DOI: https://doi.org/10.31617/3.2025(140)03
УДК 004.946.5.056:341.242.5

ЗВЄРЄВА Катерина
https://orcid.org/0000-0003-2539-7035

доктор філософії з міжнародного права,
старший викладач кафедри міжнародного, цивільного та комерційного права
Державного торговельно-економічного університету

вул. Кіото, 19, м. Київ, 02156, Україна
zvereva.kateryna@gmail.com

ZVIERIEVA Kateryna
https://orcid.org/0000-0003-2539-7035

PhD (International Law),
Senior Lecturer at the Department
of International, Civil and Commercial Law
State University of Trade and Economics

19, Kyoto St., Kyiv, 02156, Ukraine
zvereva.kateryna@gmail.com

ВІДПОВІДАЛЬНІСТЬ ДЕРЖАВИ ЗА КІБЕРАТАКИ ТРЕТІХ СТОРІН В УМОВАХ АНОНІМНОСТІ

Актуальність дослідження зумовлена стрімким зростанням кількості кібератак, що здійснюються опосередковано через третіх акторів (недержавні групи чи проксі-акторів), та складнощами притягнення держав до відповідальності за такі дії в умовах анонімності кіберпростору. Висунуто гіпотезу, що сучасні норми міжнародного права є недостатніми для ефективного "доведення причетності" держави до кібератак, здійснених третіми акторами, через проблеми атрибуції та брак чітких доказових стандартів. Для перевірки гіпотези застосовано методологію аналізу норм міжнародного права (проєкту статей про відповідальність держав за міжнародно-правові правопорушення 2001 р., актів ООН тощо), прецедентів та сучасних наукових публікацій з цієї проблематики. Проведено порівняльний аналіз критеріїв атрибуції (доктрини "ефективного контролю" та "загального контролю") в класичному міжнародному праві та їх застосування в кіберпросторі. Підтверджено, що анонімність і технічна складність кібероперацій створюють "дилему нормативної невдачі" – тобто ситуацію, за якої держави фактично можуть ухилятися від відповідальності. Встановлено, що для притягнення до відповідальності держав – спонсорів кібератак необхідно удосконалити правові механізми: запровадити чіткіші стандарти доказування причетності, розвивати міжнародне співробітництво в атрибуції, розглянути нові критерії (як-от концепцію "суттєвої підтримки" в атрибуції). Отримані результати сприяють поглибленню теорії міжнародно-правової відповідальності в кіберпросторі та можуть бути використані для формування політик і норм, що унеможливлять безкарне використання кіберпростору для агресії.

Ключові слова: кібератака, міжнародно-правова відповідальність, атрибуція, анонімність, недержавні актори, кібербезпека.

STATE RESPONSIBILITY FOR THIRD-PARTY CYBERATTACKS IN CONDITIONS OF ANONYMITY

The relevance of this research is determined by the rapid increase in the number of cyberattacks carried out indirectly via third-party actors (non-state groups or proxy actors) and the difficulties in holding states accountable for such actions under conditions of the anonymity of cyberspace. A hypothesis has been proposed that current norms of international law are insufficient for effective "proving the involvement" of a state in cyberattacks carried out by third parties, due to attribution issues and a lack of clear evidentiary standards. To verify the hypothesis, a methodology for analysing the international legal norms (including the draft articles on State responsibility for international legal violations of 2001, UN acts, etc.), precedents, and contemporary scientific publications on this issue has been applied. A comparative analysis of attribution criteria (the "effective control" vs. "overall control" doctrines) in classical international law and their application in cyberspace has been conducted. It has been confirmed that the anonymity and technical complexity of cyber operations create a "dilemma of normative failure" – that is, a situation in which states can effectively evade responsibility. It has been established that in order to hold state sponsors of cyberattacks accountable, it is necessary to improve legal mechanisms: to introduce clearer standards for proving involvement, to develop international cooperation in attribution, and to consider new criteria (such as the concept of "substantial support" in attribution). The obtained results contribute to the deepening of the theory of international legal responsibility in cyberspace and can be used to formulate policies and norms that will prevent the unpunished use of cyberspace for aggression.

Keywords: cyberattack, international legal responsibility, attribution, anonymity, non-state actors, cybersecurity.

JEL Classification: K24, K33, F51, F52, K14.

Вступ

У сучасних умовах глобальної цифрової взаємодії кібератаки стали одним з інструментів геополітичного протистояння. Вони можуть завдаватися не лише безпосередньо державними структурами, а й опосередковано – через так званих "третіх акторів". Під такими акторами розуміють недержавних суб'єктів (хакерські групи, кіберзлочинці, "проксі"), яких певна держава таємно використовує для досягнення своїх цілей. Проблема полягає в тому, що держава-ціль часто не може явно довести участь іншої держави в кібератаці, оскільки кіберпростір забезпечує високий рівень анонімності та можливість приховати сліди таких посягань. Як наслідок, виникає прогалина відповідальності: держави – замовники кібератак уникають юридичної відповідальності, посилаючись на недостатність доказів їхньої прямої причетності. Це ставить під загрозу міжнародну безпеку і підриває принцип верховенства права в міжнародних відносинах.

