УДК 342.951
DOI: https://doi.org/10.24144/2307-3322.2026.94.2.53

КІБЕРДИПЛОМАТІЯ ЯК ІНСТРУМЕНТ СТРИМУВАННЯ ДЕРЖАВНОЇ АГРЕСІЇ В КІБЕРПРОСТОРІ: МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ АТРИБУЦІЇ КІБЕРАТАК

Мануілов Я.С.,
старший науковий співробітник
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України
ORCID: 0000-0001-8149-2745

Мануілов Я.С. Кібердипломатія як інструмент стримування державної агресії в кіберпросторі: міжнародно-правові механізми атрибуції кібератак.

У статті здійснено комплексне теоретико-правове дослідження концептуальних засад кібердипломатії як відносно нового, але стратегічно важливого інструменту сучасної зовнішньої політики. Автор розглядає кібердипломатію не лише як засіб комунікації, а як багаторівневий механізм, спрямований на стримування державної агресії в цифровому просторі та формування стійкого правопорядку. Особливу увагу приділено одній із найскладніших проблем міжнародного права – атрибуції кібератак. Проаналізовано дихотомію цього процесу, який поєднує в собі складну технічну форензику (встановлення цифрового сліду) та юридичну кваліфікацію дій суб'єктів згідно з нормами про відповідальність держав за міжнародно-протиправні діяння. У контексті положень Таллінського посібника детально проаналізовано критерії розмежування «ефективного» та «загального» контролю над недержавними хакерськими угрупованнями, що діють в інтересах держав-агресорів. Доведено, що традиційні підходи до інституту атрибуції потребують адаптації через специфіку конфлікту у кіберпросторі. У статті висвітлено еволюцію «Інструментарію кібердипломатії ЄС» (Cyber Diplomacy Toolbox), зокрема механізмів колективної атрибуції та впровадження обмежувальних заходів (санкцій) як засобів підвищення «ціни» агресивної поведінки. На основі аналізу унікального досвіду України в умовах повномасштабного вторгнення РФ обґрунтовано необхідність переходу від реактивної до проактивної моделі кібердипломатії. У статті підкреслюється важливість уніфікації міжнародних стандартів для цифрових доказів, що дозволить використовувати результати технічних розслідувань у міжнародних судових інстанціях. Визначено подальші перспективи розвитку кодифікації правил поведінки держав у кіберпросторі (норми відповідальної поведінки) та висунуто пропозицію щодо створення інклюзивних міжнародних майданчиків для незалежної верифікації доказів причетності держав до масштабних кібероперацій. Зроблено висновок, що ефективна кібердипломатія є ключовим фактором забезпечення стабільності глобального інформаційного середовища та захисту національного суверенітету в епоху гібридних загроз.

Ключові слова*:* кібердипломатія, атрибуція кібератак, стримування, державна агресія, міжнародне право, інструментарій кібердипломатії ЄС, відповідальність держав, кіберпростір, цифрові докази.

Manuilov Y.S. Cyber diplomacy as a tool for deterring state aggression in cyberspace: international legal mechanisms for cyberattack attribution.

This article provides a comprehensive theoretical and legal study of the conceptual foundations of cyber diplomacy as a relatively new yet strategically vital instrument of modern foreign policy. The author conceptualizes cyber diplomacy not merely as a communication tool but as a multi-layered mechanism designed to deter state aggression in the digital realm and establish a resilient legal order. Special emphasis is placed on one of the most intricate challenges in international law – the attribution of cyberattacks. The study analyzes the dichotomy of this process, which integrates complex technical forensics (establishing a digital footprint) with the legal qualification of actors' conduct under the norms of state responsibility for internationally wrongful acts. Within the framework of the Tallinn Manual, the article provides a detailed analysis of the criteria for distinguishing between «effective» and «overall»

