УДК 341.3:004.056
DOI https://doi.org/10.32782/2524-0374/2025-8/57

ЗАСТОСУВАННЯ НОРМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА ДО КІБЕРАТАК: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

APPLICATION OF INTERNATIONAL HUMANITARIAN LAW NORMS TO CYBER ATTACKS: PROBLEMS AND PROSPECTS

Пасешник О.Р., аспірант кафедри міжнародного, цивільного та комерційного права
Державний торговельно-економічний університет

У статті проаналізовано проблему застосування норм міжнародного гуманітарного права до кібератак, що мають місце під час міжнародних і неміжнародних збройних конфліктів. У сучасних умовах кіберпростір став новим середовищем для ведення бойових дій, а кібератаки стали невід'ємною складовою сучасної війни. Такі атаки можуть мати серйозні наслідки для цивільного населення, об'єктів критичної інфраструктури, систем зв'язку та охорони здоров'я, навіть без фізичного знищення. Це зумовлює потребу в переосмисленні традиційного підходу до застосування міжнародного гуманітарного права та адаптації його норм до реалій цифрової епохи.

У статті особливу увагу приділено аналізу застосовності базових принципів міжнародного гуманітарного права до сучасних реалій кібервійн, зокрема принципу розрізнення між цивільними й військовими об'єктами, принципу пропорційності, військової необхідності, а також принципу відсутності взаємності. Розглядається роль таких документів, як Талліннський посібник 2.0, що відіграє важливу роль у доктринальному тлумаченні міжнародного права в контексті кібератак. Проаналізовано підходи Міжнародного комітету Червоного Хреста, окремих держав і міжнародних експертів до питання кваліфікації кібератак.

Також проаналізовано приклади кібератак, що мали місце під час збройного конфлікту в Україні з 2014 року, серед них атаки на енергетичну інфраструктуру, системи управління, органи державної влади. Зазначено труднощі з правовою атрибуцією таких атак, визначенням їх масштабу та оцінкою відповідності нормам міжнародного гуманітарного права. Обґрунтовується необхідність розвитку міжнародної нормативної бази, яка б регламентувала поведінку держав і недержавних акторів у кіберпросторі під час конфліктів. Пропонуються прийняття окремого міжнародного договору або додаткового протоколу до Женевських конвенцій, що регулював би особливості ведення кібератак. Дослідження спрямовано на стимулювання фахової дискусії в юридичній науці щодо гуманітарного виміру кіберпростору. Підкреслюється важливість посилення захисту цивільного населення в умовах трансформації характеру сучасних збройних конфліктів.

Ключові слова: збройний конфлікт, цивільне населення, пропорційність, розрізнення, Талліннський посібник, МКЧХ, правове регулювання, кіберпростір, війна, відповідальність, гуманітарні наслідки.

The article analyzes the issue of applying the norms of international humanitarian law to cyberattacks that occur during international and non-international armed conflicts. In the current context, cyberspace has become a new environment for conducting hostilities, and cyberattacks have become an integral part of modern warfare. Such attacks may have serious consequences for the civilian population, critical infrastructure, communication systems, and healthcare, even without physical destruction. This situation necessitates a rethinking of the traditional approach to the application of international humanitarian law and an adaptation of its norms to the realities of the digital age.

The article pays particular attention to the analysis of the applicability of the basic principles of international humanitarian law to the modern realities of cyber warfare, in particular the principle of distinction between civilian and military objects, the principle of proportionality, military necessity, and the principle of non-reciprocity. The role of documents such as the Tallinn Manual 2.0 is considered, as it plays an important role in the doctrinal interpretation of international law in the context of cyberattacks. The approaches of the International Committee of the Red Cross, individual states, and international experts to the qualification of cyberattacks are also analyzed.

The article further examines examples of cyberattacks that have occurred during the armed conflict in Ukraine since 2014, including attacks on energy infrastructure, control systems, and government institutions. The article notes the challenges of legal attribution of such attacks, determining their scale, and assessing their compliance with the norms of international humanitarian law. It substantiates the need to develop an international legal framework to regulate the conduct of states and non-state actors in cyberspace during armed conflicts. The article proposes the adoption of a separate international treaty or an additional protocol to the Geneva Conventions to regulate the specific features of cyberattacks. The research aims to stimulate professional discussion in legal scholarship regarding the humanitarian dimension of cyberspace and emphasizes the importance of enhancing the protection of the civilian population in the context of the evolving nature of contemporary armed conflicts.