Актуальність цього дослідження зумовлена нагальною потребою міжнародного співтовариства виробити підходи до притягнення держав до відповідальності за шкідливу кібердіяльність. Відсутність належної реакції на кібератаки посилює атмосферу безкарності та заохочує здійснювати подальші приховані операції. Як зазначають дослідники, нині "міжнародне право кібератрибуції майже не розвинене, а норми відповідальності держави залишаються незрозумілими та дискусійними", що робить всю систему реагування на кібератаки слабкою і малоефективною (*Banks*, 2021). Країни – жертви кібератак фактично позбавлені можливості застосувати контрзаходи чи інші легальні засоби захисту, доки не встановлено, яка держава стоїть за атакою. Водночас держави-винуватці користуються анонімністю, щоб уникнути санкцій. Такий стан справ підважує міжнародний правопорядок і потребує наукового осмислення.

Аналіз останніх досліджень показує, що проблема атрибуції кібератак перебуває в центрі уваги як зарубіжних, так і вітчизняних фахівців з міжнародного права та кібербезпеки. Зокрема, *Banks* (2021) звертає увагу на брак чітких міжнародно-правових вимог щодо доказів приписування кібератак державам і закликає держави публічно оголошувати результати атрибуції та спільно виробити стандарти доказування. *Tsagourias* (2024) досліджує політичні та юридичні аспекти атрибуції, скептично оцінюючи ідеї створення міжнародного агентства з атрибуції через небажання держав розкривати свої розвідувальні дані й поступатися суверенітетом. Серед українських дослідників питання відповідальності за кібератаки третьої сторони лише починають висвітлюватися, що зумовлює необхідність розвитку цієї тематики. Невирішеною частиною проблеми залишається визначення такого рівня контролю чи підтримки, за якого дії приватних осіб у кіберпросторі можуть юридично приписуватися державі в умовах непевності й анонімності. Саме цій прогалині й присвячено дослідження.

Метою статті є формулювання теоретично обґрунтованих підходів до вирішення проблеми відповідальності держави за кібератаки, здійснені третіми акторами, крізь призму питання "доведення причетності" в умовах анонімності.

Гіпотеза дослідження полягає в тому, що без адаптації наявних міжнародно-правових підходів держави і надалі зможуть уникати відповідальності за кібератаки, здійснені через проксі. Іншими словами, якщо не будуть розроблені нові правила атрибуції та доказування, то концепція відповідальності держави в кіберпросторі залишатиметься радше теоретичною, ніж дієвою. Для перевірки гіпотези застосовано комплексну методологію. Дослідження базується на загальнонаукових і спеціально-правових методах. Застосовано формально-юридичний метод при аналізі тексту Проєкту статей про відповідальність держав за міжнародно-правові правопорушення (Комісія міжнародного права ООН, 2001) та інших міжнародних документів. Порівняльно-правовий метод використано для зіставлення критеріїв атрибуції, вироблених Міжнародним Судом ООН та іншими трибуналами, з їх потенційною реалізацією в кіберпросторі. Крім того, застосовано кейсовий підхід: проаналізовано показові приклади кібератак (зокрема кібератаки на Естонію 2007 р., намагаючись простежити питання атрибуції; інцидент з Албанією 2022 р. тощо) та реакцію держав на них.

1. Міжнародно-правові засади відповідальності держав за кібератаки

Відповідальність держави в міжнародному праві настає за кожне міжнародно-протиправне діяння, тобто дію або бездіяльність держави, яка порушує її міжнародне зобов’язання (стаття 1 Проєкту статей про відповідальність держав, 2001) (*United Nations General Assembly*, 2001, *July* 26). Класична доктрина чітко визначає дві складові протиправного діяння: 1) наявність факту порушення міжнародного зобов’язання; 2) атрибуція цього діяння конкретній державі. Саме другий елемент – атрибуція (причислення дії суб’єкта до держави) – є ключовим у випадках кібератак з участю третіх акторів. Адже шкода може бути очевидною, але потрібно встановити, чи може вона юридично вважатися вчиненою конкретною державою.

Норми міжнародного права (як закріплено у Проєкті статей про відповідальність держав) передбачають, що державі приписуються дії:

а) органів держави (будь-який орган влади, незалежно від його ролі чи рівня, діє *ipso facto* як держава – стаття 4);

б) осіб чи утворень, які не є органами, але уповноважені державою здійснювати деякі елементи державної влади (стаття 5);

в) інших осіб або груп, які діяли за дорученням, вказівками чи під контролем держави (стаття 8) (*United Nations*, 2001, *July* 26).

