсу є принципи "безпечний за проектуванням" та "безпечний за замовчуванням". Вбудовуючи заходи безпеки у фундаментальну архітектуру систем та забезпечуючи відповідність конфігурацій за замовчуванням суворим стандартам безпеки, ці принципи зменшують вразливості та підвищують системну стійкість. Хоча "П'ять очей" діє як згуртована одиниця, його вплив поширюється на партнерство з державами-союзниками, включаючи Європейський Союз. Спільні ініціативи щодо обміну розвідувальними даними виявилися безцінними під час криз, даючи змогу країнам-союзникам ефективно протидіяти спільним загрозам. Надаючи розвідувальні дані про тероризм, кіберризики та інші транснаціональні виклики, альянс зміцнює глобальні мережі безпеки.

Серед численних платформ для обговорення і переговорів ключову роль відіграла Група урядових експертів ООН з питань розвитку інформації та телекомунікацій у контексті міжнародної безпеки. У складі представників 25 країн ця група підтвердила застосовність міжнародного права до кіберпростору. Її звіт, опублікований у 2015 р., акцентував увагу на впровадженні певних принципів і норм міжнародного права, а також запропонував набір правил для відповідальної поведінки держав. Після публікації звіту та відповідно до наданого мандату група продовжила роботу, спрямовану на деталізацію й удосконалення цих правил, норм і принципів. Міжнародна спільнота з нетерпінням очікувала нового звіту. На жаль, цей звіт так і не було опубліковано. Хоча з важливих питань було досягнуто значного прогресу, з деяких питань (включаючи питання самооборони та застосовності гуманітарного права) виникли розбіжності, і переговори зрештою провалилися. Хоча деякі пропозиції були зроблені з метою "відродження" в майбутньому Загальнодержавної ради ООН (GGE), є вагомі підстави вважати, що це буде важко зробити в короткостроковій перспективі; і навіть якщо це стане можливим, "нова" GGE навряд чи досягне високих результатів [36].

Провал Глобальної групи експертів ООН залишає міжнародне регулювання кіберпростору без централізованого форуму, і це тоді, коли необхідність діяти як ніколи актуальна – про що свідчать, зокрема, перші кібератаки з дійсно глобальним охопленням, такі як Wannacry або NotPetya, та низка недавніх досліджень, що підкреслюють ризики [36]. Хоча провал переговорів з кібербезпеки під егідою GGE ООН створив величезну прогалину в міжнародному регулюванні, нещодавні кібератаки з глобальним охопленням показали, що дії є більш нагальними, ніж будь-коли. Роздуми про стандарти, передові практики та норми мають включати суб'єктів приватного сектору, які часто є першими жертвами кібератак.

A. Sukumar та ін. [26] зазначають, що міжнародний режим кібербезпеки є типовим прикладом зростання неформальності в сучасному глобальному управлінні. Незважаючи на зростання складних кібератак у світі, держави не впроваджують формальну багатосторонню співпрацю для їх запобігання та пом'якшення. Виникає важливе питання: що пояснює перевагу неформального управління в міжнародній кібербезпеці, і чому в цій сфері поширилися необов'язкові угоди щодо "відповідальної поведінки"?

Тінь неформальності значною мірою нависає над сучасним глобальним управлінням. Останніми роками дослідники міжнародних відносин задокументували стійку, але помітну тенденцію до занепаду формальних багатосторонніх організацій та зростання, на їхню заміну, неформальних інституцій та угод у різних сферах глобального управління [20, 34]. Цей поворот до неформальності здебільшого зумовлений бажанням держав зберегти гнучкість щодо своїх багатосторонніх зобов'язань та створювати чи приєднуватися до коаліцій однодумців, членство та порядок денний яких є гнучкими, орієнтованими на конкретні завдання [19] або відкритими. Однак їхній неформальний характер також ускладнює вивчення того, як ці інституції чи угоди розвиваються, і чи вдається їм спонукати держави до дотримання зобов'язань. Підзвітність таких інструментів, деякі з яких можуть мати секретний характер [1], перед

внутрішніми та міжнародними сторонами [3] також є важливою політичною проблемою.

У міжнародній сфері кібербезпеки збереження неформального підходу, ймовірно, можна пояснити опорою держав та недержавних суб'єктів на кращий інструмент неформального управління: норми "відповідальної поведінки".

Хоча ці норми описують Група експертів ООН та інші інститути як "добровільні" чи "необов'язкові", вони тісно пов'язані з міжнародним правом. Кібернорми часто запозичують лексику міжнародного права [6], що означає, що вони є не просто неформальними рекомендаціями, а й інтерпретаціями наявних правил, що застосовуються до поведінки держав у кіберпросторі [12]. Це унікальне та дещо суперечливе формулювання норм не є випадковим. Як держави-однодумці, так і країни, які дотримуються протилежних поглядів, зацікавлені в тому, щоб неформальні норми тісно співвідносилися з формальними принципами. Країни, які дотримуються схожих поглядів, відповідно до своєї позиції про те, що існуючого міжнародного права достатньо для регулювання кібероперацій, зокрема, наполягали на використанні в нормах юридичної термінології. З іншого боку, Китай та деякі інші держави можуть не бути зацікавлені у підтвердженні застосовності чинного законодавства, але використання формальної мови підвищує статус норм та переговорів Групи експертів ООН і надає їм гнучкості для вибіркового застосування певних (сприятливих) правил, які застосовні та адаптовані для управління кібербезпекою.