control over non-state hacking groups acting on behalf of aggressor states. It is argued that traditional approaches to the institution of attribution require adaptation due to the specific nature of conflicts in cyberspace. The paper highlights the evolution of the «EU Cyber Diplomacy Toolbox», specifically the mechanisms for collective attribution and the implementation of restrictive measures (sanctions) as a means of increasing the «cost» of aggressive behavior. Based on an analysis of Ukraine's unique experience during the full-scale invasion by the Russian Federation, the author justifies the necessity of transitioning from a reactive to a proactive model of cyber diplomacy. The article underscores the importance of unifying international standards for digital evidence, which would facilitate the use of technical investigation results in international judicial instances. The study identifies future prospects for the codification of rules of state conduct in cyberspace (norms of responsible behavior) and proposes the creation of inclusive international platforms for the independent verification of evidence regarding state involvement in large-scale cyber operations. It is concluded that effective cyber diplomacy is a key factor in ensuring the stability of the global information environment and protecting national sovereignty in the era of hybrid threats. The article examines the conceptual foundations of cyber diplomacy as a strategic foreign policy tool aimed at deterring state aggression in digital space. The complex nature of international legal mechanisms for the attribution of cyberattacks, which combine technical forensics and legal qualification of actors' conduct, is analyzed. Particular attention is paid to the application of the Articles on Responsibility of States for Internationally Wrongful Acts and the provisions of the «Tallinn Manual 2.0» in the context of distinguishing between «effective» and «overall» control over non-state actors. The evolution of the «EU Cyber Diplomacy Toolbox» and collective attribution mechanisms as means of increasing the cost of aggressive behavior is highlighted. Based on Ukraine's experience during the full-scale invasion by the Russian Federation, the necessity of unifying international standards for digital evidence and creating a proactive cyber diplomacy model capable of ensuring the stability of the global information environment is substantiated. The prospects for the further development of the codification of attribution rules and the creation of inclusive international platforms for the verification of evidence have been identified.

Key words*:* cyber diplomacy, attribution of cyberattacks, deterrence, state aggression, international law, EU Cyber Diplomacy Toolbox, state responsibility, cyberspace, digital evidence.

Постановка проблеми. Сучасний етап розвитку міжнародних відносин характеризується безпрецедентним зростанням ваги цифрового суверенітету в системі національної та міжнародної безпеки. Кіберпростір, який спочатку розглядали як простір для вільного обміну інформацією та наукового прогресу, перетворився на арену інтенсивного стратегічного суперництва, де держави та підконтрольні їм суб'єкти використовують інформаційно-комунікаційні технології для досягнення геополітичних цілей. Агресія держави в кіберпросторі набуває форм, які часто залишаються нижче порогу збройного конфлікту, але здатні підірвати економічну стабільність, цілісність демократичних інститутів та функціонування критичної інфраструктури. У таких умовах кібердипломатія виникає як критично важливий інструмент зовнішньої політики, спрямований на розробку норм про відповідальність держав та формування механізмів стримування ворожої активності через правові та політичні засоби [1].

Одним із центральних викликів для міжнародного співтовариства залишається проблема атрибуції – процесу ідентифікації суб'єкта, відповідального за проведення суспільно небезпечної кібероперації. Складність технічної архітектури мережі Інтернет, використання інструментів анонімізації та залучення недержавних хакерських груп («проксі-акторів») створюють умови для «правдоподібного заперечення» причетності держави до агресивних дій у кібепросторі. Міжнародно-правові механізми атрибуції є наріжним каменем реалізації відповідальності держав, оскільки без встановлення причинового зв'язку між протиправним діянням та конкретною державою застосування санкцій стає юридично небездоганним. Таким чином, науковий аналіз взаємодії кібердипломатії та правових інструментів атрибуції є надзвичайно актуальним для вдосконалення стратегій стримування державної агресії [2].

Стратегія кібербезпеки України містить ціль С.4 «Розвиток асиметричних інструментів стримування», досягнення якої передбачає створення Україною необхідних умов для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів [3]. В даному контексті наша держава має запровадити асиметричні інструменти стримування шляхом застосування усіх доступних інструментів дипло-

матії та міжнародного права задля протидії зловмисній діяльності у кіберпросторі проти України [3].

Метою цієї статті є аналіз кібердипломатії як стратегічного інструменту зовнішньої політики, спрямованого на стримування державної агресії, а також дослідження міжнародно-правових проблем атрибуції – процесу встановлення юридичної відповідальності держав за шкідливу діяльність у кіберпросторі.

Стан опрацювання проблематики. Аналіз сучасних наукових публікацій свідчить про стійкий інтерес до кібердиплоаматії як інструменту стратегічного інструменту зовнішньої політики. Різним аспектам цього питання присвятили свої роботи О.Гайдук [4], О. Половко [5], О. Поляков [6], О.Сурілова [7], В. Г. Ціватий [8].

Істотний внесок у дослідження цієї проблеми зробили зарубіжні дослідники – Дж. Крістоу (George Christou) [9], М. Шміт (Michael Schmitt), Н.Цагуріас (Ni. Tsagourias) та М. Фаррелл (M. Farrell).

