УДК 341.1/8
DOI https://doi.org/10.32782/2524-0374/2023-9/106

ЗАСТОСУВАННЯ МГП ПО ВІДНОШЕННЮ ДО КІБЕРОПЕРАЦІЙ, ЩО ПРОВОДЯТЬСЯ ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ

THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW (IHL) TO CYBER OPERATIONS CONDUCTED DURING ARMED CONFLICTS

Фещуков Г.В., молодший науковий співробітник з міжнародного права
Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка

Ця стаття націлена на дослідження актуальної проблематики застосування міжнародного гуманітарного права (МГП) у контексті кібероперацій, які активно використовуються під час збройних конфліктів у сучасному світі. Стаття висвітлює те, як МГП, спрямоване на регулювання поведінки конфліктуючих сторін під час збройних конфліктів, може бути застосовано до нового виміру – кібервійни.

Важливим аспектом розгляду є аналіз можливостей індентифікації кібератак як актів віртуальної агресії та визначення відповідальності за ці кіберагресії. Стаття досліджує, як МГП може бути застосовано для визначення, коли кібероперації вважаються збройними діями, і які правила щодо їх ведення слід застосовувати відповідно до принципів МГП, зокрема, непридатності цілей та пропорційності.

Додатково, у статті можуть бути розглянуті конкретні приклади ситуацій зі сучасних конфліктів, де кібероперації впливають на цивільне населення та інфраструктуру. Це допоможе підкреслити важливість розуміння та регулювання кібердійсності в рамках МГП та викликати увагу до проблеми захисту прав людини та мінімізації негативних наслідків для цивільного населення у віртуальному просторі під час збройних конфліктів.

Завершуючи, стаття закликає до ретельного вивчення та удосконалення правових рамок, які регулюють так звану «кібервійну», з метою забезпечення ефективного захисту прав людини та зменшення негативних наслідків для цивільного населення в цифровому світі під час збройних конфліктів як міжнародного, так і неміжнародного характеру. Розгляд даної теми є важливим в контексті змін в сучасних методах ведення війни та їх впливу на міжнародний правопорядок, що яскраво демонструє нинішня російсько-українська війна.

Ключові слова: кібервійна, кібероперації, міжнародне гуманітарне право, кібербезпека, збройні конфлікти, кібератаки.

This article is aimed at exploring the pressing issue of the application of international humanitarian law (IHL) in the context of cyber operations actively used during armed conflicts in the modern world. The article highlights how IHL, designed to regulate the behavior of conflicting parties during armed conflicts, can be applied to the emerging dimension of cyber warfare.

An essential aspect of the discussion involves analyzing the possibilities of identifying cyberattacks as acts of virtual aggression and determining accountability for these cyber aggressions. The article investigates how IHL can be employed to determine when cyber operations qualify as armed actions and what rules, in accordance with the principles of IHL, including the principles of distinction and proportionality, should be applied to these operations.

Additionally, the article may delve into specific examples of situations from contemporary conflicts where cyber operations impact civilian populations and infrastructure. This serves to underscore the significance of comprehending and regulating cyber warfare within the framework of IHL and draws attention to the imperative of protecting human rights and minimizing adverse consequences for civilian populations in the digital realm during armed conflicts.

In conclusion, the article calls for a meticulous examination and enhancement of legal frameworks governing the so-called “cyberwar” to ensure effective protection of human rights and the reduction of negative impacts on civilian populations in the digital domain during armed conflicts, both of international and non-international nature. This discussion holds particular importance in the context of evolving warfare methods in the contemporary world, vividly exemplified by the ongoing Russia-Ukraine war.

Key words: cyber warfare, cyber operations, international humanitarian law, cybersecurity, armed conflicts, cyberattacks.

Незважаючи на те, що довести причетність тієї чи іншої держави до проведення певних кібероперацій вкрай складно, а іноді й зовсім неможливо, здійснення кібероперацій під час збройних конфліктів стало новою реальністю, яке міжнародне гуманітарне право, як і міжнародне право в цілому, не може заперечувати.

Основне завдання цієї статті – донести те, що міжнародне співтовариство має приділяти значну увагу даному питанню, усвідомлюючи той факт, що існуюче міжнародне гуманітарне право не є достатнім для застосування у кіберпросторі, заперечуючи при цьому той факт, що проведення таких операцій перебуває у правовому вакуумі.

З огляду на те, що ця тема є досить складною і має величезну кількість так званих «каменів спотикання», то я хотів би навести список певних фактів, які я скомпонував у таблиці, наведеній нижче:

Однак, крім фактів, які я зазначив вище, існує ще величезна кількість так званих «каменів спотикання» (для простоти називатимемо їх «проблемами»), найбільш значущі з яких я хотів би згадати нижче.