На рис. 2 представлено концептуальну схему міжнародного режиму кібербезпеки, на якій виділено основних дійових осіб за їхніми ролями та функціями. Два крила режиму взаємодіють із колом "кібердипломатії", яке, водночас, формує дискусії на переговорах ООН. Через дипломатичне коло учасники із зовнішніх крил намагаються забезпечити свої інтереси, залишаючись поза межами формальних дипломатичних переговорів.

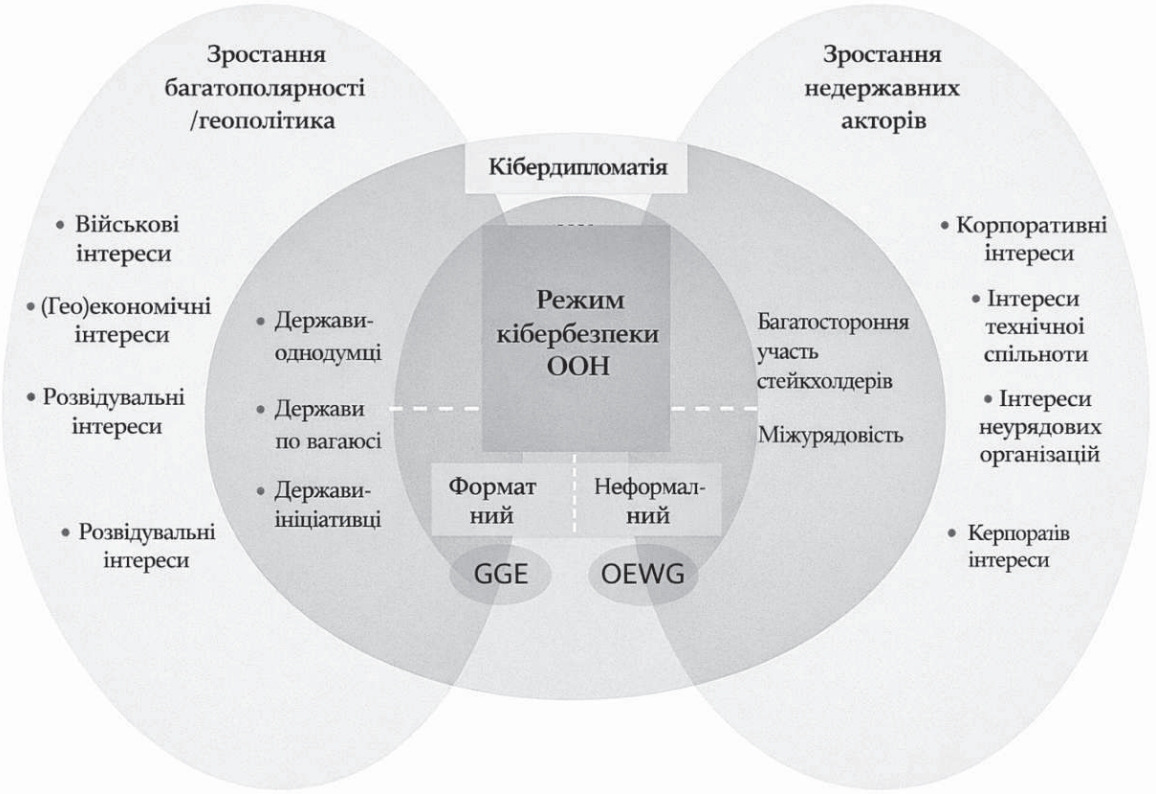

Рис. 2. Міжнародний режим кібербезпеки

Джерело: авторська розробка на основі Sukumar A. та ін. [26].

Важливо відзначити, що приватний сектор зробив свій внесок у міжнародне управління кібербезпекою через свою участь у багатосторонніх та міжурядових кібердипломатичних процесах. У рамках Глобальної групи експертів ООН та Робочої групи відкритого складу, а також у відомих багатосторонніх ініціативах, таких як Глобальна група експертів ООН з кібербезпеки та Паризька робоча група, технологічні компанії, НУО та експерти з кібербезпеки, стали впливовими учасниками діалогу. Глобальна конференція з кіберпростору (GCCS) у Лондоні у 2011 р., яка започаткувала дискусії в рамках "Лондонського процесу" щодо управління кібербезпекою, мабуть, стала першим глобальним багатостороннім форумом, де приватний сектор міг висловити свою думку з питань міжнародної кібербезпеки. Як за змістом порядку денного, так і за часом проведення, GCCS збіглася з роботою першої успішної Глобальної групи експертів ООН (2009–2010 рр.), познайомивши приватний сектор з переговорами ООН з міжнародної кібербезпеки. Найголовніше, GCCS дала приватним суб'єктам сигнал про те, що неформальне управління є шляхом вперед у цій сфері.