Остання норма якраз охоплює ситуації, коли недержавні актори здійснюють дії фактично "в інтересах" або за підтримки певної держави. Однак постає питання: який ступінь контролю чи зв'язку необхідний, щоб дії приватної особи вважалися діями держави?

Міжнародна практика виробила дві основні доктрини щодо критеріїв атрибуції дій недержавних груп державі: доктрину "ефективного контролю" та "загального контролю". Першу сформульовано Міжнародним Судом ООН у справі "Нікарагуа проти США" (1986). Суд встановив, що США не можуть бути притягнуті до відповідальності за всі дії контрас (повстанців) у Нікарагуа, оскільки не доведено повного контролю над ними. Вирішальним критерієм став "ефективний контроль": держава відповідає лише за ті дії недержавних осіб, які вона конкретно наказала здійснити або контролювала в кожному окремому випадку. Інакше кажучи, недержавна група має діяти в режимі "повної залежності" від держави (*International Court of Justice*, 1986, *June* 27), щоб її вчинки були приписані цій державі. Такий поріг є надзвичайно високим і на практиці рідко досяжним – держави зазвичай забезпечують своїм проксі певну автономію, щоб зберегти правдоподібне заперечення.

Другу доктрину – "загального контролю" – застосовано Міжнародним кримінальним трибуналом у справі "Тадіч" (*International Criminal Tribunal for the former Yugoslavia*, 1999, *July* 15) щодо конфлікту в БіГ. Судді визнали, що достатньо показати, що держава організовувала, координувала або загалом підтримувала збройну групу, аби покласти на державу відповідальність за дії цієї групи. Іншими словами, якщо держава відіграє ключову роль у створенні та функціонуванні нелегального збройного формування (постачає зброю, фінансує, віддає загальні накази), то можна стверджувати про "загальний контроль" і відповідальність держави навіть без прямого наказу щодо кожного конкретного порушення. Цей підхід значно знижує бар'єр доказування порівняно з "ефективним контролем". Однак Міжнародний Суд ООН (наприклад у справі "Боснія проти Сербії" 2007 р. (*European Court of Human Rights*, 2007, *July* 12) не прийняв концепцію "загального контролю" як універсальний критерій для відповідальності держав, наполягаючи на більш вузькому тесті "ефективного контролю" для питань державної відповідальності (водночас визнавши, що в кримінально-правовому контексті критерії можуть бути інші). Отже, в міжнародному праві наразі немає одностайності щодо того, яку планку контролю слід застосовувати.

У контексті кібератак ця невизначеність стає особливо проблемною. Анонімність кіберпростору ускладнює встановлення навіть базових фактів про те, хто саме здійснив атаку – державний орган, приватна особа, іноземний хакер (*Прим. автора:* тут і надалі в межах цієї статті вживатиметься узагальнений термін хакер у значенні кіберзлочинець; злочинець в кіберпросторі; кіберфахівець, що здійснює чорний хакінг.) тощо. На відміну від традиційних збройних дій, у кіберпросторі

відсутні однозначні "підписи" державної участі: кіберзброя може бути придбана або сконструйована будь-ким, а атаки проведені з території третіх країн або через мережі інших держав. Тому навіть доведення факту, що за атакою стоїть громадянин *X* країни *Y*, ще не відповідає на питання, чи була причетна держава *Y*. Якщо дотримуватися суворої доктрини ефективного контролю, потрібні докази, що саме органи держави *Y* дали пряму команду *X* атакувати. Зрозуміло, такі докази майже неможливо отримати без доступу до внутрішніх документів або перехоплених наказів, чого атакована держава практично не має. У результаті жодна кібератака проксі-акторів не буде формально атрибутована державі, якщо вимагати стандарту "повної залежності". Наприклад, кібератака на Естонію 2007 р. паралізувала урядові та фінансові вебсайти, і естонські офіційні особи підозрювали участь російської держави, однак відсутність прямих доказів зв'язку між хакерами та російською владою дала змогу державі-терористці заперечувати причетність. Схожа ситуація була під час масованого кібершпигунства проти Грузії та України – дії приписували групам, що базуються на території нашої східної сусідки, але формальної атрибуції державі-спонсору зроблено не було саме через невідповідність жорсткому критерію доказів.

