Наконечна І.,
доктор юридичних наук, доцент,
професор кафедри загальноправових дисциплін,
Національна академія Служби безпеки України
(м. Київ, Україна)

Бондаренко С.,
фахівець кафедри технологій захисту кіберпростору центру кібербезпеки,
Національна академія Служби безпеки України,
член громадської організації «IESF»
(м. Київ, Україна)

РОЛЬ МІЖНАРОДНОГО ПРАВА У ФОРМУВАННІ НАЦІОНАЛЬНОЇ ПОЛІТИКИ КІБЕРЗАХИСТУ: МІЖ СТВОРЕННЯМ НОРМ І СТРАТЕГІЧНОЮ ДВОЗНАЧНІСТЮ

Сучасний геополітичний і технологічний ландшафт підняв кіберпростір до сфери стратегічного значення, порівнянної за вагою з землею, морем, повітрям і космічним простором. У цьому контексті роль міжнародного права у формуванні національної політики кіберзахисту постає не лише як питання правової теорії, але й як актуальне питання національної безпеки та міжнародної стабільності. Незважаючи на швидке поширення фінансованих державою кібероперацій, критичної вразливості інфраструктури та сценаріїв гібридних конфліктів, які розгортаються в цифровому середовищі, міжнародна правова система залишається викликом через sui generis характер кіберпростору [3].

Він характеризується відсутністю кордонів, множинністю користувачів, асиметрією можливостей, а також швидкістю та анонімністю шкідливих дій. У рамках цієї парадигми міжнародне право покликане виконувати подвійну і часто суперечливу функцію: діяти в якості основи для розробки та кодифікації нормативних обмежень щодо поведінки держав у кіберпросторі та одночасно враховувати стратегічні неоднозначності, які держави використовують для збереження свободи маневру та оперативної гнучкості своїх національних позицій кіберзахисту.

Основоположні принципи Статуту ООН – суверенна рівність, невтручання, заборона застосування сили та мирне вирішення суперечок – залишаються застосовними в кіберпросторі, як підтверджено кількома звітами Групи урядових експертів ООН (англ. GGE) і Робочої групи відкритого складу

(англ. OEWG) [2, с. 15]. Однак застосування цих принципів до конкретних кіберінцидентів пов'язане з невизначеністю тлумачення. Поріг, за яким кібероперація вважається застосуванням сили або збройним нападом згідно зі статтею 2 (4) і статтею 51 Статуту ООН, залишається юридично недостатньо розробленим і політично спірним.

Подібним чином принцип відповідальності держави та правила щодо контрзаходів і необхідності, кодифіковані відповідно до статей про відповідальність держав за міжнародно-протиправні діяння (англ. ARSIWA), намагаються досягти ясності в аналізі приписування та пропорційності, необхідному для кіберпростору. Таким чином, держави опиняються в зоні правової неоднозначності, де відсутність остаточних обов'язкових норм заохочує побудову стратегічних доктрин, які охоплюють потенціал кібероперацій без чіткої юридичної кваліфікації.

Ця діалектика між нормотворенням і стратегічною двозначністю розкриває глибшу структурну особливість міжнародного права в кіберконтексті: повільний і політично обумовлений характер законотворчості на міжнародному рівні контрастує зі швидким розвитком технічних можливостей і векторів загроз у кіберпросторі. Хоча такі ініціативи, як Талліннські посібники, Паризький заклик до довіри та безпеки в кіберпросторі та регіональні інструменти, такі як Закон ЄС про кібербезпеку чи Будапештська конвенція про кіберзлочинність, сприяли поступовому роз'ясненню застосовних норм, вони залишаються необов'язковими, специфічними для окремих секторів або регіонально фрагментованими.

Більше того, добровільний і заснований на консенсусі характер процесів розробки кібернорм на базі ООН гарантує, що будь-який прогрес здійснюється через політичний компроміс, часто за рахунок юридичної точності та можливостей виконання. У такому середовищі національна політика кіберзахисту, спрямована на захист суверенітету, стримування супротивників, захист критичної інфраструктури та забезпечення безпеки інформаційного простору, як правило, формулює неоднозначні стратегічні доктрини, які є правдоподібними, але навмисно розпливчастими. Вони вибірково посилаються на міжнародне право, щоб легітимізувати певну практику, зберігаючи при цьому свободу дій для превентивних, прихованих або кіберзаходів у відповідь, правова основа яких не завжди повністю розроблена.

Крім того, на перетин міжнародного права та кіберзахисту все більше впливають конкуруючі нормативні бачення цифрового суверенітету, глобального управління та ролі недержавних акторів у формуванні кібернорм [1]. З одного боку, західні ліберальні демократії виступають за заснований на правилах міжнародний кіберпорядок, заснований на існуючому міжнародному праві та стандартах прав людини. З іншого боку, авторитарні або гібридні режими сприяють суверенному контролю над цифровою інфраструктурою, контентом і кібероперaціями під прапором державоцентричного тлумачення міжнародного права. Ці суперечливі підходи поглиблюють фрагментацію правового режиму та сприяють нормативній гонці озброєнь у кіберпросторі, де міжнародне право стає інструментом не лише дотримання правових норм,

але й стратегічного впливу. У цьому контексті національні політики кіберзахисту відображають ширші ідеологічні та геополітичні узгодження, використовуючи мову міжнародного права для просування національних інтересів, зберігаючи при цьому достатню правову двозначність, щоб уникнути обмежень, які можуть перешкоджати стратегічним варіантам реагування.