Зростання геополітичної напруженості та перехід до багатополярного світу помітно проявилися в кіберпросторі. Той факт, що кіберпростір став новою військовою сферою операцій для багатьох країн [24] та сферою для рутинної розвідувальної діяльності [21], породив скептицизм серед держав-учасниць переговорів ООН щодо справжніх намірів одна одної сприяти впровадженню правил відповідальної кіберповедінки держав. Хоча більшість держав та науковців більше не вважають термін "кібервійна" аналітично корисним, кіберконфлікт

широко визнається невід'ємною частиною сучасного державного управління.

Останніми роками цифрова економіка також стала невід'ємною частиною конкуренції великих держав, особливо між США та Китаєм. Ця геоекономічна напруженість проявляється в політичних та стратегічних рамках, таких як "роз'єднання" та "китайсько-американська технологічна війна" [11], а також в неформальному тиску США на союзників щодо присутності Huawei в ключовій інфраструктурі 5G та неформальній коаліції між США, Японією та Нідерландами з метою обмеження передачі напівпровідникових технологій Китаю. Своєю чергою, через свою програму "Один пояс, один шлях", і особливо напрямки "Цифровий шовковий шлях", Китай розширює свій глобальний вплив у технологічній сфері. Усі ці події впливають на дискусії в ООН та обмежують їх.

Важливим явищем, яке варто згадати, є кібердипломатія – нова сфера, що розвивається, інтегруючи цифрові технології та дипломатичну практику в міжнародні відносини, трансформуючи взаємодію держав у цифровій сфері. Вона відіграє вирішальну роль у вирішенні сучасних викликів кібербезпеці, одночасно сприяючи глобальній стабільності та співпраці. Кібердипломатія передбачає використання дипломатичних інструментів та стратегій для управління міжнародними відносинами у кіберпросторі. Вона охоплює дії держав, спрямовані на забезпечення кібербезпеки, встановлення норм та посилення співпраці з глобальних цифрових питань.

Поляков О. [38] стверджує, що основою кібердипломатії є формат побудови кібердіалогу. Дослідник актуалізує значення кібердипломатії у питаннях запобігання та протидії кіберінцидентам та під час оцінювання ландшафту кіберзагроз.

Однією з ключових сфер тут є штучний інтелект. ШІ не тільки змінює економіку, а й потенційно може змінити військову, розвідувальну та контррозвідувальну сфери. Це перетворює ШІ на предмет міждержавної конкуренції, а також співробітництва з питань, пов'язаних з наслідками його впровадження та створенням рамок для стійкіших та безпечніших моделей впровадження. Georgescu [9] у своїй статті представив огляд питань, пов'язаних з управлінням широким впровадженням та застосуванням технології ШІ, а також деякі зусилля в галузі кібердипломатії, які формують західні та глобальні рамки співробітництва з цього питання. Дослідник наголошує, що кібердипломатія є природним інструментом для координації та колективних дій суверенних суб'єктів, які мають принаймні частково розбіжні інтереси. Дипломатія дає змогу формалізувати обговорення принципів, цінностей, порядку денного та дій і може призвести до зближення точок зору та формування довіри для встановлення обов'язкових рамок та норм управління щодо ШІ.

"Багатосторонній підхід" відрізняється від "міжурядового підходу" як форми дипломатії, але кілька людей відіграли ключові ролі в обох типах форумів. Кібердипломати з різних міністерств закордонних справ, яких вважають "піонерами" Генеральної ради ООН з питань кібербезпеки, та, загалом, міжурядових переговорів з кібербезпеки [2], згодом обійняли впливові посади в аналітичних центрах, що беруть участь у діалогах Треку 1.5, багатосторонніх комісіях та технологічних компаніях. До них належать дипломати з політично впливових держав, таких як США, Естонія, Нідерланди, Данія, Південна Африка, Австралія та Індія. Їхній підхід до поєднання (неформальних) норм та (формальних) правил, можливо, також вплинув на роботу приватних ініціатив. Наприклад, Глобальна комісія з кібербезпеки (GCSC) (2018) встановила детальні процедури консультацій, залучення та взаємодії, щоб забезпечити допомогу міжнародних юристів у розробці та перевірці деяких із дев'яти "добровільних" норм Комісії.