Водночас, за умови застосування підходу "загального контролю" або подібних більш гнучких критеріїв, картина може змінитися. Достатньо було б довести, що держава надавала суттєву підтримку групі хакерів (фінансування, навчання, інфраструктуру) або координувала загальний напрямок їхніх атак. Такі факти встановити легше – нерідко розвідки і приватні компанії виявляють, що інфраструктура для атаки (сервери, програми) пов'язана з організаціями, афілійованими з певною державою, або що атака узгоджується з геополітичними цілями цієї держави. Проте, оскільки міжнародне право поки що однозначно не прийняло стандарт "загального контролю" як критерій державної відповідальності, виникає правовий вакуум. У науковій літературі неодноразово наголошувалося, що класичний режим відповідальності потребує адаптації до реалій кіберпростору (*Cheng & Li*, 2025). Деякі автори прямо пропонують переглянути критерії атрибуції: зокрема, на думку низки дослідників, до кібероперацій варто застосовувати менш суворий поріг, ніж "ефективний контроль", оскільки технічна складність простеження робить його практично нездійсненним (*Levite et al.*, 2022, *March* 28).

2. Виклики атрибуції кібератак в умовах анонімності

Кіберпростір надає зловмисникам безпрецедентні можливості сховати свою особу та справжнє джерело атаки. Анонімність є властивістю, вбудованою в архітектуру інтернету: пакети даних можуть проходити через десятки мереж у різних країнах, використовуючи технології маскування (*VPN*, проксі-сервери, анонімайзери, мережі *Tor*).

Хакери часто фальсифікують цифрові сліди, використовуючи *IP*-адреси інших держав або викрадені сервери, щоб заплутати слідство. Це явище називають "обфускація" – навмисне ускладнення відстеження, аж до імітації почерку іншого відомого хакера чи групи (*Sepich*, 2023, *April* 19). Отже, суто технічна атрибуція (визначення того, звідки і ким здійснено атаку) є нетривіальним завданням, що потребує значних ресурсів, часу та експертизи.

Як наслідок, держави, які стали жертвами кібератак, опиняються перед дилемою: вони можуть підозрювати конкретного противника, але збирати переконливі докази доводиться протягом тривалого часу. Наприклад, складну кібершпигунську операцію *SolarWinds* 2020 р. (злам низки американських відомств) виявили лише випадково, і тільки за декілька місяців фахівці дійшли висновку про причетність російських хакерських груп й оприлюднили атрибуцію до рф на рівні уряду США. Інший випадок – кібератака 1998 р. на американські мережі: спочатку Вашингтон помилково припустив участь Іраку (через політичний контекст), але зрештою з'ясувалося, що винуватцями були два підлітки з Каліфорнії та один з Ізраїлю (*Sepich*, 2023). Цей приклад показує небезпеку поспішної або хибної атрибуції: неправильно звинувативши державу, можна спровокувати конфлікт на хибній підставі. Отже, держави змушені діяти обережно, часто уникаючи відкритого обвинувачення без "залізних" доказів.

Політичний аспект також відіграє роль: коли держава все ж має технічні докази, вона може вагатися, чи оприлюднювати їх. Причини різні: розкриття деталей може викрити джерела розвідки або методи, якими ці докази здобуто (наприклад зламані сервери противника або секретні програми спостереження). Як зазначає *Tsagourias* (2024), держави вважають атрибуцію суверенним прерогативом і здійснюють її лише тоді, коли це відповідає їхнім інтересам. Більше того, навіть якщо держави роблять публічні заяви про причетність іншої країни до кібератаки, вони неохоче розкривають докази, на яких базуються їхні слова. У 2015 р. Група урядових експертів ООН зауважувала, що "звинувачення у вчиненні протиправних дій повинні бути обґрунтовані доказами" (*The Hague Program for Cyber Norms, n. d.*). Проте на практиці держави заявляють, що не мають юридичного обов'язку надавати доказову базу своїх звинувачень (*Tsagourias*, 2024). Як наслідок, обвинувачена держава завжди може поставити під сумнів заяву, назвавши її політично мотивованою чи недостатньо підтвердженою. Так виникає ситуація "слово проти слова", де навіть союзники можуть вимагати переконливішої інформації, щоб підтримати звинувачення. Відомо, що у випадках публічної атрибуції (наприклад, коли США та країни ЄС звинувачували КНДР у зламі *Sony Pictures* у 2014 р. чи російську державу у втручанні у вибори 2016 р.) докладні докази часто залишалися засекреченими. Це, з одного боку, убезпечує джерела, а з іншого – "не сприяє виробленню спільного розуміння стандартів доказування" в міжнародному співтоваристві (*Banks*, 2021).