Окремо хотілося б відзначити той факт, що, на жаль, ми не можемо говорити про практику міжнародних судових інстанцій, які б тією чи іншою мірою стосувалися б військових кібероперацій. Проте, я хотів би виділити *Консультативний висновок щодо законності загрози ядерною зброєю або її застосування*, зробленого МС ООН 8 липня 1996 року, а саме пункт 86 щодо військових дій та зброї майбутнього [8], а також *Рішення МС ООН «Нікарагуа проти США»* від 27 червня. 1986 року [14, с. 198], яке хоч і не має прямого відношення до кібероперацій, однак, проаналізувавши це рішення, ми можемо дійти наступних висновків:

1) застосування сили не обмежується прямим використанням збройних сил держави і може включати інші дії, зокрема озброєння, тренування тощо;

2) рішення МС ООН відкриває можливість для кваліфікації як застосування збройної сили дій посередників [15, с. 110].

Таким чином, ми можемо стверджувати про застосовність міжнародного гуманітарного права по відношенню до кібероперацій, що проводяться під час збройних конфліктів.

Таблиця 1

Факти щодо застосування МГП по відношенню до кібероперацій

Факт № 1	Потрібно розуміти, що міжнародне гуманітарне право застосовується лише до кібероперацій, що проводяться у рамках збройних конфліктів. Яскравим прикладом таких кібероперацій можна вважати кібератаки, скоєні на комунікаційні мережі Грузинської Республіки під час російсько-грузинської війни 2008 року. Так звана «Серпнева Кібервійна» 2008 року вважається першою великомасштабною кібероперацією, що проводиться паралельно з воєнними діями [1]. При цьому треба розуміти, що міжнародне гуманітарне право не застосовується до численних кібероперацій, починаючи з кіберзлочинів і кібершпигунства і закінчуючи «кіберопераціями, що підтримуються державою» (наприклад, кібератака на Естонію 2007 року [2] або ж свіжіший приклад у вигляді кібератаки на американську трубопровідну систему Colonial Pipeline 7 травня 2021 року [3]).
Факт № 2	Той факт, що міжнародне гуманітарне право застосовується до кібероперацій під час збройних конфліктів, не є приводом для того, щоб узаконити кібервійну. Цей факт випливає із преамбули Додаткового протоколу I до Женевських конвенцій 1949 р., який свідчить про те, що міжнародне гуманітарне право «не може бути витлумачено як узаконювальне або санкціонуюче будь-який акт агресії або будь-яке інше застосування сили, несумісне зі Статутом Організації Об'єднаних Націй» [4]. Таким чином, можемо сміливо стверджувати те, що міжнародне гуманітарне право не узаконює жодних форм ведення війни, зокрема й кібервійну.
Факт № 3	Ключові принципи МГП [5] (принцип гуманності, військової необхідності, проведення відмінності, пропорційності та вжиття запобіжних заходів) застосовуються до всіх військових операцій і кібероперації не є винятком. Так, наприклад, необхідно розуміти та усвідомлювати той факт, що технології пішли дуже далеко вперед і ми сміливо можемо говорити про те, що існує кіберзброя, яку можна класифікувати як таку, що є невибірковою за своєю природою, а це означає те, що вона не може використовуватись відповідно до норм звичаєвого міжнародного гуманітарного права (Норма 71) [6].
Факт № 4	Цей факт тісно переплітається з фактом № 3, доповнюючи та зміцнюючи його. У випадках, не передбачених існуючими нормами МГП, цивільні особи та комбатанти залишаються під захистом так званого застереження Мартенса, тобто на них, як і раніше, поширюється захист і дія принципів міжнародного права, що випливають із звичаїв, принципів гуманності та вимог суспільної свідомості [7]. Йдеться про так звану «зброю майбутнього [8]», термін, який МС ООН уже вжив одного разу 1996 року у своєму Консультативному висновку щодо законності загрози ядерною зброєю або її застосування. Уявімо, що в недалекому майбутньому буде розроблена кіберзброя, що дозволяє виводити з ладу атомні електростанції інших держав, брати під контроль систему авіанавігації або вивести будь-яке повітряне судно з ладу в пару кліків. Міжнародне гуманітарне право забороняє не лише використання такої зброї, а й її розробку як таку.
Факт № 5	Той факт, що на даний момент не існує єдиної міжнародної конвенції про кіберпростір (в цілому єдиним міжнародним договором у цій сфері є регіональна Конвенція про злочинність у сфері комп'ютерної інформації 2001 року, прийнята в рамках Ради Європи [9]), не впливає на застосування міжнародного гуманітарного права до кібероперацій під час збройних конфліктів через те, що воно розроблено таким чином, що застосовується «до всіх форм воєнних дій та всіх видів зброї», включаючи «воєнні дії та зброю майбутнього [8]». Проте розробка такого документа є вкрай бажаною для забезпечення кібербезпеки загалом. Таким чином, будь-які нові норми повинні взяти за основу і зміцнити існуючу правову базу, включаючи міжнародне гуманітарне право. Цієї ж думки дотримується і Міжнародний комітет Червоного Хреста у своєму документі (листопад 2019 року) [10].