Key words: Armed conflict, civilian population, proportionality, distinction, Tallinn Manual, ICRC, legal regulation, cyberspace, war, responsibility, humanitarian consequences.

У XXI столітті кіберпростір перетворився на самостійний театр воєнних дій, що має суттєвий вплив на хід і наслідки збройних конфліктів. Кібератаки дедалі частіше використовуються не лише як інструмент стратегічного впливу, а й як засіб безпосереднього ураження об'єктів критичної інфраструктури, систем зв'язку, енергетики, охорони здоров'я та інших цивільних елементів, що традиційно перебувають під захистом міжнародного гуманітарного права [1].

З 2014 року кіберпростір став одним із ключових напрямків гібридної війни між росією та Україною. У цей період зафіксовано численні хакерські атаки, які не лише супроводжували воєнні дії, а й мали серйозні гуманітарні наслідки. Одним із найбільш показових прикладів стали атаки на енергетичну інфраструктуру, що спричинили масштабні відключення електроенергії, створюючи загрозу для цивільного населення.

Поряд з цим, державні установи та військові структури України неодноразово ставали мішенню шкідливих програм, спрямованих на знищення або блокування важливих даних. Деякі з цих атак мали наслідки для економіки та безпеки країни.

Такі випадки демонструють, що сучасні збройні конфлікти супроводжуються не лише фізичним протистоянням, а й скоординованими кібератаками, які мають серйозний вплив на гуманітарну ситуацію. У цьому контексті зростає потреба у переосмисленні чинних правових механізмів, щодо їх здатності ефективно регулювати нові загрози, пов'язані з використанням кібертехнологій у війнах. Особливу складність становить те, що міжнародне гуманітарне право (МГП) не містить спеціалізованих норм, що прямо регулюють поведінку у кіберпросторі. Це створює нормативну прогалину, яку намагаються заповнити доктринальні джерела, аналітичні документи

© Пасешник О.Р., 2025
Стаття поширюється на умовах ліцензії CC BY 4.0

та національна практика. Значну роль у формулюванні доктринальних підходів відіграє Талліннський посібник 2.0, розроблений експертами при НАТО Cooperative Cyber Defence Centre of Excellence, який хоча й не має обов'язкової юридичної сили, проте став авторитетним джерелом тлумачення [1].

Кібератаки як явище виникли задовго до їхнього активного застосування у збройних конфліктах, однак саме в останнє десятиліття їхній правовий статус став предметом особливої уваги міжнародного права. Традиційно засоби і методи ведення війни визначались у фізичному вимірі, однак розвиток інформаційних технологій спричинив появу нового інструментарію, що не залишає матеріального сліду, але здатен завдати значної шкоди цивільному населенню або військовому потенціалу держави.

Міжнародне гуманітарне право не містить спеціалізованого визначення поняття «кібератака». У Талліннському посібнику, який є авторитетною доктринальною компіляцією правових позицій, під кібератакою пропонується розуміти дію, спрямовану на нанесення шкоди або знищення цілі за допомогою кіберзасобів [1]. Це означає, що для кваліфікації дії як кібератаки не обов'язково має бути фізичне ураження, достатньо порушення функціональності або спричинення значної шкоди.

У цьому контексті ключовим питанням стає класифікація кібератак як засобів або методів ведення війни, що безпосередньо визначає сферу застосування норм МГП. Згідно зі ст. 36 Додаткового протоколу I до Женевських конвенцій, держави зобов'язані оцінювати нові види озброєнь або способів ведення війни на відповідність нормам міжнародного права [2]. Варто звернути увагу на те, що не всі кібероперації можуть вважатися кібератаками з точки зору МГП. Частина таких дій (наприклад, шпигунство, пропагандистські кампанії чи психологічні операції) не підпадають під правове визначення «нападу». Натомість дії, що спричиняють вихід з ладу об'єктів критичної інфраструктури або піддають ризику цивільне населення, можуть бути розцінені як напади відповідно до ст. 49 Протоколу I [2].

Попри те, що МГП формувалося в умовах традиційної війни, його основоположні принципи залишаються актуальними і для кіберпростору. Однак їх практична реалізація в умовах сучасних збройних конфліктів стикається з багатьма викликами.