Особливо складною є ситуація, коли відбувається "атрибуційна війна" – взаємне заперечення і звинувачення. Яскравий приклад – серія кібератак на урядові сайти Албанії у 2022 р. Албанський уряд, за допомогою експертів з країн-партнерів, оперативно відніс ці атаки до дій, "організованих і спонсорованих" Іраном, заявивши про це з упевненістю "поза будь-яким сумнівом". У відповідь Іран рішуче відкинув обвинувачення, назвавши їх "необґрунтованими" і наголосивши, що з огляду на природу кіберпростору "існують серйозні виклики атрибуції в ІКТ-середовищі", застерігаючи від "негативних наслідків сфабрикованих звинувачень" (*Tsagourias*, 2024). Цей випадок показує: навіть за наявності, здавалося б, потужних доказів (настільки, що Албанія пішла на розрив дипломатичних відносин з Іраном), обвинувачена держава все одно може посіяти сумнів, апелюючи до об'єктивних труднощів атрибуції. Атрибуція перетворюється на політичний процес, де кожна сторона намагається переконати міжнародну аудиторію у своїй правоті. Відсутність загальновизнаних правил та інституцій для незалежної перевірки таких звинувачень означає, що правова площина змішується з політичною, а питання відповідальності залишається невирішеним.

Отже, виклики анонімності в кіберпросторі мають кілька вимірів.

Технічний: складність встановлення джерела атаки та особи нападника (через обфускацію, використання чужих інфраструктур, складність трасування).

Доказовий: навіть за ідентифікації ймовірного винуватця, брак прямого сліду до органів держави; висока планка доказування контролю чи наказу держави.

Політичний: небажання держав розкривати всю інформацію; використання атрибуції як інструменту політичного тиску; ризик помилкової атрибуції.

Правовий: відсутність узгоджених міжнародних процедур чи форуму для підтвердження атрибуції (наприклад, немає спеціального міжнародного трибуналу з кіберінцидентів; Міжнародний Суд ООН теоретично може розглядати позов про кібератаку, але для цього потрібна згода держави – відповідача на юрисдикцію Суду, чого на практиці важко досягти).

Комбінована дія цих факторів призводить до того, що сучасна система міжнародного права поки що "слабко реагує на кібератаки" (*Banks*, 2021). Деякі експерти, зокрема й *Banks* (2021), характеризують кіберпростір як "Дикий Захід" (*Wild West*) у сенсі правового регулювання, де відсутність неминучого покарання породжує нові напади. За таких умов виникла нагальна потреба у вдосконаленні механізмів доведення причетності та притягнення до відповідальності.

3. Підходи до "доведення причетності" та вдосконалення міжнародно-правових механізмів

Стикаючись із наведеними труднощами, міжнародне співтовариство поступово формулює норми та принципи, покликані зменшити простір для безкарної анонімності. Хоча обов'язкових до виконання спеціальних договорів про кібератаки наразі немає, м'яке право та політичні зобов'язання держав починають заповнювати цю нішу. Важливим кроком стала консенсусна доповідь Групи урядових експертів ООН (*GGE*) 2015 р., де прямо зазначено: "Держави не повинні використовувати проксі для здійснення міжнародно-протиправних дій з використанням ІКТ і мають уживати заходів, щоб їхня територія не використовувалась недержавними акторами для таких дій" (*The Hague Program for Cyber Norms, n. d.*). Ця норма фактично встановлює політичне зобов'язання двоякого роду: заборона державам використовувати "пішаки" (наприклад хакерів-найманців) для кібератак, а також позитивний обов'язок держави не допускати, щоб з її території діяли кіберзлочинці, що атакують інші країни. Хоча формально рекомендація *GGE* є добровільною, її підтримали всі великі держави і вона відображає очікування міжнародної спільноти. У 2021 р. наступна *GGE* знову підтвердила цей принцип. Отже, навіть якщо важко довести, що держава контролювала хакерів, є інша підстава вимагати відповідальності – держава не виконала свій обов'язок належної сумлінності (*due diligence*) у запобіганні атакам зі своєї території. Принцип *due diligence* походить ще з рішення Міжнародного Суду у справі "Корфу" (1949), де йшлося, що держава має не допускати використання своєї території на шкоду іншим. У кіберконтексті це означає: якщо держава знала (або повинна була знати) про діяльність хакерської групи на своїй території і нічого не вчинила, її можуть вважати співвідповідальною за завдану шкоду. Хоча на практиці довести знання чи бездіяльність держави також непросто, цей механізм зменшує залежність від атрибуції: достатньо встановити факт, що атака фізично йшла з ресурсів на території держави *X* і що *X* не допомогла її зупинити. Наприклад, у випадку масових *ransomware*-атак 2021 р. (на кшталт *Colonial Pipeline* у США) американська сторона поставила вимогу до російської держави як до країни, де орудували групи здирників, вжити заходів проти них, вказуючи, що невиконання такого обов'язку буде розцінено негативно.

Другий підхід – підвищення прозорості та співпраці в атрибуції. У відповідь на проблему, що держави не діляться доказами, з'являються ініціативи зі створення міжнародних платформ обміну інформацією про кібератаки. Одна з ідей – заснувати міжнародне агентство з атрибуції, яке б незалежно розслідувало великі кіберінциденти і робило авторитетний висновок щодо винуватців. На перший погляд, це схоже на моделі в інших сферах (наприклад МАГАТЕ в ядерній галузі або Спільний механізм ООН-ОЗХЗ з розслідування хімічних атак у Сирії).