Стандарти кібербезпеки, розроблені приватними суб'єктами, не обмежуються технічними аспектами. Як зазначає Josephine Wolff [35], страхові компанії відіграють "тиху", але впливову роль у формуванні норм кібербезпеки за умов конфліктів. Страховики, такі як Lloyd's, пише Wolff, виключили зі свого страхового покриття кібероперації, які підтримує держава і які проводиться під час війни. Оскільки точність поліса важлива для визначення страхового покриття, Асоціація ринку Lloyd's (LMA) навіть визначила через свої робочі групи, що являє собою "кібероперація", що означає, що така операція "проводиться в рамках війни", і який вплив ці операції повинні мати, щоб бути виключеними зі страхового покриття. Положення LMA також передбачають, що заяви держав про атрибуцію кібероперацій мають враховувати страховики та застраховані організації під час визначення того, що є "підтримуваною державою" діяльністю, і, отже, виключається зі страхового покриття. Ці критерії можуть не бути обов'язковими, як зазначає Wolff, але вони, безумовно, мають серйозні комерційні наслідки. Страхові поліси можуть спонукати держави до розгляду або навіть ухвалення зазначених стандартів для зменшення політичного ризику або відтоку капіталу з їхніх цифрових економік.

Отже, ландшафт багатосторонності в домені глобального управління кібербезпекою є надзвичайно складним та багатовекторним. Водночас, ефективність міжнародних інструментів стримування кіберзагроз є вочевидь недостатніми. Однією з кореневих причин цього, на наш погляд, є системні ефекти, які можуть мати як синергетичну, так і нетропічну спрямованість.

Обговорення отриманих результатів. Кібератаки за останнє десятиліття стали поширенішими та масштабнішими. Хоча значна частина цих атак припадає на кіберзлочини, скоєні злочинцями і привертає більшу частину уваги світу, державні структури також стали важливими гравцями та несуть відповідальність за істотні порушення кібербезпеки завдяки спонсорству, ресурсам, можливостям та рівню знань, якими володіють лише вони. Багато держав визнали цю стратегічну загрозу, але розроблення ефективних інструментів стримування є надзвичайно важким завданням, з огляду на складність імплементації будь-яких норм чи паттернів відповідальності, а також зіткнення різновекторних (а іноді й діаметрально протилежних) інтересів держав та недержавних акторів.

Ранні дискусії про потребу інтеграції кіберпростору з ширшими концепціями та теоріями міжнародних відносин почали переміщуватися з периферії до ядра дисципліни [8]. Водночас, дослідження в цій галузі можна розділити на кілька ключових напрямків. Один напрямок зосереджений на проблемах встановлення гегемонії для просування стратегій великих держав у кіберпросторі. Другий напрямок літератури зосереджений на складності режимів, щоб описати проблеми регулюван-

ня Інтернету, що виникають, серед іншого, через безліч залучених суб'єктів, різних типів правил, інститутів, що перетинаються, і різноманітності регульованих питань. Третій напрямок літератури зосереджений на ролі, яку відіграють міжнародні актори у встановленні та формуванні кібер-норм. Однак, як справедливо пояснює Джозеф С. Най, норми є компонентом режимів, тоді як управління Інтернетом – це набір слабо пов'язаних норм та інституцій з фрагментованою практикою і без "ядра, що ідентифікується" [16].

Основою міжнародного права є державний суверенітет, який, однак, важко вписується в реальність кіберпростору [33]. Незважаючи на досягнутий консенсус щодо реалізації державного суверенітету в кіберпросторі, за що треба подякувати Групі експертів ООН, жодна з наявних держав не може претендувати на суверенітет, який охоплював би весь кіберпростір [22]. Так відбувається тому, що багато елементів інфраструктури, на базі яких існує кіберпростір, знаходяться в межах різних суверенних територій [22] і, отже, згідно з міжнародним правом, належать до різних юрисдикцій. Тим не менш J. Trachtman [29] справедливо зазначає, що поділ юрисдикцій не має бути підставою для відмови від регулювання всього кіберпростору: зрештою, дії в кіберпросторі все одно здійснюються на конкретній території, як і їх наслідки відчуваються в конкретній області. Той факт, що окремі проблеми виходять за межі конкретних юрисдикцій, не є чимось новим для міжнародного права (згадаймо, наприклад, міжнародне морське право, відкритий космос, зміну клімату). Основні проблеми пов'язані з юридичною атрибуцією: часто нелегко визначити, хто відповідальний, звідки виходить кібератака чи грає роль посередника. Саме атрибуція становить найбільші труднощі. Навіть наявні норми кіберправа можуть втратити свою ефективність, зіткнувшись із проблемою атрибутування.

Іншим ключовим фактором, що ускладнює взаємовідносини між кібербезпекою та міжнародним правом, є проблема сумісності ролей держави та приватного сектору у кіберпросторі. Роль держави, як арбітра, кіберпростору є предметом запеклих дискусій. З одного боку, можна стверджувати, що національні держави зобов'язані встановлювати правові рамки, що обмежують або в інший спосіб спрямовують діяльність приватних компаній у кіберпросторі. У цьому випадку аргументом "за" є перелік обов'язків держав відповідно до норм міжнародного права: захист прав людини, підтримка міжнародного миру та безпеки, дотримання принципу "не зашкодь", захист критичної інфраструктури тощо. Дані зобов'язання можуть бути дотримані в кіберпросторі лише за умови, якщо відповідні права та обов'язки покладаються і на недержавних акторів [13].

