DOI: 10.33498/louu-2024-03-034

Лілія Невара

кандидатка юридичних наук, доцентка,
доцентка кафедри міжнародного, цивільного
та комерційного права
Державного торговельно-економічного університету
(Київ, Україна)
Researcher ID: https://publons.com/researcher/2983018/liliia-nevara/
ORCID ID: https://orcid.org/0000-0003-1775-8806,
l.nevara@knute.edu.ua

УДК 341.1/.8

МІЖНАРОДНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРАТАКИ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ КРІЗЬ ПРИЗМУ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА

Анотація. Актуальність теми обґрунтовано стрімким використанням кіберпростору для вчинення серйозних міжнародних злочинів. Держави дійшли консенсусу, що кіберпростір – це нова сфера, яка потребує міжнародно-правового регулювання для запобігання кіберзлочинам і встановлення міжнародної кримінальної відповідальності. Залежність суспільства та збройних сил від цифрових технологій і цифрової інфраструктури обумовлює зростаючу кількість кібератак у рамках збройних конфліктів і гібридних війн. Такі виклики потребують нових підходів до протидії кібератакам. За допомогою міжнародного гуманітарного права можна розкрити критерії, за якими кібератаку можна тлумачити як акт війни та розглянути застосування принципів міжнародного гуманітарного права до кібервійни.

У статті проаналізовано право на самооборону відповідно до ст. 51 Статуту Організації Об'єднаних Націй у відповідь на кібератаку. Обґрунтоване, чи може кібератака вважатися збройним нападом. Авторка дослідила застосовність основних принципів міжнародного гуманітарного права *jus in bello* до кібератак. Кібератаки можуть мати такий самий ефект, як і збройні напади. Вони можуть призвести до порушення прав людини, знищення критичної інфраструктури, втрати життя та майна. Кіберпростір є оперативною зоною військових дій на рівні з суходолом, морем, повітрям. Держави НАТО віднесли кібератаки до головних сучасних гібридних загроз.

У статті проаналізовано експертні висновки, наукові думки, міжнародні акти, що розкривають і встановлюють межі відповідальності за кібератаки. Досліджено юрисдикцію Міжнародного кримінального суду (МКС) щодо злочинів, заподіяних кібератаками, що становлять воєнні злочини. Досліджується пропозиція розширення застосування Римського статуту МКС на кіберпростір. Зростаюча інтенсивність і частота кібероперацій також підкреслює важливість розвитку та вдосконалення власної операційної практики МКС.

Сьогодні, з огляду на стрімкий розвиток нових технологій озброєння, виникає обов'язок міжнародної спільноти систематично проводити оцінку законності зброї, методів і засобів ведення війни. Виникла нагальна необхідність розроблення політики щодо розслідування та переслідування кіберзлочинців, що підпадають під вимоги Римського статуту. Потрібен новий погляд на міжнародне право, яке б враховувало специфіку кіберпростору.

Ключові слова: кібератака; кіберзлочин; збройний напад; самозахист; воєнні злочини; відповідальність; міжнародне гуманітарне право; Римський статут.

Російська збройна агресія проти України, яка розпочалася у 2014 р., має багатовимірний характер і проявляється у завданні максимальної шкоди

цивільному населенню, включаючи використання кіберпростору. Кібератаки часто супроводжуються збройними атаками, а також інформаційно-психологічними та пропагандистськими операціями і становлять гібридну загрозу для сучасного світу. Зі стрімким розвитком інформаційних технологій світ стає більш цифровізованим, і тим смертоноснішими можуть бути кібератаки, що мають більш руйнівні наслідки у випадку збройного конфлікту. Кібератаки можуть приносити не менше шкоди і страждань цивільному населенню, ніж ракетні обстріли. Тому кібератаки можуть прирівнюватись до воєнних злочинів. Міжнародне гуманітарне право зобов'язане запропонувати нові підходи щодо протидії кібератакам і розглянути застосування принципів міжнародного гуманітарного права до кібервійни. Основним завданням, як для України, так і для міжнародних партнерів, є виявлення всіх кореляцій у діях Російської Федерації (далі – РФ), а також необхідність розробити всеохоплюючу стратегію протидії цим атакам на глобальному рівні та притягнення до міжнародної кримінальної відповідальності.

