DOI https://doi.org/10.36059/978-966-397-601-3-164

КОНЦЕПЦІЯ СУВЕРЕНІТЕТУ В КІБЕРПРОСТОРІ ТА ВІДПОВІДАЛЬНІСТЬ ДЕРЖАВИ ЗА НЕПРИПИНЕННЯ ШКІДЛИВОЇ КІБЕРДІЯЛЬНОСТІ

Олександр ПАСЕШНИК
аспірант кафедри міжнародного, цивільного та комерційного права
Державний торговельно-економічний університет
м. Київ, Україна

Швидке розширення цифрових технологій зумовило не лише трансформацію економічних, політичних і безпекових процесів, а й появу нових викликів для міжнародного права. Кіберпростір давно перестав бути суто технічним середовищем обміну інформацією. Сьогодні він є сферою здійснення владних функцій, функціонування критичної інфраструктури, зв'язку, оборони, фінансової стабільності та публічних послуг. За таких умов дедалі більшої ваги набуває питання про те, як саме слід розуміти суверенітет держави в кіберпросторі та чи може держава нести міжнародно-правову відповідальність за бездіяльність у випадках, коли з простору під її юрисдикцією здійснюється шкідлива кібердіяльність проти інших держав.

На сучасному етапі вже майже не викликає сумнівів, що міжнародне право застосовується до поведінки держав у кіберпросторі. Цей підхід відображений як у документах Організації Об'єднаних Націй, так і в офіційних позиціях окремих держав. Водночас набагато складнішим є питання про зміст конкретних міжнародно-правових наслідків такої застосовності. Одним із найбільш дискусійних і практично значущих питань є межі відповідальності держави у разі, коли вона не припиняє шкідливу кібердіяльність, що виходить із її території або з інфраструктури, яка перебуває під її юрисдикцією[1].

У класичному міжнародно-правовому розумінні суверенітет держави пов'язується з її верховенством у межах власної території та незалежністю у зовнішніх відносинах. Проте в цифрову епоху зміст цієї категорії потребує уточнення. Територія держави вже не може сприйматися лише як фізичний простір. Вона охоплює також цифрову інфраструктуру, що функціонує в межах її юрисдикції: мережі, сервери, центри обробки даних, платформи та інші технологічні компоненти. Саме через ці компоненти сьогодні можуть виникати серйозні загрози для інших держав, навіть якщо формально вони не супроводжуються фізичним вторгненням через державний кордон.

[1] Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Report. UN Doc. A/76/135. 2021. P. 17.

У зв'язку з цим суверенітет у кіберпросторі має не лише захисний, а й зобов'язальний вимір. З одного боку, він означає право держави здійснювати юрисдикцію над цифровою інфраструктурою, особами та діяльністю у межах її території. З іншого боку, він передбачає, що така держава не може повністю абстрагуватися від того, як саме використовується відповідний цифровий простір. Якщо з її території систематично здійснюється шкідлива кібердіяльність, що завдає істотної шкоди іншій державі, проблема набуває вже не лише технічного, а й міжнародно-правового характеру. Тому сучасна доктрина дедалі частіше пов'язує суверенітет у кіберпросторі з обов'язком належної обачності та недопущення використання власної території як джерела серйозної кіберзагрози[2].

Разом із тим слід чітко розмежовувати відповідальність держави за власну участь у шкідливій кібероперації та відповідальність за неприпинення такої діяльності. У першому випадку йдеться про пряму атрибуцію дій державі. У другому випадку предметом правової оцінки є саме бездіяльність, тобто невиконання обов'язку належно реагувати на ситуацію, коли шкідлива кібердіяльність уже відбувається або є очевидною загрозою. Така постановка питання є особливо важливою, оскільки в кіберпросторі не кожна атака безпосередньо здійснюється державними органами. Нерідко шкідливу активність реалізують недержавні актори, приватні групи, кримінальні мережі або напівформальні структури, які використовують інфраструктуру, розміщену на території певної держави. Це не означає, що держава автоматично відповідає за будь-який такий інцидент. Однак це не означає, що вона повністю звільняється від міжнародно-правових обов'язків.