З іншого боку, існують аргументи проти широкої участі держав у регулюванні кіберпростору: (i) для приватного сектору не існує серйозних стимулів для співпраці з державними інстанціями, оскільки останні можуть перешкодити реалізації комерційних інтересів перших (репутаційні збитки, пряма дія з боку конкурентів за допомогою створюваних технологій); (ii) заходи контролю уповільнюють інноваційний розвиток [33].

Альтернативним рішенням може стати регулювання кіберпростору на базі юридично обов'язкових (або таких, що не є такими) норм корпоративної етики, які будуть вироблені безпосередньо працюючими в кіберпросторі недержавними інститутами, що й спостерігається сьогодні в масштабі "нового мультилатералізму". Однак, як було описано вище, участь недержавних акторів переслідує все ж таки саме свої власні інтереси. Тому роль держав як суб'єктів нового мультилатералізму в управлінні глобальною кібербезпекою має бути спрямована насамперед на впорядкування та синергізацію мотивації та зусиль недержавних акторів.

Окрім того, цифровізація та цифрова трансформація світу та суспільних відносин йде небувалими темпами. На відміну від того, як творці норм міжнародного права діяли в XXI ст., створюючи, наприклад, концепцію "виключної економічної зони" в рамках морського права і забезпечуючи захист морського дна, визначаючи його статус як "загальної спадщини людства", кіберреволюція йде з такою швидкістю і настільки непередбачувано, що законодавці не встигають за інноваціями. Окрім того, що це є важливим аргументом для широкого залучення та інституціоналізації участі недержавних акторів, це водночас визначає критичну необхідність проактивного підходу та Agile-парадигми. Реалізація механізму нового мультилатералізму на основі принципів Agile фреймворку уможливить як максимально швидке реагування на зміни (навіть невеликі) у ландшафті глобальної/регіональної кібербезпеки, так й імплементацію проактивних підходів на основі прогнозування. Впровадження Agile підходу до кібербезпеки допомагає організаціям керувати кібербезпекою ефективно, і цей досвід корпоративного сектору може бути привнесений та адаптований для застосування у глобальному управлінні кібербезпекою.

Висновки

Кіберпростір став складнішим і проблематичнішим, ніж будь-коли, через швидкий технологічний прогрес, зростання витонченості кіберзлочинності та глибоко взаємопов'язані ланцюги поставок. Кіберпростір також став фактично полем бою. Національні держави дедалі частіше використовують кіберінструменти для шпигунства, порушення критичної інфраструктури держав-конкурентів та впливу на громадську думку. У міру загострення цих цифрових конфліктів фахівці з кібербезпеки опиняються на передовій нового виду війни.

Тим часом, дії кібердержав показують, що вони користуються відсутністю обов'язкового регулювання, щоб поставити себе в кращу конкурентну позицію для гегемонної влади, що перешкоджає створенню збалансованого регулювання з кожного з основних питань: інформаційний суверенітет і безпека, мілітаризація кіберпростору та міжнародне право. Доки вони вважають, що можуть отримати більше користі від можливостей у нерегульованому середовищі та що вони ще не вичерпали свої можливості для створення відносної переваги, цілком зрозуміло, що вони не братимуть на себе зобов'язання щодо обов'язкового застосування інструментів глобального управління кібербезпекою. Натомість, конкуренція між кібердержавами, особливо навколо інновацій в галузі ІКТ, змушує їх йти на більші ризики для досягнення короткострокових вигод, водночас кожна з них формує глобальні умови для застосування інструментів в майбутньому в обов'язковому порядку. Отже, у сучасному глобальному конкурентному середовищі незалежні дії кібердержав та розширення їхнього впливу серед країн-однодумців є кориснішими для пот-

реб безпеки кожної країни, ніж цінність колективної кібербезпеки в обов'язкових міжнародних рамках.

Однак унікальна природа сфери кібербезпеки характерна неформальністю міжнародного режиму кібербезпеки через максимальний вплив геополітики та інтересів/діяльності недержавних суб'єктів. Зростання впливу недержавних суб'єктів на міжнародне управління кібербезпекою створює для держав як можливості, так і виклики. З одного боку, очевидно, що деякі приватні компанії та організації громадянського суспільства з ентузіазмом сприйняли неформальне управління та представили свої пропозиції державам також у формі необов'язкових норм. З іншого боку, така широка та, значною мірою, вирішальна участь недержавних суб'єктів створює досить високі ризики ентропії. Це вимагає розроблення нової системи, яка б забезпечила ефективність та проактивну гнучкість у глобальному управлінні кібербезпекою, заснованій на парадигмі гнучкості (Agile).