Проте дослідники скептично оцінюють реалізовність такої ідеї у кіберсфері. *Tsagourias* (2024) зазначає низку проблем: небажання держав поступатися суверенітетом і дозволяти зовнішнім агентствам "копатися" в їхніх мережах; ризик розкриття чутливої інформації; складність досягнення згоди щодо того, які повноваження матиме таке агентство. Потенційно потужні держави або бойкотуватимуть, або обмежуватимуть мандат такої установи, щоб захистити власні кібертаємниці. До того ж, як слушно зауважено науковцем, стандарти доказування досі різняться – немає єдиного критерію (на кшталт "поза розумним сумнівом" чи "високого ступеня ймовірності"), що приймався б усіма сторонами для кіберінцидентів. Без цього навіть висновки агентства можуть оскаржуватися окремими державами. Тому, принаймні у короткостроковій перспективі, більш реалістичним є розширення добровільного міждержавного співробітництва: створення коаліцій з розслідування (як це відбувається вже зараз у форматі спільних заяв кількох союзників щодо атрибуції певної атаки), обмін даними між національними командами реагування на інциденти (*CERT*), спільні кібернавчання тощо. В таких умовах держави, що технологічно відстають, можуть отримати допомогу від партнерів у встановленні винних, а відповідні заяви будуть більш легітимними, якщо їх підтримує багато країн.

Третій напрям – адаптація правових критеріїв атрибуції під реалії кібероперацій. Якщо повернутися до доктрин "ефективного" і "загального контролю", в науці дедалі частіше лунає думка, що вони є двома точками спектра, а не взаємозаперечними опціями. Деякі автори пропонують проміжні або комбіновані критерії. Так, китайські дослідники *Cheng* та *Li* (2025) вводять концепцію "суттєвої підтримки" як критерію: якщо держава надала приватній групі хакерів суттєві ресурси чи переваги, що зробили можливою або значно посилили атаку, цього може бути достатньо для атрибуції відповідальності. Простіше кажучи, навіть якщо держава прямо не керувала кожним кроком, але створила умови для атаки (дала техніку, фінанси, доступ до мереж), вона має нести відповідальність поряд із виконавцями. Ця пропозиція фактично є розвитком ідеї "співучасті" держави (*aider and abettor*) у чужому правопорушенні.

У класичному міжнародному праві є норма про заборону державі надавати допомогу або підтримку в здійсненні правопорушення іншою державою (стаття 16 Проєкту статей). У кіберсфері ж пропонується притягати державу за допомогу недержавним суб'єктам. Наприклад, якщо з'ясується, що спецслужби держави *A* передали хакерам інформацію про вразливості систем держави *B*, які ті потім використали для атаки, – держава *A* могла б бути відповідальною на підставі "суттєвої підтримки", навіть якщо не віддавала наказу атакувати. Такий підхід, безумовно, полегшить доведення причетності, бо залишає менше простору для маневру: державам-спонсорам доведеться або повністю відмовляти в будь-якій підтримці хакерам, або ризикувати бути викритими.

Низка експертів також наголошує на необхідності розробити чіткі стандарти доказів і рівень впевненості, потрібний для міжнародно-правової атрибуції. Зараз кожна держава де-факто вирішує сама, який обсяг доказів вважає достатнім, щоб публічно звинуватити іншу в кібератаці. Відсутність узгодженості веде до різних практик: одні країни пред'являють технічні звіти, інші обмежуються загальними заявами. Уявна "шкала впевненості" коливається від дуже низької (лише підозра) до майже повної (заснованої на секретних даних розвідки). Для підвищення довіри деякі дослідники пропонують встановити спільний режим розкриття доказів: наприклад, публікувати індикатори компрометації (*IoC*) атак, хеші шкідливого ПЗ, маршрути, залучені *IP* – тобто технічну інформацію, яку можуть перевірити незалежні експерти (*Tsagourias*, 2024). Це б дозволило світовій спільноті самостійно оцінити атрибуцію, а не сприймати її як політичну заяву. Звичайно, частина даних (зокрема розвідувальні джерела) лишатиметься закритою, але хоча б мінімальний прозорий пакет доказів міг би стати новим стандартом. У 2015 р. та ж доповідь *GGE* зазначила: факт, що атака ніби "почалася з території держави *X*", сам по собі не є доказом вини держави *X* (*The Hague Program for Cyber Norms, n. d.*). Тому просто вказати на чужий *IP* недостатньо, треба обґрунтувати зв'язок із державною політикою або органами. Це теж свого роду керівництво для доведення причетності.