Таблиця 2

Проблеми, що стосуються застосування МГП по відношенню до кібероперацій

Проблема № 1	Незважаючи на те, що склався певний консенсус щодо того, що «міжнародний збройний конфлікт виникає тоді, коли держави вдаються до збройної сили щодо між собою», ми не можемо сміливо говорити про те, що сама по собі воєнна кібероперація може стати початком збройного конфлікту. тобто, що ми не можемо говорити про застосування правила «першого пострілу», який виходить із звичаєвого міжнародного гуманітарного права. Таким чином, ключове питання «чи може сама по собі воєнна кібероперація, яка не підкріплена подальшими збройними діями, є підставою для застосування міжнародного гуманітарного права» залишається без відповіді.
Проблема № 2	Ця проблема стосується захисту даних цивільних осіб, які існують тільки в кіберпросторі (бази даних та інше). Питання, чи можемо ми поширювати такий самий захист на ці дані, що й на цивільні об'єкти? На жаль, очевидної відповіді на це питання немає, а думки експертів розходяться.
Проблема № 3	На жаль, ми повинні розуміти і усвідомлювати той факт, що існує низка організацій, які здатні проводити воєнні кібероперації, однак вони не асоціюють себе з якою б то не було державою (Anonymous [11]) або ж не діють від його імені / не перебувають у його підпорядкуванні (Ukrainian Cyber Alliance), хоча і асоціюють себе з якоюсь певною державою. Таким чином, у ряді випадків можуть виникати деякі проблеми з визначенням статусу того чи іншого «хактивіста» (відмінності між найманцями та добровольцями). Найманці не набувають статусу комбатанта та військовополоненого, проте вони мають право на гуманне ставлення до себе відповідно до спільної ст. 3 Женевських Конвенцій 1949 року [13].

ЛІТЕРАТУРА

1. J. Markoff Before the Gunfire, Cyberattacks. *The New York Times*. 2008. Vol. 1, № 2. URL:https://web.archive.org/web/20190330172829/https://www.nytimes.com/2008/08/13/technology/13cyber.html (date of access: 21.08.2023).

2. I. Traynor Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. 2007. URL:https://www.theguardian.com/world/2007/may/17/topstories3.russia (date of access: 21.08.2023).

3. C.Bing, S. Kelly Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed. *Reuters*. 2021. URL:https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ (date of access: 21.08.2023).

4. T. Rodenhäuser Le droit international humanitaire peut-il limiter la cyberguerre? *ICRC*. 2021. URL: https://www.icrc.org/fr/document/le-droit-international-humanitaire-peut-il%20limiter-la-cyberguerre%3F (date of access: 21.08.2023).

5. Core principles of international humanitarian law. *UNODC*.
URL: https://www.unodc.org/e4j/en/terrorism/module-6/key-issues/core-principles-of-ihl.html (date of access: 21.08.2023).
6. International Humanitarian Law Databases. *ICRC*. Rule 71. URL: https://ihl-databases.icrc.org/customary-ihl/rus/docs/v1_rul_rule71 (date of access: 21.08.2023).
7. Див. ст. 1–2 Додаткового протоколу I до Женевських конвенцій від 8 червня 1977; п. 9 преамбули до Гаазької конвенції II 1899; № 8 преамбули до Гаазької конвенції IV 1907 р.
8. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, International Court of Justice (ICJ), 8 July 1996, P. 86. URL: https://www.refworld.org/cases,ICJ,4b2913d62.html (date of access: 21.08.2023).
9. Конвенція про кіберзлочинність ETS № 185: Рішення Комітету міністрів Ради Європи від 23.11.2001 р. URL:https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 21.08.2023).
10. International Humanitarian Law and Cyber Operations During Armed Conflicts. Presentation of the ICRC Position (November 2019). URL: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf (date of access: 21.08.2023).
11. Coleman, Gabriella (November 4, 2014). Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. Verso Books. ISBN 978-1781685846. URL:https://archive.org/details/2014TheManyFacesOfAnonymous (date of access: 21.08.2023).
12. International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4 December 1989, United Nations. URL:https://ihl-databases.icrc.org/en/ihl-treaties/conv-mercenaries-1989?activeTab=undefined (date of access: 21.08.2023).
13. Summaries of Judgments, Advisory Opinions and Orders of the International Court of Justice (1948–1991). United Nations. 1992. URL: https://legal.un.org/icjsummaries/documents/english/st_leg_serf1.pdf (date of access: 21.08.2023).
14. Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America). Judgment of 27 June 1986, P. 110) – https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-FR.pdf (date of access: 21.08.2023).