> Інструменти, які використовуються для вчинення серйозних міжнародних злочинів, постійно розвиваються – від куль і бомб до соціальних мереж, інтернету і, можливо, тепер навіть штучного інтелекту. Оскільки держави й інші суб'єкти все частіше вдаються до операцій у кіберпросторі, цим новим і швидко розвиваючим засобом управління державою та ведення війни можна зловживати для здійснення або сприяння воєнним злочинам, злочинам проти людяності, геноциду та навіть агресії однієї держави проти іншої[1].

Кібератаки на цивільну інфраструктуру можуть мати суттєвий вплив на життя людей і такий самий ефект, як і збройні напади, але без фізичної присутності агресора. Вони можуть призвести до порушення прав людини, знищення критичної інфраструктури, втрати життя та майна.

Стаття 51 Статуту Організації Об'єднаних Націй (далі – ООН) зберігає за державами право на індивідуальну або колективну самооборону, якщо відбудеться збройний напад на Члена Організації[2]. Оскільки Статут ООН передбачає застосування сили у відповідь на збройний напад, критичним стає питання про те, чи може кібератака вважатися збройним нападом, і якщо так, то за яких умов. Кіберпростір, як нове поле бою у війні, також може бути захищений згідно зі ст. 51 Статуту ООН. Держави погоджуються, що кіберпростір – це не особлива сфера, вільна від регулювання, а скоріше та, де міжнародне право відіграє чітку роль, як і у повітрі, на суходолі, морі, у космосі. Положення ст. 2 Статуту ООН не стосуються конкретної зброї і застосовуються до будь-якого застосування сили, незалежно від використовуваної зброї, оскільки зброя визначається її дією, а не своєю природою і є засобом вчинення актів насильства проти людей.

[1] Khan K, 'Technology Will Not Exceed Our Humanity' *(Digital Front Lines)* <https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity> (accessed: 19.03.2024).

[2] Статут Організації Об'єднаних Націй та Статут Міжнародного суду <https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf> (дата звернення: 19.03.2024).

Міжнародна група експертів (далі – *IGE*), створена НАТО, розробила Талліннський посібник, де одноголосно погодилася, що кібератака може досягти рівня збройного нападу, і запропонувала використовувати аналогічний метод для визначення того, чи відповідає кібератака порогу збройної атаки. *IGE* (2013) запропонувала використовувати критерії масштабу та наслідків[3]. Критерії масштабу та наслідків порівнюють результат кібератаки зі звичайними атаками. Для визначення того, чи є кібератака збройною атакою, потрібно оцінити її наслідки. Наслідки нападу мають бути безпосередньо пов'язані з причиною і проводяться проти національної критичної інфраструктури. Крім того, зловмисник повинен мати на меті завдання шкоди нападом. Метод аналогії порівнює наслідки кібератаки з наслідками звичайних атак, щоб визначити, чи є кібератака збройним нападом. Деякі прихильники підходу, заснованого на впливі, стверджують, що 'збройний напад має включати насильство та має призвести, як очікується, до поранення, смерті чи пошкодження майна'[4].

Юристи та військові експерти, урядовці та вчені обговорюють застосовність міжнародного гуманітарного права до кібервійни. *IGE* у Талліннському посібнику підтвердила застосовність міжнародного гуманітарного права до кібернетики. Як зазначає Т. Короткий,

> "Талліннське керівництво із застосування міжнародного права до кібероперацій" містить практики, доктрини, оцінку застосовності наявних норм міжнародного права (міжнародного гуманітарного права, права міжнародної безпеки) до кібератак, а також їх кваліфікацію в контексті МГП[5].

Якщо кібератака може бути збройним нападом, як стверджують експерти, то така кібератака може мати далекосяжні наслідки. Однак страх відплати, можливо за допомогою звичайних військових ударів, зможе допомогти стримувати використання кіберзброї.

Збройні кібератаки являють собою застосування сили, яке порушує норми міжнародного гуманітарного права, за винятком випадків самозахисту. *IGE* (2013) встановила, що '<…> право застосовувати силу для самозахисту поширюється за межі кінетичних збройних нападів на ті, які здійснюються виключно через кібероперації' (с. 54). Заява *IGE* посилює концепцію міжнародного гуманітарного права щодо невід'ємного права держави на самооборону. Міжнародне гуманітарне право не обмежує засобів, які використовуються для захисту від збройного нападу. Зброя, заборонена міжнародним гуманітарним правом, включає біологічну та хімічну зброю. Згідно з міжнародним гуманітарним правом і міжнародною групою експертів '<…>

[3] Schmitt M (ed), *Tallinn manual on the international law applicable to cyber warfare* (Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013).