Ключове значення має характер обов'язку держави. У сучасному розумінні йдеться не про абсолютний обов'язок гарантувати повну відсутність будь-якої шкідливої кібердіяльності з її території. Такий стандарт був би нереалістичним і не відповідав би реальним технічним можливостям навіть найбільш розвинених держав. Держава повинна вживати заходів, які є для неї об'єктивно доступними, юридично можливими та розумно очікуваними за конкретних обставин. Це означає, що міжнародно-правове значення має не сам по собі факт походження шкідливої активності з певної юрисдикції, а те, як держава поводилася після того, як дізналася або повинна була дізнатися про таку діяльність[3].

У практичному вимірі зміст цього обов'язку може бути різним залежно від масштабу інциденту, технічної спроможності держави, характеру загрози та наявності достовірної інформації. Йдеться, зокрема, про реагування компетентних органів на повідомлення іншої

[2] Germany. On the Application of International Law in Cyberspace: Position Paper. 2021. P. 3.
[3] Germany. On the Application of International Law in Cyberspace: Position Paper. 2021. P. 3.

держави, перевірку відомостей про функціонування шкідливої інфраструктури, взаємодію з провайдерами, блокування або обмеження очевидно небезпечних ресурсів, проведення внутрішнього розслідування, а також співпрацю з іншими державами у разі транскордонного характеру загрози. Очевидно, що держава не зобов'язана до неможливого. Проте якщо вона має достатні правові та технічні засоби реагування, але свідомо або безпідставно їх не використовує, така бездіяльність може набути міжнародно-протиправного характеру.

Найбільш складним питанням у цій сфері є визначення критеріїв відповідальності держави. Насамперед ідеться про те, коли держава справді не знала про шкідливу кібердіяльність, а коли свідомо уникала з'ясування відповідних обставин. Це питання не може вирішуватися лише формальним запереченням. У кіберпросторі держава може посилатися на складність технічної атрибуції, багаторівневу маршрутизацію, використання проксі-інфраструктури або неможливість швидко встановити всі обставини. Частково такі аргументи можуть бути виправданими, однак вони не повинні перетворюватися на універсальний спосіб уникнення відповідальності.

Доцільно виходити з критерію розумної поінформованості. Якщо шкідлива кібердіяльність має тривалий, масштабний або технічно очевидний характер, пов'язана з інфраструктурою, локалізованою в межах певної держави, а потерпіла держава надсилала відповідні повідомлення, технічні індикатори чи дипломатичні сигнали, посилання на повну необізнаність втрачає переконливість. За таких умов значення має не лише пряме знання, а й ситуація свідомої сліпоти. Держава може не мати повної картини події, але водночас мати достатні підстави для перевірки, втручання або принаймні мінімального реагування. Якщо вона цього не робить, твердження про необізнаність не може вважатися достатнім виправданням бездіяльності[4].

Отже, формула «не хотіла знати» має розумітися не як побутовий вислів, а як юридична характеристика поведінки держави, яка свідомо уникає перевірки очевидних сигналів, не використовує доступні механізми реагування, не співпрацює з потерпілою стороною або не реагує належним чином на продовження шкідливої активності. У такому випадку міжнародно-правова проблема полягає не в обов'язковій підтримці атаки, а в допущенні її продовження через невиконання обов'язку діяти належним чином. У кіберпросторі це особливо небезпечно, оскільки одна й та сама шкідлива інфраструктура може неодноразово використовуватися, швидко адаптуватися, змінювати конфігурацію та спричиняти каскадні наслідки для різних держав.

[4] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. ed. by M. N. Schmitt. Cambridge University Press, 2017. P. 33.

Важливим аргументом на користь можливості міжнародно-правової відповідальності за таку бездіяльність є загальна конструкція права міжнародної відповідальності держав. Проєкт статей про відповідальність держав за міжнародно-протиправні діяння виходить із того, що міжнародно-протиправне діяння може полягати як у дії, так і в бездіяльності, якщо така поведінка порушує міжнародне зобов'язання, покладене на державу. Саме ця логіка дозволяє розглядати неприпинення шкідливої кібердіяльності не просто як політичну проблему або недружню поведінку, а як потенційно самостійне порушення міжнародного права за умови, що існування відповідного обов'язку в конкретній ситуації є достатньо переконливо встановленим[5].