Напруга між нормативністю та двозначністю виявляється найгостріше у формулюванні національної політики кіберзахисту, яка все більше ґрунтується на принципах міжнародного гуманітарного права, права прав людини та загальних принципів міжнародної відповідальності, але залишається під впливом політичних і військових імперативів, які протистоять відкритим юридичним обмеженням. Держави часто вибірково посилаються на міжнародне право, щоб узаконити кібероперації, приписати ворожі дії або виправдати контрзаходи, водночас зберігаючи оперативну непрозорість і зберігаючи дискреційний простір для наступальних і превентивних кіберпозицій. Ця подвійність вказує на формувальну парадигму, згідно з якою міжнародне право не є ані повністю визначальним, ані абсолютно нерелевантним, а функціонує як поле юридично-політичного змагання, в якому державні та недержавні актори домовляються про повноваження щодо тлумачення та стратегічну легітимність. У цьому контексті міжнародне право не просто накладає обов'язкові зобов'язання, але функціонує як основа для формування очікувань, структурування відповідей і створення коаліцій, таким чином слугуючи як нормативним, так і інструментальним цілям в архітектурі кіберзахисту.

Крім того, нами підкреслюється, що національна політика кіберзахисту більше не розробляється ізольовано, а вбудовується в транснаціональні мережі правового тлумачення, технічної стандартизації та багатосторонньої дипломатії. Юридичний вимір кіберзахисту за своєю суттю гібридизований — переплітає жорстке право з м'яким правом, політичні зобов'язання з технічними протоколами та етичні норми з оперативними доктринами. У цьому відношенні дотримання міжнародного права в кіберпросторі залежить не лише від вірності тексту, а й від стратегічного сигналу, нормативного узгодження та геополітичного розрахунку. Отже, юридична визначеність і ефективність роботи повинні постійно збалансовуватися з плинністю технологічних інновацій і мінливістю міжнародних відносин. Стратегічна неоднозначність, яка зберігається багатьма державами, є не просто функцією правових прогалин, а й навмисною тактикою для стримування супротивників, управління ризиками ескалації та збереження свободи маневру в спірному цифровому просторі битви, який швидко розвивається [4].

Зрештою, автори роблять висновок, що майбутнє міжнародного права в національній політиці кіберзахисту залежить від здатності міжнародної спільноти узгодити нормативні вимоги правового порядку зі стратегічними імперативами національної безпеки. Це вимагатиме активізації багатосторонньої взаємодії, розробки спільних механізмів приписування, зміцнення юридично-технічної експертизи та розвитку довіри за допомогою

заходів прозорості та інструментів зміцнення довіри. Хоча міжнародне право не може усунути неоднозначності, властиві кіберконфлікту, воно може забезпечити процедурну легітимність і нормативну основу, необхідну для обмеження шкідливої поведінки, запобігання ескалації та інституціоналізації кіберпорядку, заснованого на правилах. У цьому сенсі міжнародне право є не просто пасивним відображенням поведінки держави, а активним компонентом у побудові відповідальної, стійкої та стратегічно узгодженої національної політики кіберзахисту.

З цього випливає, що міжнародне право відіграє незамінну, але за своєю суттю обмежену роль у формулюванні національних стратегій кіберзахисту. Він забезпечує нормативну основу для формулювання допустимої поведінки, але йому бракує інституційних механізмів примусового виконання та одностайності тлумачення, щоб функціонувати як остаточний регулятор кіберконфлікту. У результаті міжнародне право в кіберпросторі існує в стані динамічної напруги між прогресивним розвитком норм і збереженням двозначності як стратегічного активу. Майбутній розвиток цієї правової сфери залежатиме від взаємодії між державною практикою, opinio juris, технологічним розвитком та розбудовою інституційної спроможності.

Підвищення правової ясності без руйнування стратегічних потреб національної оборони вимагатиме сприяння більшому багатосторонньому консенсусу, розширення повноважень міжнародних судових або квазісудових органів для розгляду кіберспорів та інтеграції технічної експертизи у формування правових норм. Поки такий режим не дозріє, співіснування нормативності та двозначності залишатиметься визначальною рисою міжнародно-правового регулювання кіберзахисту, що змушуватиме держави орієнтуватися на цій території як із юридичною витонченістю, так і зі стратегічною обережністю.

Список використаних джерел

1. Broeders D., Cristiano F. Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road. *SSRN Electronic Journal*. 2020. URL: https://doi.org/10.2139/ssrn.3819171 (дата звернення: 18.04.2025).

2. Moynihan H. The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*. 2020. С. 1–17. URL: https://doi.org/10.1080/23738871.2020.1832550 (дата звернення: 18.04.2025).

3. Raymond M. Social Practices of Rule-Making for International Law in the Cyber Domain. *Journal of Global Security Studies*. 2020. URL: https://doi.org/10.1093/jogss/ogz065 (дата звернення: 18.04.2025).

4. Why the World Needs an International Cyberwar Convention - Philosophy & Technology. *SpringerLink*. URL: https://link.springer.com/article/10.1007/s13347-017-0271-5 (дата звернення: 18.04.2025).