Практична реалізація нових підходів поки відбувається повільно, але деякі тенденції додають оптимізму. По-перше, дедалі більше держав публічно визнають, що міжнародне право поширюється на кіберпростір, і намагаються конкретизувати як. Наприклад, низка західних країн оприлюднила національні позиції, де прямо згадується відповідальність держав за кібератаки та допускається застосування контрзаходів у відповідь на кіберправопорушення. Це створює прецеденти політичної волі не залишати інциденти без наслідків. По-друге, співпраця з приватним сектором (зокрема з великими *IT*-компаніями та кібербезпековими фірмами) допомагає отримувати докази. Неурядові актори, такі як компанія *Microsoft* чи лабораторії *Mandiant*, нерідко самі проводять атрибуцію складних атак і називають винуватців – іноді навіть раніше за уряди. Хоча їхні звіти не мають статусу офіційного міжнародно-правового доказу, вони формують суспільне сприйняття і створюють тиск на уряди з метою визнати факти. Нерідко держави спираються на такі розслідування, щоб зробити офіційний висновок. У такий спосіб розширюється багатостороннє коло суб'єктів атрибуції, що сприяє об'єктивності.

По-третє, триває робота в рамках ООН: окрім *GGE*, з 2019 р. функціонує Відкритий робочий механізм (*Open-Ended Working Group*, *OEWG*), де всі держави можуть обговорювати питання міжнародної інформаційної безпеки. У своєму звіті 2021 р. *OEWG* закликав продовжувати діалог щодо застосування міжнародного права в кіберпросторі та згадав про необхідність мирного вирішення спорів і дотримання

суверенітету в ІКТ-середовищі (*Schmitt*, 2021, *June* 10). Хоча конкретних нових норм *OEWG* не запропонував, сам факт багаторазового підтвердження принципів (нерозповсюдження конфлікту, неприпустимості втручання) формує очікування відповідальної поведінки. Це означає, що держава, причетна до кібератаки, все більше ризикує отримати негативні політичні та репутаційні наслідки.

Загалом можна окреслити кілька перспективних напрямів удосконалення. Розвиток звичаєвих норм: поступове перетворення рекомендацій *GGE* (про заборону проксі, *due diligence*) на загальновизнані звичаї, обов'язкові для всіх держав. Якщо більшість держав буде їх дотримуватися і посилатися на них, порушники нестимуть репутаційні втрати і матимуть менше підтримки.

Зміна підходу судових інстанцій: у разі, якщо справа про кібератаку коли-небудь дійде до Міжнародного Суду ООН чи арбітражу, ці органи можуть використати шанс уточнити критерії атрибуції в кіберпросторі – можливо, відійти від буквалізму "ефективного контролю" і врахувати специфіку кібероперацій. Таке рішення стало б прецедентом.

Перегляд проєкту статей про відповідальність: теоретично, в майбутньому *ILC* могла б доповнити статті 2001 р. коментарями щодо кіберпростору або навіть новими положеннями (наприклад окремою статтею про відповідальність за кібератаки, здійснені недержавними акторами). Поки цього не сталося, але тема обговорюється серед юристів-міжнародників.

Міжнародні договірні ініціативи: деякі держави пропонують укласти глобальну або багатосторонню угоду про правила поведінки в кіберпросторі. Якби в такому документі прописали обов'язок співпраці в атрибуції, обміні інформацією, можливо, навіть створили механізм розслідування, це стало б значним прогресом. Наразі позиції держав (особливо кібердержав на кшталт США, росії, Китаю) щодо такого договору різняться, тому його перспектива туманна. Водночас ідеї "Паризького заклику" 2018 р., "Норм поведінки в кіберпросторі" від груп експертів тощо – це кроки до спільних рамок.

Розширення публічної атрибуції: експерти радять державам частіше робити спільні публічні заяви про винуватців кібератак, за можливості супроводжуючи їх доказами (*Banks*, 2021). Така публічність виконує дві функції: з одного боку, стримує потенційних агресорів (бо вони бачать, що їх викриють і їм доведеться реагувати на звинувачення), з іншого – легітимує відповідні дії жертви (наприклад контрзаходи чи санкції) в очах міжнародної спільноти. Іншими словами, прозора атрибуція робить відповідальність більш реальною.

Підсумовуючи, можна сказати, що механізм "доведення причетності" у випадках кібератак лише формується. На перехідному етапі міжнародне право стикається з "дилемою нормативної невдачі" (*Cheng & Li*, 2025), коли наявні правила не дають чіткого результату. Але розуміння проблеми та накопичення практики поступово прокладають шлях до нових рішень.