[4] Valeriano B, Maness R, *Cyber war versus cyber realities: Cyber conflict in the international system* (Oxford University Press 2015).

[5] Назарчук І, 'Кібератака на Україну: які висновки, зокрема правові, маємо зробити?' (*Юридична Газета,* 18.01.2022) <https://yur-gazeta.com/dumka-eksperta/kiberataka-na-ukrayinu-yaki-visnovki-zokrema-pravovi-maemo-zrobiti.html> (дата звернення: 19.03.2024).

держава, яка зазнала збройної кібератаки, має право відповісти кінетичною зброєю'[6].

Основою міжнародного гуманітарного права є теорія справедливої війни, включаючи принципи *jus ad bellum* і *jus in bello.* Основні принципи міжнародного гуманітарного права, які регламентують ведення воєнних дій стороною збройного конфлікту: принцип розрізнення; принцип пропорційності; принцип необхідності – є основоположними для *jus in bello.* Вони призначені для захисту цивільних осіб від наслідків воєнних дій. Держава може відповісти на збройну кібератаку за допомогою звичайної зброї. Межі *jus in bello* необхідності та пропорційності будуть застосовуватися до такої відповіді. Тому держава, яка відповіла, повинна показати, що відповідь була необхідною для відбиття атаки. Збройні напади повинні відповідати стандартам цих основних принципів.

Принцип необхідності стверджує, що застосування сили має бути необхідним для досягнення військової мети. Принцип розрізнення вимагає, щоб учасники збройного конфлікту розрізняли цивільні та військові цілі та щоб дії були спрямовані на військові цілі. Він передбачає, щоб сторони збройного конфлікту завжди проводили розрізнення між цивільними особами і цивільними об'єктами – з одного боку, і комбатантами та військовими об'єктами – з другого. Сторона збройного конфлікту може здійснювати напад тільки на комбатантів або на військові об'єкти. Принцип розрізнення закріплений у ст. 48 Додаткового протоколу І Женевських конвенцій[7] та нормі 1 Звичаєвого міжнародного гуманітарного права[8].

'Принцип пропорційності вимагає лише того, щоб будь-яка шкода чи смерть цивільного населення була пропорційна військовій меті'[9]. Пропорційність стосується рівня побічної шкоди цивільному населенню в результаті нападу.

Заборонено застосовувати зброю, снаряди і матеріали, а також методи ведення війни, які можуть завдати надмірних ушкоджень або спричинити зайві страждання. Сторона, що здійснює напад, має зробити все можливе, щоб упевнитися в тому, що об'єкти нападу є військовими цілями. Відповідно до норм звичаєвого міжнародного гуманітарного права напади не повинні спрямовуватися проти цивільних осіб, цивільних об'єктів.

Статут ООН і міжнародне гуманітарне право вважають використання сили несправедливим, за винятком випадків самозахисту. Держави НАТО віднесли кібератаки до головних сучасних гібридних загроз. Кіберпростір є оперативною зоною військових дій на рівні із суходолом, морем, повітрям. Кіберзахист визнано важливим елементом колективної оборони ('кібера-

[6] Cook J L, 'Is there anything morally special about cyberwar?' in J D Ohlin, K Govern, C Finkelstein (eds), *Cyberwar: Law and ethics for virtual conflicts* (Oxford University Press 2015) 16–36.

[7] Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року <https://zakon.rada.gov.ua/laws/show/995_199#Text> (дата звернення: 19.03.2024).

[8] *Звичаєві норми міжнародного гуманітарного права* (Фенікс 2018) 20.

[9] Dinniss H, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012).

така може призвести до застосування положення про колективну оборону (ст. 5) Північноатлантичного договору НАТО'[10]).

Експерти і дослідники дійшли висновку, що кібератака може являти собою збройний напад і таким чином застосовувати закони про збройні конфлікти. Більшість експертів, зокрема й *IGE*, стверджують, що для того, щоб кібератака досягла рівня збройної атаки, кібератака має призвести до втрати життя, поранень та/або фізичних пошкоджень, а її наслідки еквівалентні наслідкам звичайного збройного конфлікту: ефект атаки переважає.