Принцип розрізнення, що вимагає чіткого розмежування між військовими цілями та цивільними об'єктами, ускладнюється в кіберпросторі через подвійне призначення більшості систем: телекомунікаційних мереж або енергетичної інфраструктури, які одночасно використовуються як цивільними, так і збройними силами. Ідентифікація цілі у цифровому середовищі нерідко неможлива без тривалого технічного аналізу, що позбавляє сторону конфлікту оперативної впевненості в правомірності атаки.

Принцип пропорційності забороняє атаки, в яких очікувана шкода цивільному населенню є надмірною порівняно з очікуваною воєнною перевагою. У випадку кібератак це правило вимагає оцінки потенційних побічних наслідків, які часто є непередбачуваними, а спричинена шкода може проявитися із затримкою, що ускладнює її прогнозування та оцінку.

Принцип військової необхідності дозволяє сторонам конфлікту застосовувати лише ті засоби і методи, які є необхідними для досягнення конкретної воєнної мети. У кіберпросторі реалізація цього принципу стикається з труднощами, пов'язаними з оцінкою фактичної ефективності кібератаки та прогнозуванням її результатів. Часто відсутність миттєвого зворотного зв'язку унеможливлює об'єктивну перевірку доцільності втручання. Крім того, ризик подвійного призначення цифрових систем ускладнює визначення, чи є конкретна кібероперація дійсно воєнно необхідною, чи вона лише створює непрямі перешкоди противнику без стратегічної потреби.

Принцип відсутності взаємності забороняє одній стороні конфлікту порушувати норми гуманітарного права лише тому, що інша сторона їх не дотримується. У контексті кібервійни, де відповідальність за атаки часто важко довести, цей принцип відіграє важливу роль, адже забезпечує обов'язковість дотримання правил навіть у випадку провокацій або очевидних порушень з боку противника. Водночас він стикається зі складністю ідентифікації порушника, що створює ризик неправомірного або непропорційного реагування [3].

В умовах відсутності спеціалізованих міжнародно-правових норм, що безпосередньо регулюють ведення кібероперацій у збройних конфліктах, ключову роль у формуванні праворозуміння відіграють доктринальні джерела та практичні підходи окремих держав. Особливе місце серед них посідає Талліннський посібник, який, хоча і не є юридично обов'язковим документом, став одним із найавторитетніших довідників у сфері застосування міжнародного права до кіберпростору.

Талліннський посібник 2.0 є результатом роботи групи незалежних експертів під егідою НАТО. У ньому докладно аналізуються, як норми МГП, включаючи принципи розрізнення, пропорційність, військову необхідність та захист цивільного населення, можуть застосовуватись до кібератак. Документ охоплює понад 150 «правил», кожне з яких супроводжується коментарями, що ґрунтуються на практиці держав, рішеннях міжнародних судів та авторитетних наукових позиціях. Посібник підтримує підхід, згідно з яким базові принципи міжнародного права застосовуються до кібероперацій, якщо останні досягають рівня «нападу» у розумінні Протоколу I до Женевських конвенцій. Таким чином, кібератака може розцінюватися як збройний напад, якщо її наслідки за масштабом та ефектом прирівнюються до традиційного застосування сили, а відповідальність за дотримання гуманітарних норм покладається як на держави, так і на інші сторони збройного конфлікту [1].

Окремий напрям формування доктринальної бази становлять позиції Міжнародного комітету Червоного Хреста (МКЧХ), який наголошує на застосовності МГП до кібероперацій. Так, у своїх доповідях МКЧХ підкреслює, що навіть у цифровому вимірі війни діють загальні гуманітарні обмеження, спрямовані на захист цивільного населення та об'єктів, які не мають військового призначення [4].

Особливу увагу МКЧХ приділяє зростанню ролі цивільних осіб у проведенні кібератак, що може призвести до стирання меж між комбатантами та некомбатантами. Активне залучення незалежних осіб, приватних груп і волонтерів у кіберконфлікти не лише створює нові ризики для цивільного населення, але й може призвести до зміни їхнього правового статусу. Відповідно до МГП, цивільні особи втрачають правовий захист, якщо безпосередньо беруть участь у бойових діях, включно з кіберопераціями, спрямованими на завдання шкоди противнику. Щодо міждержавних підходів, можна спостерігати відсутність єдиної уніфікованої позиції, кожен представник демонструє своє бачення ситуації, залежно від особливостей держави.

