5. У вільному доступі з’явився унікальний інструментарій із цифровізації медіації. Прес-реліз. PRAVO. Видавництво ЮРИДИЧНА ПРАКТИКА. 20.02.2026, 17:39. URL: https://pravo.ua/u-vilnomu-dostupi-z-iavyvsia-unikalnyi-instrumentarii-z-tsyfrovizatsii-mediatsii/.

DOI https://doi.org/10.36059/978-966-397-607-5-25

КІБЕРАТАКИ У КОНТЕКСТІ ПРИНЦИПУ ВІЙСЬКОВОЇ НЕОБХІДНОСТІ

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

Розвиток інформаційно-комунікаційних технологій перетворив кіберпростір на окреме середовище ведення ворожих дій у сучасних збройних конфліктах. Кібератаки дедалі частіше застосовуються поряд із традиційними засобами боротьби та можуть бути спрямовані на системи військового управління, зв’язку, енергетичну інфраструктуру, транспортні мережі, державні реєстри й інші інформаційні ресурси. У зв’язку з цим особливої актуальності набуває питання застосування норм міжнародного гуманітарного права до кібератак і можливості їх правового виправдання з позицій принципу військової необхідності.

Міжнародне гуманітарне право поширюється на всі засоби і методи ведення війни, незалежно від рівня їх технічної новизни. Тому кібератаки, якщо вони здійснюються у зв’язку зі збройним конфліктом, також підпадають під його регулювання. Визначальне значення має принцип військової необхідності, оскільки саме він дає змогу оцінити, чи існує правове виправдання для застосування кібератак у конкретній бойовій ситуації.

Принцип військової необхідності означає, що сторона конфлікту може вдаватися лише до тих засобів і методів ведення війни, які об’єктивно необхідні для досягнення законної військової мети. Він не є самостійним дозволом на будь-які дії, що здаються ефективними з оперативного погляду, і діє лише в межах інших норм міжнародного гуманітарного права. Тому військова необхідність не виправдовує невибіркові дії, напади на цивільні об’єкти чи заподіяння надмірної шкоди цивільному населенню [1].

У кіберпросторі застосування цього принципу ускладнюється тим, що кібератака не завжди супроводжується фізичним руйнуванням об'єкта. Її наслідком може бути втрата функціональності системи, знищення або спотворення даних, порушення роботи мережі чи дестабілізація управлінських процесів. За таких умов особливого значення набуває кваліфікація такого втручання як атаки у розумінні міжнародного гуманітарного права, навіть якщо фізичного пошкодження немає, але система фактично виводиться з ладу. Саме від цього залежить обсяг правових обмежень, які мають враховуватися під час планування та проведення кібератаки.

Надто вузьке тлумачення поняття атаки створює ризик, що значна частина небезпечних кібердій формально опиниться за межами повноцінного гуманітарно-правового контролю. Однак для цивільного населення наслідки втрати функціональності можуть бути не менш тяжкими, ніж наслідки фізичного ураження. Якщо внаслідок кібератаки припиняє працювати енергосистема, медична мережа, система водопостачання або транспортні сервіси, це прямо впливає на безпеку, здоров'я і життя цивільних осіб. З огляду на це оцінка військової необхідності не може обмежуватися лише з'ясуванням того, чи був пошкоджений матеріальний об'єкт. Вона має включати оцінку реального функціонального ефекту операції та його значення для цивільного середовища [2, с. 250, 261].

Особливу складність становить те, що значна частина сучасної цифрової інфраструктури має подвійне призначення. Ті самі мережі, канали зв'язку, серверні потужності, навігаційні системи чи елементи хмарного зберігання даних можуть одночасно використовуватися як військовими структурами, так і цивільними установами. Це означає, що навіть операція, яка формально спрямована на досягнення законної військової мети, може зачіпати інтереси цивільного населення. За таких умов принцип військової необхідності вимагає встановити, що втручання справді необхідне для досягнення військової переваги, що менш шкідливої альтернативи не існує, а наслідки для цивільної інфраструктури не виходять за межі допустимого.

Саме тут виявляється ключова межа між військовою необхідністю і військовою доцільністю. Не кожна дія, яка може послабити противника, є необхідною у юридичному значенні. Якщо того самого результату можна досягти іншим способом, який створює менший ризик для цивільних осіб і цивільних об'єктів, то вибір більш небезпечної кібератаки буде сумнівним з погляду міжнародного гуманітарного права. Військова необхідність не виправдовує максимізацію шкоди, а вимагає обрання такого засобу, який забезпечує досягнення військової мети з дотриманням установлених правових меж. У кіберпросторі ця

вимога набуває особливої ваги через складність контролю за поширенням технічних наслідків втручання [3, с. 797-798, 803].