Беручи участь у кібероперацiях, навіть у рамках самооборони, країни повинні приділяти особливу увагу принципу пропорційності *jus in bello.* Принцип пропорційності діє незалежно від того, яка зброя використовується, кінетична чи кібернетична. Будь-який супутній збиток цивільному населенню, включаючи майно, тілесні ушкодження або втрату життя, має бути пропорційним військовій меті. Кіберзброя викликає нові проблеми щодо пропорційності через її неконтрольованість і невибірковість.

Додатковий протокол I Женевських конвенцій посилює та доповнює захист, який надається цивільному населенню під час війни. Протокол базується на принципах *jus in bello* розрізнення, необхідності та пропорційності і разом із Женевськими конвенціями застосовується під час збройних конфліктів і має на меті обмежити жертви та збитки серед цивільного населення.

Учені зазначають, що 'кібератаки під час збройного конфлікту можуть підпадати під дію положень Додаткового протоколу I. Протокол визначає атаку як акт насильства. Додатковий протокол I стосується лише кібератак, які завдають фізичної шкоди або травм'[11].

Міжнародне гуманітарне право дозволяє державі, яка стала жертвою збройної кібератаки, відповісти застосуванням сили, зокрема й звичайної зброї для самозахисту та не робить різниці щодо того, яка зброя використовується, і тому може застосовуватися до будь-якого методу нападу. Держави повинні залишатися обережними щодо запуску кібератак, які можуть завдати фізичної шкоди та/або втрати життя, за винятком випадків самозахисту. *IGE* встановила, що відповідно до міжнародного гуманітарного права держава, яка стала жертвою збройної кібератаки, має право використовувати у відповідь звичайну зброю.

Як зазначає О. Мережко, нині в міжнародному праві поступово формується заборона використання масштабної кіберсили, яка за своїми наслідками може бути співмірною із застосуванням збройної сили. А незастосування сили в міжнародних відносинах є одним із принципів міжнародного права. Він закріплений у ст. 2(4) Статуту ООН. 'Однак, ще необхідно довести, що кіберсила (наприклад, у вигляді серії атак) використовувалася під контро-

[10] North Atlantic Treaty. (1949, April 4). Washington, D.C.: NATO.
[11] Schmitt M, Vihul L, 'The emergence of international legal norms for cyberconflict' in F Allhoff, A Henschke, B J Strawser (eds), *Binary bullets: The ethics of cyberwarfare* (Oxford University Press 2016) 34–55.

лем конкретної держави. Це нелегко, це потребує взаємодії юристів і фахівців з інформаційних технологій'[12].

Міжнародна спільнота може вважати кібератаки, які завдають фізичної шкоди та/або загибель людей, конструктивними актами війни. Це може мати глибокий вплив на життя людей. Спроби вплинути на критично важливу інфраструктуру, таку як медичні заклади чи системи керування виробництвом електроенергії, можуть призвести до негайних наслідків для багатьох, особливо для найбільш уразливих верств та об'єктів. Також зловживання інтернетом для поширення ненависті та дезінформації, що може сприяти чи навіть безпосередньо призводити до скоєння злочинів, мають розглядатись як докази кіберзлочинних дій.

Отже, кібератаку можна розглядати як нову форму збройного конфлікту, зокрема тому, що 'засоби та методи ведення війни, які використовують кібертехнології, підпадають під дію міжнародного гуманітарного права, як і будь-яка нова зброя'[13]. Група експертів у Талліннському посібнику (2017) визнала, що дії, вчинені за допомогою кіберзасобів, можуть кваліфікуватися як воєнні злочини, оскільки право збройних конфліктів застосовується до нових засобів і методів ведення війни, які не передбачалися на момент появи норм звичаєвого права[14].

З початком збройного конфлікту РФ проти України з 2014 р. вона здійснила численні кібератаки на українську державу. У результаті численних кібератак на державні та публічні сайти, мільйони українців залишились без живлення, засобів зв'язку тощо. У 2015 р. РФ запустила *DDoS*-атаки на державні та публічні вебсайти та здійснила кібератаки на об'єкти енергетики[15]. Атаки на енергооб'єкти "Карпаттяобленерго" та "Київобленерго" продемонстрували російські кіберможливості та залишили майже чверть мільйона українців без живлення. Напади ототожнювали з РФ, і в жовтні 2020 р. суд присяжних у Піттсбурзі, штат Пенсільванія, висунув звинувачення шістьом офіцерам російського Головного розвідувального управління[16].