Виклад основного матеріалу. Кібердипломатія не є виключно технічним або допоміжним напрямом дипломатичної діяльності, а являє собою складний комплекс заходів, що включає двосторонні та багатосторонні переговори, розробку міжнародних стандартів, розбудову кіберспроможностей та координацію спільних відповідей на інциденти. У широкому розумінні кібердипломатія включає в себе кібербезпеку, кіберзлочинність, зміцнення довіри, свободу Інтернету та управління Інтернетом [10]. Основна мета кібердипломатії в контексті стримування полягає у підвищенні «ціни» агресивної поведінки для порушника. Це досягається через комбінацію дипломатичного тиску, політичної ізоляції та правових наслідків. Стримування в кіберпросторі традиційно поділяється на два вектори: стримування шляхом заперечення (deterrence by denial), що фокусується на зміцненні захисту, та стримування шляхом застотсування покарання (deterrence by punishment) як відплату за вчинену атаку[11].

Стратегічне суперництво в кіберпросторі відображає глобальний конфлікт між ліберальною та авторитарною моделями цифрового порядку. Якщо такі демократичні держави (групи держав), як США та ЄС виступають за відкритий, вільний та безпечний Інтернет, заснований на повазі до прав людини та верховенства права, то авторитарні режими розглядають кіберпростір як засіб контролю над інформаційним потоком та інструмент підриву демократичних процесів у державах, з якими вони конкурують. Кібердипломатія в цьому аспекті стає засобом захисту цінностей, оскільки через міжнародні організації та форуми просуваються норми, що обмежують можливість держав втручатися в приватне життя громадян та функціонування іноземних інституцій. Конфлікт між ідеологіями «свободи інформації» та «інформаційного контролю» визначає динаміку міжнародних переговорів у межах ООН та інших політичних майданчиків [11].

Важливим компонентом кібердипломатії є формування довіри між державами (Confidence Building Measures, CBMs). Міжнародні заходи із зміцнення довіри спрямовані на зменшення ризику випадкової ескалації конфлікту через непорозуміння або неправильну інтерпретацію кібероперацій. Дипломатичні канали зв'язку дозволяють сторонам оперативно обмінюватися інформацією про інциденти та запитувати роз'яснення, що є критично важливим у ситуаціях, коли технічна атрибуція займає тривалий час. Разом із тим, дипломатія слугує платформою для формування коаліцій, здатних на колективну атрибуцію, що значно посилює сигнал стримування, оскільки агресор стикається з консолідованою позицією групи впливових держав [12].

Кібердипломатія також виконує функцію легітимізації контрзаходів. Згідно з міжнародним правом, держава, яка визнається жертвою агрсії, має право на вжиття пропорційних заходів у відповідь на протиправне діяння іншої держави. Проте в кіберпросторі межа між правомірною відповіддю та актом агресії є надзвичайно тонкою. Дипломатичний супровід процесу атрибуції дозволяє представити докази світовій спільноті, обґрунтувати необхідність реакції та запобігти звинуваченням у порушенні міжнародного права з боку самої держави-жертви. Таким чином, кібердипломатія трансформує технічні дані про атаку в політико-правовий аргумент, зрозумілий для міжнародних партнерів [13].

Фундаментом для застосування дипломатичних інструментів стримування є чинне міжнародне право, норми якого передбачають відповідальність держав за міжнародно-протиправні діяння. Основним принципом є те, що держава несе відповідальність за будь-яку дію, яка приписується їй згідно з міжнародним правом і становить порушення її міжнародного зобов'язання. Якщо кібероперація визнається складовою збройного конфлікту, до неї мають застосовуватися основополож-

ні принципи міжнародного гуманітарного права: пропорційності; незастосування невибіркової зброї; розмежування між військовими цілями та цивільними особами і недопущення вероломства [14]. В контексті кіберпростору це означає, що держави повинні дотримуватися принципів суверенітету, невтручання у внутрішні справи та утримуватися від загрози силою або її застосування. Усі члени Генеральної Асамблеї ООН неодноразово підтверджували доцільність застосування цих норм до ІКТ-середовища, що створює правову основу для дипломатичного тиску на правопорушників [15].

Принцип державного суверенітету в кіберпросторі має двояку природу. З одного боку, держава має виключне право здійснювати владу над кіберінфраструктурою та діяльністю на своїй території. З іншого боку, це право супроводжується обов'язком не допускати використання своєї території для вчинення дій, що завдають шкоди іншим державам (принцип «належної обачності» або due diligence). Порушення цього обов'язку може стати підставою для міжнародної відповідальності, навіть якщо держава безпосередньо не організовувала атаку, але знала про неї та не вжила заходів для її припинення. Кібердипломатія використовує цей принцип для тиску на держави, що надають «безпечні гавані» для кіберзлочинців [16].