References

1. Allen, G. C., & Benson, E. (2023). Clues to the U. S. – Dutch – Japanese semiconductor export controls deal are hiding in plain sight. URL: https://www.csis.org/analysis/clues-us-dutch-japanese-semiconductor-export-controls-deal-are-hiding-plain-sight
2. Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs, 3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924
3. Bradley, C., Goldsmith, J., & Hathaway, O. A. (2023). The rise of nonbinding international agreements: An empirical, comparative, and normative analysis. *University of Chicago Law Review, 90*. URL: https://live-chicago-law-review.pantheonsite.io/sites/default/files/2023-09/01_Bradley_ART_Final.pdf
4. Butcher, J., & Beridze, I. (2019). What is the state of artificial intelligence governance globally? *The RUSI Journal, 164*(5-6), 88–96. https://doi.org/10.1080/03071847.2019.1694260
5. Cai, C., & Zhang, R. (2025). Fragmentation of global cybersecurity governance: quasi-public goods and multi-level conflicts. *Global Political Economy, 4*(1), 32–50. https://doi.org/10.1332/26352257Y2024D000000016
6. Delerue, F., Douzet, F., & Géry, A. (2020). The geopolitical representations of international law in the international negotiations on the security and stability of cyberspace (Report No. 75). IRSEM/EU Cyber Direct. URL: https://www.irsem.fr/media/5-publications/etudes/report-75-delerue-et-al.pdf
7. Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy, 45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062
8. Gartzke, E., & Lindsay, J. R. (2024). *Elements of deterrence*. Oxford University Press.
9. Georgescu, A. (2022). Cyber diplomacy in the governance of emerging AI technologies – a transatlantic example. *International Journal of Cyber Diplomacy, 3*, 13–22. https://doi.org/10.54852/ijcd.v3y202202
10. Greiman, V. (2015). Cybersecurity and global governance. *Journal of Information Warfare, 14*(4), 1–14. https://www.jstor.org/stable/26487502
11. Inkster, N. (2021). *The great decoupling: China, America and the struggle for technological supremacy*. Hurst.
12. Johnstone, I., Sukumar, A., & Trachtman, J. (Eds.). (2023). *Building an international cybersecurity regime*. Edward Elgar Publishing.
13. Kittichaisaree, K. (2017). *Future prospects of public international law of cyberspace. Public international law of cyberspace*. Springer International.
14. Maas, M., & Villalobos, J. (2023). International AI institutions: a literature review of models, examples, and proposals. *AI Foundations Report 1*. https://doi.org/10.2139/ssrn.4579773
15. Natorski, M. (2025). *Multilateralism in the global governance of artificial intelligence.* Maastricht University. https://doi.org/10.48550/arXiv.2508.15397
16. Nye, J. (2014). *The Regime Complex for Managing Global Cyber Activities*, vol. 1. Cambridge: Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University.
17. Obodiak, V., & Kotukh, Y. (2020). The main challenges of governance in the field of cybersecurity. *Theory and Practice of Public Administration*, *4*(71), 38–46. https://doi.org/10.34213/tp.20.04.05
18. Raymond, M., & Sherman, J. (2023). Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice. *Contemporary Security Policy. 45*(8), 1–31. https://doi.org/10.1080/13523260.2023.2269809
19. Reykers, Y., Karlsrud, J., Brosig, M., Hofmann, S. C., Maglia, C., & Rieker, P. (2023). Ad hoc coalitions in global governance: Short-notice, task- and time-specific cooperation. *International Affairs*, *99*(2), 727–745. https://doi.org/10.1093/ia/iiac319
20. Roger, C., & Rowan, S. (2023). The New terrain of global governance: Mapping membership in informal international organizations. *Journal of Conflict Resolution, 67*(6), 1248–1269. https://doi.org/10.1177/00220027221139431
21. Rovner, J. (2023). The elements of an intelligence contest. In R. Chesney & M. Smeets (Eds.), *Deter, disrupt or deceive. Assessing cyber conflict as an intelligence contest* (pp. 17–42). Georgetown University Press.
22. Schmitt M., et al. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
23. Schmitt, L. (2022). Mapping global AI governance: a nascent regime in a fragmented landscape. *AI Ethics, 2*, 303–314. https://doi.org/10.1007/s43681-021-00083-y
24. Smeets, M. (2022). No shortcuts: Why states struggle to develop a military cyber-force. Hurst & Oxford University Press.
25. Stephen, M. (2025). *The diffusion of global power and the decline of global governance*. Cambridge University Press.
26. Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy*, *45*(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739
27. Sundari, S., Astuti, Y., Uceng, A., Jumirah, J. (2025). Universal data security in building a global governance framework. *SSRN*. https://doi.org/10.2139/ssrn.5186245
28. Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., Lundgren, M. (2023). The global governance of artificial intelligence: Next steps for empirical and normative research. *International Studies Review, 25*(3). https://doi.org/10.1093/isr/viad040
29. Trachtman, J. (2013). *Cyberspace and cybersecurity. The future of international law: Global government*. Cambridge: Cambridge University Press.
30. Urgessa, W. (2020). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. *Computer Law & Security Review, 36*, 105368. https://doi.org/10.1016/j.clsr.2019.105368
31. Vandendriessche, M. (2025). Global cybersecurity governance: a hallmark of heterogeneity? In: J. Jordana, M. Vandendriessche, & J. Wouters (eds). *Institutions of global governance*. Edward Elgar Publishing. https://doi.org/10.4337/9781035302581.00013
32. Veale, M., Matus, K., & Gorwa, R. (2023). AI and global governance: Modalities, rationales, tensions. *Annual Review of Law and Social Science, 19,* 255–275. https://doi.org/10.1146/annurev-lawsocsci-020223-040749
33. Vergne, J., & Duran, R. (2014). Cyberespace et organisations "Virtuelles": L' état Souverain a-t-Il Encore un Avenir? [Cyberspace and "Virtual" Organizations: Does the Sovereign State Still Have a Future?]. *Regards Croisés sur L'Économie, 1*(14), 126–139. https://doi.org/10.3917/rce.014.0126
34. Westerwinter, O., Abbott, K. W., & Biersteker, T. (2021). Informal governance in world politics. *The Review of International Or-*