Висновки

Проведене дослідження підтвердило, що чинний міжнародно-правовий режим не забезпечує ефективного механізму притягнення держав до відповідальності за кібератаки, здійснені третіми акторами. Критерій "ефективного контролю" встановлює надмірно високий стандарт доказування, що в умовах кіберпростору майже неможливо реалізувати. Як наслідок, держави – спонсори кібератак успішно приховують свою причетність, використовуючи технології анонімізації та правові прогалини. Відсутність узгоджених міжнародних процедур атрибуції значно ускладнює реалізацію жертвами кіберінцидентів свого права на контрзаходи та самооборону, а також сприяє збереженню безкарності у кіберсфері.

Водночас у міжнародній практиці простежуються позитивні зрушення – формування політичних зобов'язань щодо заборони використання проксі-акторів, вимог до належної сумлінності держав та пошуку нових критеріїв атрибуції, зокрема на основі концепції "суттєвої підтримки". Для розв'язання цих проблем запропоновано низку нових підходів. Зокрема, рекомендується запровадити гнучкіші критерії атрибуції – наприклад проміжний стандарт "суттєвої підтримки", що дозволяє приписати відповідальність державі, яка надає суттєву підтримку недержавним акторам, навіть без прямого "ефективного контролю". Одночасно необхідно розробити спільні стандарти доказування та прозорості при публічній атрибуції (наприклад публікацію технічних індикаторів кібератак і залучення незалежних експертів) та посилити роль міжнародних інституцій і співпрацю з приватним сектором у розслідуваннях інцидентів. Реалізація цих заходів може перевести питання відповідальності за кібератаки з гіпотетичної площини у практичну й поступово приборкати нинішній "Дикий Захід" у кіберпросторі. Загалом формування ефективного режиму атрибуції та відповідальності потребує консолідації політичної волі держав і оновлення правових доктрин, адже лише так можна забезпечити безпечне та стабільне цифрове майбутнє.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCE

Banks, W. C. (2021). Cyber attribution and state responsibility. *International Law Studies*, *97*(1), 1039–1072. https://digital-commons.usnwc.edu/ils/vol97/iss1/43

Cheng, L., & Li, H. (2025). *State responsibility in the context of cyberwarfare: dilemma identification and path reconstruction.* https://www.degruyterbrill.com/document/doi/10.1515/ijld-2025-2005/html

European Court of Human Rights. (2007, July 12). *Case of Jorgić v. Germany* (Application no. 74613/01), Judgment. https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-117698&filename=CASE%20OF%20JORGIC%20v.%20GERMANY%20-%20%5BUkrainian%20Translation%5D%20by%20the%20COE%20Human%20Rights%20Trust%20Fund.docx

International Court of Justice. (1986, June 27). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Merits Judgment. https://www.icj-cij.org/case/70

International Criminal Tribunal for the former Yugoslavia. (1999, July 15). *Prosecutor v. Dusko Tadić.* Appeals Chamber Judgment. https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

Levite, A. E., Lu, C., Perkovich, G., & Yang, F. (2022, March 28). *Managing U.S. – China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/03/28/managing-u.s.-china-tensions-over-public-cyber-attribution-pub-86693

Schmitt, M. (2021, June 10). *The Sixth United Nations GGE and International Law in Cyberspace*. https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

Sepich, J. (2023, April 19). *The evolution of cyber attribution.* American University, Center for Security, Innovation & New Technology. https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm

The Hague Program for Cyber Norms. (n. d.). *Cumulative Recommendations in the UN GGE Reports (2010–2015).* https://www.thehaguecybernorms.nl/cumulative-recommendations-in-the-un-gge-reports

Tsagourias, N. (2024). *Cyber Attribution Agencies: A Sceptical View.* https://www.qil-qdi.org/cyber-attribution-agencies-a-sceptical-view/

United Nations General Assembly. (2001, July 26). *Responsibility of States for Internationally Wrongful Acts: Titles and Texts of the Draft Articles.* https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

Конфлікт інтересів. Автор заявляє, що не має фінансових чи нефінансових конфліктів інтересів щодо цієї публікації; не має відносин із державними органами, комерційними або некомерційними організаціями, які могли б бути зацікавлені у поданні цієї точки зору. З огляду на те, що автор працює в установі, яка є видавцем журналу, що може зумовити потенційний конфлікт або підозру в упередженості, остаточне рішення про публікацію цієї статті (включно з вибором рецензентів та редакторів) приймалося тими членами редколегії, які не пов'язані з цією установою.

Автор не отримувала фінансування для цього дослідження. Дослідження здійснено за кошти автора та з її власної ініціативи.

Звєрєва, К. (2025). Відповідальність держави за кібератаки третіх сторін в умовах анонімності. *Зовнішня торгівля: економіка, фінанси, право*. Серія. Юридичні науки, *3*(140), 32–44. https://doi.org/ 10.31617/3.2025(140)03

Надійшла до редакції 16.07.2025.
Прийнято до друку 26.08.2025.
Публікація онлайн 16.09.2025.