15 лютого 2022 р. російські хакери розпочали найпотужнішу в історії України *DDoS*-атаку, яка, серед іншого, була спрямована на фінансовий сектор (*DDoS*-атака на 15 банківських сайтів, сайтів із доменом *gov.ua,* також сайтів Міноборони, Збройних Сил та Міністерства з питань реінтеграції тимчасово окупованих територій, що тривала близько 5 годин). 23 лютого, перед початком широкомасштабного російського вторгнення в Україну, було повторно атаковано низку державних і банківських сайтів. За даними державного оператора системи передачі електроенергії "Укренерго", пік кібератак проти енергетичного сектору припав на момент підключення

[12] Назарчук (н 5).
[13] ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts,* Report, 311C/n/5.1.2, Pp. 36–37.
[14] Schmitt (n 3) 392.
[15] Shuya M, 'Russian Cyber Aggression and the New Cold War' [2018] 11 (1) Journal of Strategic Security 1–18. https://doi.org/10.5038/1944-0472.11.1.1646.
[16] Kipybida S P, 'Gaps in International Humanitarian Law Regarding the Creation and Deployment of International Volunteer Cyber Armies" (Utica University, graduate work 2022) 55.

української електромережі до європейської *ENTSO-E* (тобто на 23–24 лютого 2022 р.)[17]. Під час деяких атак на "Укренерго" російські хакери навіть не намагались ховати своє походження і використовували російські IP-адреси для сканування мережі державного енергетичного оператора.

Після повномасштабного вторгнення 24 лютого 2022 р. РФ активно продовжує здійснювати кібератаки на цивільну критичну інфраструктуру, цивільне населення. Кількість і темпи кібератак, спрямованих проти України, неухильно зростають, а їхні наслідки становлять загрозу безпеці, життю і здоров'ю українських громадян. Їх уже фіксують мільйонами. РФ скоює кібератаки на критично важливу та цивільну інфраструктуру, поєднуючи з ракетними ударами. Україна вважає ці дії воєнними злочинами та збирає і передає відповідну інформацію до Міжнародного кримінального суду (далі – МКС) в Гаагу.

Під час збройного конфлікту життєво важливо ідентифікувати учасників бойових дій і притягнути підрозділи або командирів до відповідальності за потенційні порушення міжнародного гуманітарного права, якщо вони мають місце. Однак кібероперації не вимагають, щоб суб'єкти загрози діяли в зоні конфлікту чи навіть у тій самій державі.

Переслідування учасників кіберкомбатантів, які активно беруть участь у конфлікті, залежить від того, де комбатант виконував свої операції, які дії виконував, і чи був комбатант залучений до кіберополчення, визнаного та схваленого стороною конфлікту. Більшість держав і міжнародних організацій мають власні закони щодо кіберактивності та несанкціонованого доступу до комп'ютерних мереж. Залежно від того, як кібератор брав участь у конфлікті, важко визначити, яка держава або держави можуть переслідувати підозрювану злочинну діяльність.

Діяльність хакерів або тісно пов'язаних із ними груп є злочинною і може переслідуватись як державою-жертвою, так і приймаючою державою. Росія має довготривалу практику використання та фінансування кіберзлочинців і цивільного населення для проведення кібероперацій проти Естонії, Грузії та України. Російські групи користуються прокурорським імунітетом у Росії, а міжнародна спільність вважає російський уряд відповідальним за напади[18].

Міжнародно-правовий обов'язок щодо дотримання міжнародного гуманітарного права несуть держави. Саме держава несе відповідальність за порушення норм міжнародного гуманітарного права, вчинених усіма гілками влади й особами, що перебувають під її юрисдикцією. І ця відповідальність розповсюджується і на кіберзлочини.

Компетенція МКС заснована на Римському статуті і поширюється на випадки, коли злочин було вчинено на території держави – учасниці Рим-

[17] 'Кібератаки, артилерія, пропаганда. Загальний огляд вимірів російської агресії' (*Державна служба спеціального зв'язку та захисту інформації України,* 17.01.2023) <https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi> (дата звернення: 19.03.2024).

[18] Connell M, Vogler S, 'Russia's Approach to Cyber Warfare' (*CNA,* 2017 March) <https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf> (accessed: 19.03.2024).