Особливе значення для інтерпретації міжнародного права в цій сфері має «Посібник Таллінна 2.0» (Tallinn Manual 2.0). Хоча він не є юридично обов'язковим договором, цей документ відображає консенсус провідних експертів щодо того, як існуючі норми застосовуються до кібероперацій. У посібнику підкреслюється, що держава несе відповідальність за міжнародно-протиправне діяння, вчинене у кіберпросторі (правило 14). Важливою новацією цього посібника є деталізація критеріїв, за якими кібератака може бути класифікована як «застосування сили» або навіть «збройний напад» у розумінні Статуту ООН, що відкриває шлях до реалізації права на самооборону [17].

Кваліфікація кібероперації як міжнародного злочину (агресії, воєнних злочинів або злочинів проти людяності) є ще одним інструментом кібердипломатії. Якщо кібератака спричиняє наслідки, які можна порівняти з результатами фізичного (кінетичного) нападу – загибель людей, масштабні руйнування або знищення критичної інфраструктури – вона може бути розглянута Міжнародним кримінальним судом (МКС). Прокурорами МКС підтверджено, що за певних обставин кібердіяльність може підпадати під юрисдикцію цього Суду. Це створює додатковий рівень стримування для державних діячів та військового командування, які можуть бути притягнуті до юридичної відповідальності за віддання наказів про проведення руйнівних кібероперацій у кіберпросторі [18].

Еволюція міжнародного права в цій сфері також пов'язана з діяльністю Групи урядових експертів ООН (UNGGE) та Робочої групи відкритого складу (OEWG). Ці майданчики використовуються кібердипломатами для формалізації рекомендаційних норм, що визначають поведінку держав. Наприклад, норма про неприпустимість атак на медичні заклади або виборчу інфраструктуру в мирний час стає частиною очікуваної поведінки держав. Хоча ці норми мають характер «м'якого права», їх систематичне порушення створює підстави для політичного осуду та запровадження колективних санкцій з боку міжнародної спільноти, що посилює загальну архітектуру стримування [19].

В рамках нашого дослідження важливо розкрити механізми атрибуції. Атрибуція в кіберпросторі – це не одноразова дія, а багатоетапний процес, який поєднує технічні інструменти, аналіз розвідувальних даних та правову оцінку. Технічна атрибуція полягає у виявленні джерел атаки шляхом аналізу шкідливого коду, IP-адреси, серверів управління та контролю (C2), а також специфічних технік, тактик та процедур (TTPs), які використовує зловмисник. Аналітики збирають індикатори компрометації (IoCs) на кожній стадії атаки: від підготовчої розвідки та доставки шкідливого програмного забезпечення до виконання злочинних завдань. Проте, самі по собі технічні докази часто є недостатніми для звинувачення держави, оскільки сучасний агресор майстерно використовує фальшиві цифрові сліди для відведення підозр [20].

Юридична атрибуція спрямована на встановлення зв'язку між конкретною особою чи групою, що вчинили атаку, та державою як суб'єктом міжнародного права. Відповідно до Талліннського посібника 2.0 дії державних органів, таких як збройні сили або розвідувальні служби, безумовно приписуються державі (правило 15). Це включає випадки, коли посадові чи службові особи діють ultra vires, тобто перевищуючи свої повноваження або всупереч посадовим інструкціям. У сучасній практиці прикладами такої прямої атрибуції є ідентифікація причетності ГРУ рф до атак на Україну та західні інституції, або кібершпигунство спецслужбами Китаю [17].

Найскладнішим аспектом атрибуції є доведення відповідальності держави за дії недержавних акторів – хакерських угруповань, «патріотичних» хакерів або приватних підрядників. Традиційний міжнародно-правовий тест «ефективного контролю» (effective control), викладений Міжнародним судом ООН у справі «Нікарагуа», вимагає доказів того, що держава керувала кожним конкретним аспектом протиправного діяння. У кіберпросторі такий рівень доказовості є майже недосяжним. У відповідь на це кібердипломати та юристи пропонують використовувати тест «загального контролю» (overall control) або нову концепцію «контролю та спроможностей» (control and capabilities). Остання передбачає аналіз сукупності факторів: фінансування групи державою, надання їй інфраструктури, використання схожого коду з державними розробками та політичну мотивацію [21].

Атрибуція часто здійснюється через призму національної безпеки та розвідувальних оцінок, які не завжди оприлюднюються в повному обсязі. Це породжує проблему довіри до публічних звинувачень. Наприклад, у 2016 році США офіційно звинуватили росію у втручанні у виборчий процес через злам мереж Демократичної партії, проте значна частина доказової бази залишилася засекреченою для захисту методів розвідки. У таких випадках кібердипломатія працює для створення механізмів колективної атрибуції, коли кілька держав одночасно підтверджують висновки одна одної, що підвищує легітимність звинувачення без необхідності розкриття чутливих технічних деталей [22].