ganizations, *16*(1), 1–27. https://doi.org/10.1007/s11558-020-09382-1
35. Wolff, J. (2024). The role of insurers in shaping international cyber-security norms about cyber-war. *Contemporary Security Policy*, *45*(1), 141–170. https://doi.org/10.1080/13523260.2023.2279033
36. Zhang, P., Zheng, B., Ding, H., & Ruan, J. (2025). Cybersecurity: Challenges, Technologies and Future Trends. In: Proceedings of 4th International Conference on Electronics, Integrated Circuits and Communication Technology (EICCT), Chengdu, China, 2025 (pp. 485-489). https://doi.org/10.1109/EICCT65471.2025.11099896
37. Вівчар, І., Постельжук, О., & Валюх, Л. (2025). Кібербезпека як сфера міжнародного співробітництва у період глобальної кризи безпеки. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія, 2*(65). https://doi.org/10.21564/2663-5704.65.331787
38. Поляков, О. (2024). Кібердипломатія як важливий напрямок міжнародно-правового співробітництва в умовах режиму воєнного стану. *Нове Українське Право, 6*, 70–76. https://doi.org/10.51989/NUL.2024.6.10
39. Стежко, С. & Шевченко, Т. (2021). Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформація і Право, 2*(37), 139–144. https://doi.org/10.37750/2616-6798.2021.2(37).238349
40. Черниш, Р. (2021). Міжнародний організаційний досвід у сфері забезпечення кібербезпеки. *Вісник Кримінального Судочинства*, *3-4,* 112–121. https://doi.org/10.17721/2413-5372.2021.3-4/112-121

V. O. Tkach

Ukrainian National Forestry University, Lviv, Ukraine

GLOBAL CYBERSECURITY GOVERNANCE: INSTITUTIONS AND ADAPTATION TO MODERN CHALLENGES

Introduction. New opportunities and advantages generated by the large-scale introduction of digital technologies into all spheres of public relations are accompanied by the emergence of new types of dangers and criminal encroachments ("cyberattacks", "cyber threats"), which have actually turned into a new global problem for all of humanity. Today, it can be confidently stated that ensuring cybersecurity (and, in a broader context, information security) is one of the most pressing challenges that states will have to respond to, acting both individually and jointly within international organizations and international integration associations. However, due to the complexity and duration of coordinating the positions of states at the global level (in particular, within the UN), their international cooperation and integration in the field of joint cybersecurity is currently developing not evidently successfully.

Meanwhile, without a fundamental change in the nature of relations between all or even between the main players, the multiplication of the number of poles inevitably means the multiplication of the number of security risks. Therefore, in the analysis of future models of world order, along with the concepts of multipolarity and polycentrism, it is important to turn to the concept of multilateralism. Finding ways to build a new, effective and flexible environment of multilateral cooperation to counter emerging cybersecurity threats is an extremely urgent scientific task.

Materials and Methods. The study is based on an integrative review tool using the Mixed Methods Assessment Tool (MMAT). The methodological apparatus of the study implied integration of systemic, comparative, historical-genetic and functional methods, which provides a comprehensive study of international multilateral mechanisms for global cybersecurity governance.

Analysis of Literary Sources. The analysis of academic sources demonstrates that the issue of global cybersecurity governance has been widely studied from institutional, legal, and technological perspectives. Previous studies have emphasized the fragmented and heterogeneous nature of the global cybersecurity landscape, highlighting the challenges associated with the development of unified legal norms and coordinated international responses to cyber threats. Researchers have identified the lack of effective international cooperation, differences in national cybersecurity strategies, and the growing geopolitical competition among major powers as key barriers to the formation of a comprehensive global cybersecurity regime.

The literature also underscores the increasing role of non-state actors, including private companies, international organizations, and civil society institutions, in shaping cybersecurity standards and governance mechanisms. Special attention has been given to the emergence of artificial intelligence as a factor influencing cybersecurity governance and requiring the development of new institutional frameworks. Despite the growing number of initiatives and cooperative platforms, scholars agree that global cybersecurity governance remains characterized by institutional fragmentation, the predominance of non-binding norms, and limited enforcement mechanisms.