ського статуту (ст. 12(2)(a)) або коли це було вчинено громадянином держави-учасниці (ст. 12(2)(b))[19]. 'Юрисдикція Міжнародного кримінального суду розповсюджується і на кібератаки, оскільки вони є новим способом вчинення злочину, новим способом досягнення тих самих цілей, що й кінетична атака'[20]. Стаття 8 Римського статуту передбачає, що суд має юрисдикцію щодо воєнних злочинів, зокрема, якщо вони скоєні в межах плану або політики, або при великомасштабному скоєнні таких злочинів. Воєнними злочинами є серйозні порушення міжнародного гуманітарного права, за які міжнародним правом передбачена міжнародна кримінальна відповідальність як держав, так і конкретних індивідів. Для притягнення індивідів до міжнародної кримінальної відповідальності створюються міжнародні суди та трибунали. Згідно з Міжнародним Комітетом Червоного Хреста, коли кібератаку неможливо контролювати та обмежити лише військовою ціллю, вона становитиме воєнний злочин. Кваліфікація воєнних злочинів може бути застосована до кібератак, якщо вони пов'язані зі збройним конфліктом, міжнародним чи неміжнародним. Воєнні злочини – це серйозні порушення Женевських конвенцій про захист жертв війни (1949 р.) у сенсі ст. 50 першої Женевської конвенції[21], ст. 51 другої Женевської конвенції[22], ст. 130 третьої Женевської конвенції[23], ст. 147 четвертої Женевської конвенції[24], ст. 85 Додаткового протоколу I до Женевських конвенцій[25]. На міжнародному рівні юрисдикція МКС доповнює ширшу юрисдикцію держав і може стати важливою частиною колективної відповіді на злочини у кіберпросторі.

Використання "невибіркової" зброї заборонено згідно з міжнародним гуманітарним правом. Для переслідування в МКС за воєнні злочини, скоєні у кіберпросторі, виникла необхідність внести зміни до ст. 8(2)(b)(xx) Римського статуту. На сьогодні ці питання можуть бути вирішені лише за допомогою додаткової державної практики та потенційної судової практики МКС та інших міжнародних і національних органів.

Прокурор МКС Карім А. А. Хан зазначає, що міжнародне кримінальне правосуддя може і повинно адаптуватися до операцій у кіберпросторі, використання якого зловживається і використовується для ведення війни, для здійснення або сприяння воєнним злочинам, злочинам проти людяності, геноциду та навіть агресії однієї держави проти іншої. Хоча положення Римського статуту не стосується кіберзлочинів і не містить термін "кібератака",

[19] Римський статут Міжнародного кримінального суду від 17 липня 1998 р. <https://zakon.rada.gov.ua/laws/show/995_588#Text> (дата звернення: 19.03.2024).
[20] Blank L R, 'International Law and Cyber Threats from Non-State Actors' (2013) 89 International Law Studies 406.
[21] Конвенція про поліпшення долі поранених і хворих у діючих арміях від 12 серпня 1949 р. <https://zakon.rada.gov.ua/laws/show/995_151#Text> (дата звернення: 19.03.2024).
[22] Конвенція про поліпшення долі поранених, хворих та осіб, які зазнали корабельної аварії, зі складу збройних сил на морі від 12 серпня 1949 р. <https://zakon.rada.gov.ua/laws/show/995_152#Text> (дата звернення: 19.03.2024).
[23] Женевська конвенція про поводження з військовополоненими від 12 серпня 1949 р. <https://zakon.rada.gov.ua/laws/show/995_153#Text> (дата звернення: 19.03.2024).
[24] Конвенція про захист цивільного населення під час війни від 12 серпня 1949 р. <https://zakon.rada.gov.ua/laws/show/995_154#Text> (дата звернення: 19.03.2024).
[25] Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року (н 7).

така поведінка потенційно може відповідати елементам багатьох основних міжнародних злочинів. Таким чином, кібератаки можна вважати новим способом вчинення традиційних дій, які становлять злочин агресії, воєнний злочин, злочин проти людяності або геноцид. Прокурор МКС Карім А. А. Хан заявив, що при дотриманні вимог Римського статуту кіберзлочини можуть підпадати під юрисдикцію МКС[26].

7 вересня 2023 р. Прокурор МКС підтвердив, що має намір переслідувати воєнні злочини у кіберпросторі. Він зазначив:

> Офіс вважає, що за відповідних обставин поведінка в кіберпросторі потенційно може вважатися воєнними злочинами, злочинами проти людяності, геноцидом та/або злочином агресії, і що така поведінка потенційно може переслідуватися в Суді, якщо справа є досить серйозною[27].