Процес атрибуції також стикається з викликами, пов'язаними з «територіальною атрибуцією». Оскільки атака може здійснюватися з серверів, розташованих у третіх країнах без відома їхніх урядів, просте виявлення географічного походження сигналу щн не означає провини цієї держави. Це підкреслює важливість співпраці між правоохоронними органами різних країн для швидкого отримання електронних доказів. Проте, за відсутності згоди держави на співпрацю, атрибуція стає інструментом політичного тиску, де кібердипломатія використовується для пред'явлення ультиматумів державам, що ігнорують зловмисну діяльність у своїх межах [23].

Європейський Союз розробив одну з найбільш комплексних рамок дипломатичного реагування на кіберзагрози, відому як «Інструментарій кібердипломатії» (Cyber Diplomacy Toolbox, CDT). Ухвалений у 2017 році, цей акт надав державам-членам та інституціям ЄС набір інструментів для запобігання, стримування та реагування на шкідливу кібердіяльність. CDT базується на Спільній зовнішній та безпековій політиці (CFSP) і передбачає використання як м'яких заходів (заяви, демарші), так і жорстких обмежень (санкції). Основна ідея CDT полягає в тому, що спільна відповідь ЄС має більшу вагу, ніж індивідуальні дії держав, і здатна ефективно впливати на розрахунки агресора [24].

Ключовим елементом CDT є режим кіберсанкцій, запроваджений у 2019 році. Він дозволяє ЄС накладати обмежувальні заходи (замороження активів, заборона на в'їзд) на фізичних та юридичних осіб, відповідальних за кібератаки, що мають значний вплив на Союз або його держави-члени. Це включає атаки проти критичної інфраструктури, послуг першої необхідності, демократичних інститутів та викрадення інтелектуальної власності. У 2020 році ЄС вперше застосував ці заходи проти суб'єктів з рф, Китаю та КНДР, що стало серйозним сигналом про готовність Європи захищати свій цифровий суверенітет [25].

Оновлення CDT у 2022 році, спричинене повномасштабним вторгненням росії в Україну та різким зростанням кіберзагроз, посилило координаційну роль Європейської служби зовнішніх справ (EEAS). Нові керівні принципи фокусуються на покращенні ситуаційної обізнаності та швидкості прийняття рішень. Важливою інновацією стала вимога тіснішої співпраці між цивільними та військовими структурами, оскільки сучасні кіберконфлікти часто мають гібридний характер. ЄС також почав активніше використовувати CDT для підтримки країн-партнерів, зокрема України, надаючи допомогу в атрибуції атак та запроваджуючи санкції проти тих, хто атакує українські мережі [26].

Структура CDT включає кілька рівнів реагування, що дозволяє гнучко підходити до кожного інциденту залежно від його серйозності та наявних доказів. На найнижчому рівні це можуть бути технічні консультації та обмін інформацією. На вищих рівнях – це офіційні заяви Високого представника ЄС від імені всіх держав-членів, які мають на меті «публічне визнання» агресора. Найвищим рівнем є санкції, рішення про які приймається Радою ЄС одностайно. Така архітектура формування санкцій забезпечує політичну солідарність, хоча необхідність одностайності іноді сповільнює процес реагування на критичні інциденти [27].

Ефективність CDT також залежить від взаємодії з іншими правовими актами ЄС, такими як Директива NIS 2 та Акт про кіберстійкість. Ці акти створюють надійну правову основу для кібердипломатії, оскільки забезпечують високий рівень технічного захисту, що робить зовнішні зусилля зі стримування більш ефективними. Крім того, ЄС активно просуває свій підхід на міжнародній арені, намагаючись встановити глобальні стандарти для санкційних режимів у кіберпросторі. Це сприяє формуванню трансатлантичної та глобальної мережі демократичних держав, здатних на скоординовану відсіч цифровій агресії [28].

Україна займає унікальне місце в системі світової кібербезпеки, оскільки протягом останнього десятиліття вона стала головним полігоном для випробування російської кіберзброї. Атаки на енергомережі у 2015-2016 роках, руйнівний вірус NotPetya у 2017 році та масовані кібероперації під час повномасштабного вторгнення дали українським експертам безцінний досвід технічної атрибуції. Це дозволило Україні стати активним суб'єктом кібердипломатії, просуваючи ідею визнання кібератак актами агресії на міжнародному рівні. Досвід України свідчить, що технічна атрибуція повинна відбуватися максимально швидко, щоб стати основою для політичних рішень союзників [29].