У цьому контексті міжнародно-правова оцінка бездіяльності держави має базуватися на реалістичних критеріях. Недостатньо стверджувати, що держава повинна була повністю контролювати весь цифровий простір у межах своєї юрисдикції. Вирішальне значення мають її фактичні технічні та інституційні можливості, характер загрози, ступінь її очевидності та наслідки для потерпілої сторони. Лише такий підхід дає змогу уникнути як покладання на державу надмірного тягаря, так і нівелювання її обов'язків у разі очевидної шкідливої активності.

Окремого аналізу потребує питання про правові наслідки для потерпілої держави. Якщо держава, з юрисдикції якої виходить шкідлива кібердіяльність, не виконує обов'язку належного реагування, потерпіла сторона може порушувати питання про міжнародно-правову відповідальність і за певних умов вдаватися до контрзаходів. У межах загального права міжнародної відповідальності контрзаходи є тимчасовими заходами у відповідь на міжнародно-протиправне діяння з метою спонукати державу-порушницю до припинення порушення та виконання пов'язаних із відповідальністю обов'язків. У сучасних офіційних підходах держав визнається можливість застосування цього інституту і в кіберпросторі, хоча його реалізація потребує особливої обережності[6].

Водночас контрзаходи не є засобом вільного розсуду потерпілої держави. Їх правомірність залежить від дотримання низки умов, зокрема наявності попереднього міжнародно-протиправного діяння, можливості приписати його державі-порушниці, пропорційності, тимчасового характеру та спрямованості на припинення порушення, а не на покарання. Для кіберпростору це особливо важливо, оскільки цифрова відповідь може вийти за межі початкового задуму та зачепити третіх осіб або цивільну інфраструктуру.

Специфіку в кіберпросторі має і питання попереднього повідомлення держави-порушниці. У класичному праві міжнародної відповідальності

[5] Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. International Law Commission. 2001. P. 31.

[6] Application of international law to states' conduct in cyberspace: UK statement. Foreign, Commonwealth & Development Office. 2021. P. 16-18.

попередня вимога про припинення порушення вважається бажаною, однак у цифровому середовищі прихований характер діяльності, швидкий розвиток подій і потреба у конфіденційності можуть обмежувати можливість такого повідомлення. Тому в сучасних позиціях окремих держав визнається, що в певних ситуаціях попереднє повідомлення не є безумовною передумовою правомірності контрзаходів[7].

Отже, концепція суверенітету в кіберпросторі не може обмежуватися лише ідеєю виключного контролю держави над цифровою інфраструктурою у межах її юрисдикції. У сучасних умовах вона охоплює також обов'язок держави не допускати використання такого простору як джерела серйозної шкоди для інших держав. З цього випливає міжнародно-правове значення неприпинення шкідливої кібердіяльності. Якщо держава знала або повинна була знати про таку діяльність, мала реальні можливості для реагування, але не вжила належних заходів, її бездіяльність може розглядатися як порушення міжнародного зобов'язання. Межа між ситуацією, коли держава справді не знала, і ситуацією, коли вона фактично не хотіла знати, повинна визначатися через аналіз конкретних обставин, зокрема очевидності загрози, тривалості активності, наявності достовірних повідомлень та реальних можливостей для реагування. За наявності такого порушення потерпіла держава може, за дотримання умов міжнародного права, вдаватися до контрзаходів для спонукання порушника до припинення протиправної поведінки та відновлення правопорядку.

Таким чином, питання відповідальності держави за неприпинення шкідливої кібердіяльності є одним із важливих напрямів розвитку сучасного міжнародного права. Воно засвідчує, що цифровий вимір міжнародних відносин не усуває класичних правових категорій, а навпаки, потребує їх переосмислення та точнішого застосування. Суверенітет у кіберпросторі дедалі більше постає не лише як право, а й як відповідальність. Від такого розуміння залежить можливість формування дієвого міжнародно-правового режиму, здатного забезпечити баланс між незалежністю держав, стабільністю міжнародного правопорядку та належним реагуванням на сучасні кіберзагрози.

[7] Application of international law to states' conduct in cyberspace: UK statement. Foreign, Commonwealth & Development Office. 2021. P. 19.