Таким чином, на сучасному етапі розвиток доктрини і практики у сфері кібератак в умовах збройного конфлікту відбувається переважно в площині «м'якого права» та політико-правових декларацій. Однак, накопичення державної практики та авторитетних наукових підходів поступово створює підґрунтя для формування загальновизнаних правил поведінки у цифровому середовищі під час війни.

З початку збройної агресії Російської Федерації проти України у 2014 році кіберпростір став одним із головних

фронтів гібридної війни. Кібератаки проти української держави відбуваються системно, мають координаційний характер і, в окремих випадках, становлять загрозу для життя і здоров'я цивільного населення. Досвід України є унікальним прикладом того, як кібератаки можуть здійснюватися у тісному зв'язку з кінетичними діями та відігравати роль елементів широкомасштабного збройного конфлікту.

Одним із найяскравіших прикладів цілеспрямованого кібернападу стало виведення з ладу енергосистеми західної України 23 грудня 2015 року, внаслідок якого близько 220 тисяч осіб залишилися без електропостачання. Згідно з офіційним звітом CISA, атака була проведена за допомогою шкідливого програмного забезпечення BlackEnergy і супроводжувалась вторгненням у внутрішні мережі енергокомпаній, а також маніпуляціями з системами дистанційного управління. Цей інцидент став першим задокументованим випадком, коли кібератака призвела до фізичного відключення електроенергії у великому масштабі [5].

Ще одним прикладом стало поширення шкідливого програмного забезпечення NotPetya у червні 2017 року, що почалося з ураження українських урядових структур та підприємств, а згодом вийшло за межі України, спричинивши мільярдні збитки на глобальному рівні. Хоча атака не була спрямована безпосередньо на збройні сили, її наслідки для державних служб і логістичних систем були значними, що ставить під сумнів її відповідність принципам МГП [6].

Окрему загрозу становлять кібератаки на медичні установи, які підпадають під особливий захист відповідно до статей 12 і 18 Додаткового протоколу I до Женевських конвенцій. За даними МКЧХ, на початку 2022 року фіксувалися спроби ураження українських систем охорони здоров'я шляхом знищення або блокування доступу до медичних баз даних та порушення роботи інфраструктури лікарень.

Лютий та березень 2024 року стали серйозним випробуванням для американської системи охорони здоров'я. Наприкінці лютого хакерське угруповання Blackcat здійснило атаку на Change Healthcare, ключову частину UnitedHealth Group, що обробляє майже половину всіх запитів до медичних страхових компаній у США. Інфраструктура компанії охоплює близько 900 000 лікарів, 33 000 аптек, 5 500 лікарень і 600 лабораторій [7].

Внаслідок цієї атаки робота медичних установ та фармацевтичних сервісів зазнала серйозних перебоїв, оскільки значна частина американської системи охорони здоров'я базується на страхових виплатах. Інцидент продемонстрував високу вразливість цифрової інфраструктури медичного сектору перед кібератаками та необхідність посилення захисту критично важливих систем.

Ці факти підкреслюють зростаючу роль кібератак у сучасних збройних конфліктах та необхідність їхнього врахування в рамках МГП.

З аналізу цих прикладів випливає, що значна частина ворожих кібероперацій відповідає критеріям, які дозволяють розглядати їх у межах дії МГП. При цьому не всі атаки є прямими «нападами» у розумінні МГП, однак їх кумулятивний вплив, масштаб і скоординованість з воєнними діями свідчать про систематичне використання кіберзасобів як компоненту збройного конфлікту.

Попри зростаюче визнання можливості застосування МГП до кібератак, на практиці існує низка суттєвих труднощів, що ускладнюють ефективне правозастосування у цій сфері. Ключовою проблемою є відсутність універсального міжнародного договору, який би спеціально регулював поведінку держав та інших суб'єктів у кіберпросторі під час збройних конфліктів. Хоча загальні положення Женевських конвенцій та Додаткових протоколів можуть тлумачитись розширено, у низці випадків вони не враховують специфіки кіберпростору.