Атака NotPetya стала класичним прикладом того, як кібердипломатія може бути використана для колективної відповіді. Після того як українські фахівці спільно з партнерами довели причетність ГРУ рф, уряди Великої Британії, США, Австралії та інших країн виступили з синхронними заявами про атрибуцію. Це був перший масштабний випадок колективної відповіді, який продемонстрував росії, що агресія в кіберпросторі не залишиться непоміченою. Проте, незважаючи на політичний осуд, юридичні наслідки були обмеженими, що підкреслює необхідність вдосконалення міжнародно-правових механізмів притягнення до відповідальності [30].

Для України питання атрибуції має не лише оборонний, а й компенсаційний аспект. У межах міжнародних позовів проти рф за агресію, докази кібератак використовуються як складова частина загальної шкоди, завданої державі.

З цього приводу українські дослідники О. Половко та С. Глотов наголошують на необхідності створення національної правової бази, яка б дозволяла визнавати цифрові докази легітимними в судах усіх рівнів. Це вимагає впровадження стандартів форензики, сумісних із міжнародними, що є частиною зобов'язань України в межах інтеграції до Єдиного цифрового ринку ЄС [31].

Важливим напрямом кібердипломатії є участь України в діяльності Центру передового досвіду НАТО з питань кібероборони (CCDCOE) та співпраця з Європейським агентством з кібербезпеки (ENISA). Ці платформи дозволяють українським дипломатам брати участь у розробці нових редакцій Талліннського посібника та формуванні спільної позиції Альянсу щодо стримування. Україна також активно використовує тристоронні та регіональні формати (наприклад, Люблінський трикутник) для координації кіберзахисту. Викликом залишається відсутність єдиного міжнародного органу з атрибуції, пропозиції щодо створення якого Україна неодноразово підтримувала на форумах ООН [32].

Українська стратегія кібердипломатії також враховує необхідність захисту від дезінформації та інформаційних операцій, які часто переплітаються з технічними атаками. Гібридний характер агресії рф вимагає від атрибуції врахування не лише коду, а й наративів, що поширюються одночасно з інцидентом. Це розширює сферу діяльності кібердипломатів від захисту мереж до захисту когнітивної сфери та демократичної стійкості суспільства. Взаємодія з приватним сектором (Big Tech компаніями, такими як Microsoft та Google) стала критичним елементом української атрибуції, оскільки ці компанії володіють глобальними даними про активність ворожих APT-груп [1].

Майбутнє кібердипломатії як інструменту стримування залежатиме від здатності міжнародної спільноти подолати правову невизначеність у питаннях атрибуції. Одним із перспективних шляхів є розробка багатосторонньої конвенції про цифрові докази та атрибуцію, яка б встановлювала єдині стандарти для представлення технічних даних у дипломатичних та судових процесах. Це дозволило б відійти від ситуативних звинувачень до системного правового тиску. Також актуальним є створення міжнародного арбітражу або трибуналу з кіберпитань, який міг би надавати незалежну оцінку інцидентам, що спричиняють міждержавні суперечки [29].

Розвиток технологій штучного інтелекту та квантових обчислень створює нові виклики для атрибуції. Агресори зможуть автоматизувати створення «дипфейків» у коді та інфраструктурі, роблячи ідентифікацію ще складнішою. Кібердипломатія повинна адаптуватися до цього, впроваджуючи механізми «алгоритмічної атрибуції», де легітимність доказів підтверджується за до-

помогою децентралізованих технологій (блокчейн) для фіксації логів атак без можливості їх зміни. Це потребуватиме нових угод про стандартизацію технологічних засобів розслідування на глобальному рівні [31].

Стримування в кіберпросторі також має стати більш проактивним. Концепція «постійного залучення» (persistent engagement), яку активно просувають США, передбачає безперервну присутність у мережах противника для зриву його операцій ще на стадії планування. Кібердипломатія відіграє тут роль обмежувача, встановлюючи рамки такої діяльності, щоб вона не переросла у відкриту війну. Це вимагає тонкого балансу між розвідувальними операціями та дипломатичними домовленостями про «ненапад» на цивільні об'єкти, що має бути закріплено в новому поколінні заходів зміцнення довіри [33]. Посилення ролі міжнародних організацій, таких як ООН, у верифікації атрибуції може стати ключовим чинником стабільності. Створення постійного Механізму ООН з питань кібербезпеки дозволило б державам, що не мають потужних власних розвідувальних спроможностей, отримувати об'єктивну інформацію про атаки проти них. Це сприятиме демократизації кіберпростору та захисту менш розвинених країн від цифрового колоніалізму та агресії з боку технологічних потуг. Кібердипломатія в цьому сенсі стає інструментом глобальної справедливості [34].