Overall, the reviewed literature confirms the necessity of developing more adaptive and inclusive multilateral approaches capable of integrating state and non-state actors and responding effectively to the rapidly evolving cybersecurity environment.

Despite the significant body of research devoted to global cybersecurity governance, several important aspects of the general problem remain insufficiently addressed. The existing literature primarily focuses on legal frameworks, institutional structures, and national cybersecurity strategies, while limited attention has been given to the integration of adaptive governance models capable of responding to rapidly evolving cyber threats.

Results. Multilateral cooperation in cyber- and information spheres is needed more than ever, especially at a time when geopolitical conflicts threaten to spiral out of control. Civilian and military forces need to work together to agree on the operational boundaries of the latter and how best to share information and behave responsibly in cyber- and information spheres.

The study results demonstrate the growing importance of adaptive and multilateral approaches in the development of global cybersecurity governance systems. The conducted analysis made it possible to identify the key structural elements of contemporary cybersecurity governance, including institutional cooperation mechanisms, regulatory frameworks, and multi-stakeholder interaction models. The findings reveal that the effectiveness of existing international cybersecurity arrangements remains limited due to fragmented governance structures, inconsistent regulatory standards, and the lack of enforceable global norms.

A conceptual diagram of the international cybersecurity regime is presented, highlighting the main actors according to their roles and functions. The two wings of the regime interact with the "cyber diplomacy" circle, which in turn shapes discussions at UN negotiations. Through the diplomatic circle, actors from the outer wings try to secure their interests while remaining outside the formal diplomatic negotiations.

The results also indicate that the integration of Agile-based governance principles into multilateral cybersecurity frameworks can significantly enhance institutional flexibility and responsiveness to emerging cyber threats. Particular attention was given to the increasing role of non-state actors, including private technology companies and international organizations, whose participation contributes to the development of operational standards and collaborative mechanisms.

Furthermore, the study identified the necessity of strengthening trust-building measures, improving cyber incident attribution mechanisms, and expanding international cooperation platforms to support coordinated responses to transnational cyber threats. Overall, the obtained results confirm the feasibility of developing integrated governance models based on the principles of new multilateralism, which are capable of ensuring greater resilience, adaptability, and sustainability of global cybersecurity systems in the context of rapid technological change.

Discussion. The discussion of the obtained results confirms the relevance of transforming traditional models of global cybersecurity governance toward more flexible and adaptive multilateral frameworks. The interpretation of the findings demonstrates that the identified institutional limitations and regulatory inconsistencies correspond with trends highlighted in contemporary academic literature, particularly regarding the fragmented nature of global cybersecurity regimes. The results obtained in this study support the assumption that the effectiveness of international cybersecurity cooperation depends on the ability of governance systems to integrate diverse stakeholders and ensure coordinated decision-making processes.

The discussion also highlights the significance of combining state-centered regulatory mechanisms with multi-stakeholder initiatives involving private sector entities, international organizations, and civil society actors. Such integration is considered essential for enhancing the operational capacity of cybersecurity governance systems and addressing the increasing complexity of transnational cyber threats. In addition, the findings underline the necessity of introducing adaptive governance approaches, including Agile-based coordination mechanisms, as a means of improving responsiveness to rapidly evolving technological and geopolitical conditions.

Moreover, the discussion emphasizes the importance of strengthening international trust-building measures, harmonizing cybersecurity standards, and improving attribution procedures for cyber incidents. The interpretation of the results confirms that the implementation of integrated governance models based on the principles of new multilateralism can contribute to increasing the resilience and sustainability of global cybersecurity governance systems. Overall, the discussion substantiates the practical relevance of the proposed approaches and highlights their potential applicability in the development of future international cybersecurity strategies.

It is highlighted that implementing a mechanism for new multilateralism based on the principles of the Agile framework will enable both the fastest possible response to changes (even small ones) in the global/regional cybersecurity landscape and the implementation of proactive approaches based on forecasting. The implementation of Agile approach to cybersecurity helps organizations manage cybersecurity effectively, and this experience of the corporate sector can be brought and adapted for use in global cybersecurity management.

Conclusion. Cyberspace became more complex and problematic than ever before, due to rapid technological advances, the increasing sophistication of cybercrime, and deeply interconnected supply chains. Cyberspace also became a de facto battlefield. Meanwhile, the actions of cyberstates show that they are taking advantage of the lack of mandatory regulation to better compete with hegemonic powers, which hinders the creation of balanced regulation on each of the main issues: information sovereignty and security, the militarization of cyberspace, and international law. However, the unique nature of the cybersecurity sphere is characterized by the informality of the international cybersecurity regime due to the maximum influence of geopolitics and the interests/activities of non-state actors. The growing influence of non-state actors on international cybersecurity governance creates both opportunities and challenges for states. This requires the development of a new system that would ensure efficiency and proactive flexibility in global cybersecurity management, based on the Agile paradigm.

Keywords: cybersecurity; cyber threats; non-state actors (stakeholders); global cybersecurity landscape; public governance; global governance; security challenges for Ukraine.