Однією з найбільш складних юридичних проблем є встановлення відповідальності конкретного суб'єкта за певну кібератаку. Через анонімність кіберпростору, використання проміжних серверів, маскування шкідливого програмного забезпечення, визначення виконавця або держави, що стоїть за атакою, є технічно та юридично складним. Без чіткої атрибуції застосування норм МГП, у тому числі щодо відповідальності, практично неможливе.

У зв'язку з вищезазначеним, наукова спільнота все частіше порушує питання про необхідність кодифікації норм, які б спеціально регулювали поведінку в кіберпросторі під час збройних конфліктів. Існує кілька можливих підходів до такого вдосконалення:

Розширене тлумачення чинних норм МГП, зокрема шляхом закріплення в офіційних коментарях до Женевських конвенцій положень щодо кібератак.

Розробка додаткового протоколу до чинних конвенцій із визначенням основних термінів: кібератака, кібервійна, кібероперація і закріпленням спеціального режиму захисту цивільного населення.

Укладення нової універсальної угоди щодо поведінки держав у кіберпросторі у період збройного конфлікту, з обов'язковим механізмом верифікації та притягнення до відповідальності.

Перспективним також є залучення елементів міжнародного кримінального права, в тому числі юрисдикції Міжнародного кримінального суду щодо серйозних кібератак, які можуть кваліфікуватися як воєнні злочини. Це особливо актуально в умовах сучасних гібридних конфліктів, таких як війна в Україні, де кібератаки стали частиною загальної військової кампанії.

Застосування норм МГП до кібератак викликає низку теоретичних і практичних викликів. Аналіз підтверджує, що, попри формування МГП в епоху традиційних війн, його основоположні принципи – розрізнення, пропорційності, воєнної необхідності та відсутності взаємності залишаються актуальними, хоча їхня реалізація в кіберпросторі стикається з труднощами. Ці виклики включають проблеми з кваліфікацією кібератак як «нападів», правовою атрибуцією, а також відсутністю чітких критеріїв для розмежування військових і цивільних об'єктів у цифровому середовищі. Аналіз прикладів кібератак на енергетичну інфраструктуру, органи державного управління та медичні заклади, продемонстрував, що такі операції можуть мати серйозні гуманітарні наслідки та порушувати норми МГП.

Доктринальні джерела, зокрема Талліннський посібник і позиції Міжнародного комітету Червоного Хреста, свідчать про зростаючу підтримку ідеї застосовності МГП до кіберпростору. Водночас наявні правові інструменти не є достатніми для забезпечення належного захисту цивільного населення. У зв'язку з цим, актуальним залишається питання вдосконалення правового регулювання. Перспективними шляхами є розширене тлумачення чинних положень Женевських конвенцій, розробка спеціального протоколу або нового міжнародного договору про правила ведення кібервійни.

З огляду на гібридний характер сучасних збройних конфліктів, інтеграція кібератак у систему воєнного протистояння вимагає як посилення норм превентивного захисту, так і впровадження ефективних механізмів притягнення до відповідальності. Забезпечення належного рівня захисту цивільного населення в умовах кіберзагроз має стати одним із ключових напрямів розвитку сучасного міжнародного гуманітарного права.

ЛІТЕРАТУРА

1. Tallinn manual 2.0 on the international law applicable to cyber operations / general editor Michael N. Schmitt. Cambridge : Cambridge University Press, 2017. 598 p.

2. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text (дата звернення: 07.05.2025).

3. Сенаторова О. В. Права людини і збройні конфлікти : навчальний посібник. Київ : ФОП Голембовська О. О., 2018. 208 с.

4. International Humanitarian Law and Cyber Operations during Armed Conflicts : position paper. Geneva: ICRC, 2019. 9 p. URL: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf (Last accessed: 07.05.2025).

5. Cyber Attack Against Ukrainian Critical Infrastructure. *Cybersecurity and Infrastructure Security Agency* : Website. URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (Last accessed: 07.05.2025).

6. Рада національної безпеки і оборони України. НКЦК при РНБО України попереджає про кібератаку на систему документообігу державних органів. Веб-сайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/4823.html (дата звернення: 08.05.2025).

7. Рада національної безпеки і оборони України. Річний аналітичний огляд: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 році. Київ : РНБО, 2025. 32 с. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf (дата звернення: 08.05.2025).

Дата першого надходження рукопису до видання: 18.08.2025
Дата прийнятого до друку рукопису після рецензування: 23.09.2025
Дата публікації: 26.09.2025