Висновки. Кібердипломатія пройшла шлях від вузькоспеціалізованої сфери до одного з головних інструментів стримування державної агресії в XXI столітті. Її ефективність безпосередньо корелює з якістю та швидкістю механізмів атрибуції кібератак. Встановлення юридичної відповідальності держав через тести «загального контролю» та концепцію «належної обачності» дозволяє міжнародній спільноті реагувати на гібридні загрози, які раніше залишалися безкарними. Європейський досвід «Інструментарію кібердипломатії» та українська практика протистояння російській агресії демонструють, що колективна відповідь та публічна атрибуція є потужними засобами підвищення політичної та економічної ціни за порушення міжнародних норм.

Подальший розвиток галузі потребує глибшої кодифікації правил атрибуції та створення інклюзивних міжнародних майданчиків для верифікації доказів. Стримування через кібердипломатію буде успішним лише тоді, коли агресор розумітиме: анонімність у мережі є ілюзорною, а правові наслідки за деструктивну діяльність – невідворотними. Україна, як держава з унікальним досвідом, повинна й надалі відігравати роль лідера у формуванні цих стандартів, перетворюючи свій досвід на глобальні інструменти безпеки. Врешті-решт, стабільність у кіберпросторі залежить не лише від досконалості коду, а й від міцності міжнародно-правового порядку, який здатний захистити суверенітет держав у цифрову епоху [14].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Cyber Diplomacy for Strategic Competition. *AFSA*. URL: https://afsa.org/cyber-diplomacy-strategic-competition (дата звернення: 22.03.2026).
2. State responsibility: attribution of cyber intrusions and Tallinn Manual 2.0. *Texas Law Review*. URL: https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/ (дата звернення: 22.03.2026).
3. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 року №447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
4. Гайдук О.В. Кібердипломатія України: нові горизонти дипломатичної діяльності у цифровому світі. *Кібердипломатія: матеріали Міжнародної науково-практичної конференції (м. Київ, 15–16 травня 2024 р.)* / за заг. ред. О.Г.Корченка. Київ: ДУІКТ, 2025. С. 6–8.
5. Половко О. Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення: дис. … д-ра філософії: 081. Нац. ун-т «Одеська юридична академія». Одеса, 2021. 219 с.
6. Поляков О.М. Кібердипломатія як важливий напрямок міжнародно-правового співробітництва в умовах режиму воєнного стану. *Нове українське право*. 2024. № 6. С. 44–47. DOI: https://doi.org/10.32689/2522-4603.2023.3.7.
7. Сурілова О.О. Публічна атрибуція кібератак державами-членами ЄС та застосування кіберсанкцій Союзом щодо кібератак, які становлять загрозу ЄС та його членам. *Правова держава*. 2021. № 43. С. 209–218. DOI: https://doi.org/10.18524/2411–2054.2021.43.241005.
8. Ціватий В.Г. Концепт «кібердипломатія» і міжнародні переговори в умовах цифрового суспільства XXI століття: практико-орієнтований, протокольно-етикетний та інституціональний дискурси. *Кібердипломатія: матеріали Міжнародної науково-практичної кон-*