Звідси випливає ще одна важлива проблема, а саме необхідність прогнозування побічних ефектів кібератаки. У традиційних формах ведення бойових дій наслідки застосування сили часто є більш видимими й відносно передбачуваними. У кіберпросторі навіть обмежене втручання в одну мережу може спричинити ланцюгову реакцію в інших системах, які з нею пов'язані. Порушення функціонування одного вузла може вплинути на роботу лікарень, транспорту, банківських сервісів, систем цивільного оповіщення або державних реєстрів. За таких обставин посилання на військову необхідність не може бути переконливим, якщо сторона конфлікту не здійснила належної попередньої оцінки ризиків і не вжила всіх практично можливих заходів для локалізації наслідків.

Окремої уваги потребує питання про статус даних у сучасному цифровому середовищі. У багатьох випадках саме дані, а не матеріальна інфраструктура, становлять основну цінність цивільної системи. Медичні записи, банківська інформація, податкові бази, державні реєстри, персональні дані та логістичні масиви мають критичне значення для повсякденного функціонування суспільства. Їх знищення або спотворення може паралізувати цілі сектори цивільного життя навіть без будь-якого фізичного пошкодження обладнання. Тому при оцінці кібератаки крізь призму принципу військової необхідності не можна ігнорувати нематеріальний, але суспільно значущий характер шкоди. Якщо військова перевага досягається шляхом втручання у дані, необхідні для забезпечення базових потреб цивільного населення, така операція потребує особливо суворої правової оцінки [4, с. 30-32].

Принцип військової необхідності слід тлумачити у взаємозв'язку з принципами розрізнення і пропорційності. Якщо кібератака не дає змоги чітко відмежувати військову ціль від цивільних систем або створює значний ризик зупинення життєво важливих сервісів за відносно обмеженої військової переваги, її правомірність викликає сумнів. Саме тому у цифровому середовищі принцип військової необхідності має тлумачитися вузько.

Нові виклики у цій сфері пов'язані також із використанням автономних кіберсистем і технологій штучного інтелекту. Якщо рішення про спосіб втручання, визначення вразливостей або подальше поширення шкідливого програмного коду частково передаються автоматизованим системам, це зменшує безпосередній людський контроль над межами операції. За таких умов складніше гарантувати, що застосований засіб буде використано саме в обсязі, необхідному для досягнення законної військової мети, і що його наслідки не вийдуть за

передбачувані межі. Отже, використання високого рівня автоматизації не знімає вимоги дотримання принципу військової необхідності, а навпаки, посилює потребу в особливо ретельній правовій та технічній перевірці [5, с. 3-5].

Отже, кібератаки не перебувають у правовому вакуумі, однак їх оцінка потребує більшої точності, ніж у багатьох традиційних випадках застосування сили. Специфіка цифрового середовища, подвійний характер значної частини інфраструктури, складність прогнозування побічних наслідків і ризик невибіркового поширення шкідливого коду істотно ускладнюють застосування принципу військової необхідності. Саме тому подальший розвиток міжнародно-правової доктрини має бути спрямований не стільки на повторне підтвердження застосовності загальних норм до кіберпростору, скільки на вироблення чіткіших критеріїв, за якими можна встановити межі військово необхідного і юридично допустимого у сфері кібератак. Лише за таких умов принцип військової необхідності зможе виконувати свою справжню функцію, а саме обмежувати застосування сили настільки, наскільки це потрібно для досягнення законної військової мети, не руйнуючи водночас основу гуманітарного захисту цивільного населення.

Література

1. International Committee of the Red Cross. The principles of humanity and necessity. URL: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf (дата звернення: 1.03.2026).

2. Biggio G. Regulating non-kinetic effects of cyber operations: the ‘Loss of Functionality’ approach and the military necessity-humanity balance under international humanitarian law. Journal of Conflict and Security Law. 2025. Vol. 30. No. 2. P. 241–263. DOI: 10.1093/jcsl/kraf008.

3. Schmitt M.N. Military necessity and humanity in international humanitarian law. URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/07/Military-Necessity-Humanity-Balance.pdf (дата звернення: 4.03.2026).

4. International Committee of the Red Cross. Twenty years on: international humanitarian law and cyber operations. International Review of the Red Cross. URL: https://international-review.icrc.org/sites/default/files/reviews-pdf/2020-10/Twenty-years-on-IHL-and-cyber-operations-final-version.pdf (дата звернення: 5.03.2026).

5. International Committee of the Red Cross. Artificial intelligence and machine learning in armed conflict. Geneva, 2019. URL: https://www.icrc.org/sites/default/files/document_new/file_list/ai_and_machine_learning_in_armed_conflict-icrc.pdf (дата звернення: 5.03.2026).