ференції (м. Київ, 15–16 травня 2024 р.) / за заг. ред. О. Г. Корченка. Київ: ДУІКТ, 2025. С. 35–38.
9. Christou G. Cyber diplomacy: from concept to practice. *Tallinn Papers*. 2024. N. 12. 34 p. URL: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_ Practice_Christou.pdf (дата звернення: 22.03.2026).
10. Кібердипломатія. URL: https://warn-erasmus.eu/ua/glossary/kiber-diplomatiya/(дата звернення: 22.03.2026).
11. How European and allied cybersecurity strategies are shifting from defence to offence. *Binding Hook*. URL: https://bindinghook.com/how-european-and-allied-cybersecurity-strategies-are-shifting-from-defence-to-offence/ (дата звернення: 22.03.2026).
12. A Complete Guide to EU Cyber Diplomacy Toolbox. *UpGuard*. URL: https://www.upguard.com/blog/eu-cyber-diplomacy-toolbox (дата звернення: 22.03.2026).
13. Cyber Diplomacy: From Concept to Practice. *CCDCOE*. URL: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf (дата звернення: 22.03.2026).
14. Красніков С.А. Геополітика кіберконфліктів і кібервійн:міжнародно-правові виклики. Інформація і право. 2025. № 3(54). С. 147-156. DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340522.
15. EU Statement – UN General Assembly 1st Committee. *EEAS*. URL: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-general-assembly-1st-committee-other-disarmament-measures-and-international_en(дата звернення: 22.03.2026).
16. Revised Implementing Guidelines, Cyber Diplomacy Toolbox. *Cyber Diplomacy Toolbox*. URL: https://www.cyber-diplomacy-toolbox.com/Revised_Implementing_ Guidelines_Cyber_ Diplomacy_Toolbox.html (дата звернення: 22.03.2026).
17. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge University Press*. URL: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/law-of-international-responsibility/99E333F8578ADCC567A92BECF932E4C3 (дата звернення: 22.03.2026).
18. Cyber Operations and the Crime of Aggression. *Case Western Reserve Journal of International Law*. URL: https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2698&context=jil.
19. Cyber attribution: technical and international law methodologies. *European Journal of International Law*. URL: https://eprints.whiterose.ac.uk/id/eprint/159651/1/ NTsagourias%20and%20MFarrell%20Cyber%20attribution%20EJIL%20March%202020%20final.pdf (дата звернення: 22.03.2026).
20. Toward a New Lex Specialis Governing State Responsibility for Third-Party Cyber Incidents. *CCDCOE*. URL: https://ccdcoe.org/uploads/2018/10/Art-10-Toward-a-New-Lex-Specialis-Governing-State-Responsibility-for-Third-Party-Cyber-Incidents.pdf(дата звернення: 22.03.2026).
21. State responsibility: attribution of cyber intrusions and Tallinn Manual 2.0. *Texas Law Review*. URL: https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/ (дата звернення: 22.05.2025).
22. The Ultimate Challenge: Attribution for Cyber Operations. *Air University*. URL: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/WF_70_HILL_THE_ULTIMATE_CHALLENGE_ATTRIBUTION_FOR_CYBER_OPERATIONS.PDF.
23. European Union cyber diplomacy evolution. *EUI Cadmus*. URL: https://cadmus.eui.eu/bitstreams/923b2390-aa12-419d-aafa-32425dbf86fa/download.
24. Restrictive measures regarding cyberattacks and the Charter of Fundamental Rights. *ECLIC*. URL: https://www.researchgate.net/publication/382536551_THE_COMPATIBILITY_OF_RESTRICTIVE_MEASURES_REGARDING_CYBERATTACKS_WITH_THE_CHARTER_OF_FUNDAMENTAL_RIGHTS_OF_EU (дата звернення: 22.03.2026).
25. The Cyber Diplomacy Toolbox. *Cyber Diplomacy Toolbox*. URL: https://www.cyber-diplomacy-toolbox.com/ (дата звернення: 22.05.2025).
26. Space Diplomacy Toolbox and Digital Sovereignty. *EU Cyber Direct*. URL: https://eucyberdirect.eu/blog/space-diplomacy-toolbox-and-digital-sovereignty-lessons-from-european-cyber-diplomacy(дата звернення: 22.03.2026).

27. Cyber Diplomacy Toolbox: between sanctions and a lawful response to cyber-attacks. *European Papers*. URL: https://www.europeanpapers.eu/system/files/pdf_version/EP_e_J_2022_ 1_2_ Articles_Yuliya_Miadzvetskaya_Ramses_Wessel_00570.pdf.
28. International Law Perspective on NotPetya. *Ludovika*. URL: https://openaccess.ludovika.hu/nke/catalog/download/309/2936/6769?inline=1(дата звернення: 22.03.2026).
29. Analysis of policy responses to WannaCry and NotPetya. *SWP Berlin*. URL: https://www.swp-berlin.org/10.18449/2021RP11/(дата звернення: 22.03.2026).
30. Музика В.В. Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення. дис. … д-ра філософії: 081. Одеська юридична академія. 2021. 219 с.
31. EU Policy on Cyber Defence. *European Cyber Defence Policy*. URL: https://www.european-cyber-defence-policy.com/(дата звернення: 22.03.2026).
32. How European and allied cybersecurity strategies are shifting from defence to offence. *Binding Hook*. URL: https://bindinghook.com/how-european-and-allied-cybersecurity-strategies-are-shifting-from-defence-to-offence/.
33. EU Statement – UN General Assembly 1st Committee. *EEAS*. URL: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-general-assembly-1st-committee-other-disarmament-measures-and-international_en

Дата першого надходження рукопису до видання: 26.03.2026
Дата прийняття до друку рукопису після рецензування: 23.04.2026
Дата публікації: 10.05.2026