Першою справою, яка розглядається, цілком можуть бути кібератаки РФ на цивільну критичну інфраструктуру в Україні. Звинувачення проти російських хакерів у Гаазі змусять 123 країни – учасниці Римського статуту сприяти затриманню та екстрадиції засуджених військових злочинців, включаючи країни, які не мають договорів про екстрадицію зі США. Ці звинувачення також можуть бути поширені на вищі ешелони командування в російській військовій структурі.

Висновки. Зважаючи на викладене вище, можна зазначити, що стрімке використання інформаційного простору призвело до використання його у збройних конфліктах. Кіберпростір став новою сферою ведення гібридних війн, збройних конфліктів та обумовлює зростаючу кількість кібератак. Такі виклики потребують нових підходів до протидії кібератакам та встановлення міжнародно-правової відповідальності. Міжнародна спільнота має змінювати правила, вчасно й адекватно реагувати та протидіяти кіберзлочинам.

З початком збройної агресії 2014 р. Росія супроводжує збройні атаки на Україну кібератаками, які завдають фізичної шкоди та/або призводять до загибелі людей, руйнують цивільні об'єкти. Збройні кібератаки являють собою застосування сили, яке порушує норми міжнародного гуманітарного права, за винятком випадків самозахисту. Відповідно до принципів *jus in bello* міжнародного гуманітарного права держава може відповісти на збройну кібератаку за допомогою звичайної зброї. Отже, кібератаку можна розглядати як нову форму збройного конфлікту, зокрема тому, що засоби та методи ведення війни, які використовують кібертехнології, підпадають під дію міжнародного гуманітарного права, як і будь-яка нова зброя. Міжнародне гуманітарне право розкриває критерії, за якими кібератаку можна кваліфікувати як збройний напад. Міжнародна група експертів визнала, що дії, вчинені за допомогою кіберзасобів, можуть кваліфікуватись як воєнні

[26] 'Кіберзлочини можуть підпадати під юрисдикцію МКС – прокурор Хан' (*Укрінформ,* 22.01.2024) <https://www.ukrinform.ua/rubric-world/3816924-kiberzlocini-mozut-pidpadati-pid-urisdikciu-mks-prokuror-han.html> (дата звернення: 19.03.2024).

[27] Khan (n 1).

злочини, оскільки право збройних конфліктів застосовується до нових засобів і методів ведення війни.

Міжнародно-правовий обов'язок щодо дотримання міжнародного гуманітарного права несуть держави. Саме держава несе відповідальність за порушення норм міжнародного гуманітарного права. І ця відповідальність розповсюджується і за кіберзлочини. За серйозні порушення міжнародного гуманітарного права, до яких відносяться воєнні злочини, передбачена міжнародна кримінальна відповідальність як держав, так і індивідів. Прокурор МКС підтвердив, що має намір переслідувати воєнні злочини у кіберпросторі. Звинувачення можуть бути поширені на вищі ешелони командування в російській військовій структурі, оскільки вони не мають імунітету відповідно до ст. 27 Римського статуту.

REFERENCES

Bibliography

Authored books

1. Dinniss H, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012).
2. Valeriano B, *Maness R, Cyber war versus cyber realities: Cyber conflict in the international system* (Oxford University Press 2015).

Edited books

3. Cook J L, 'Is there anything morally special about cyberwar?' in J D Ohlin, K Govern, C Finkelstein (eds), *Cyberwar: Law and ethics for virtual conflicts* (Oxford University Press 2015).
4. Schmitt M (ed), *Tallinn manual on the international law applicable to cyber warfare* (Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013).
5. Schmitt M, Vihul L, 'The emergence of international legal norms for cyberconflict' in F Allhoff, A Henschke, B J Strawser (eds), *Binary bullets: The ethics of cyberwarfare* (Oxford University Press 2016).
6. *Zvychaievi normy mizhnarodnoho humanitarnoho prava* (Feniks 2018).

Journal articles

7. Blank L R, 'International Law and Cyber Threats from Non-State Actors' (2013) 89 International Law Studies 406.
8. Shuya M, 'Russian Cyber Aggression and the New Cold War' [2018] 11 (1) Journal of Strategic Security 1–18. https://doi.org/10.5038/1944-0472.11.1.1646.

Newspaper articles

9. Nazarchuk I, 'Kiberataka na Ukrainu: yaki vysnovky, zokrema pravovi, maiemo zrobyty?' *(Iurydychna Hazeta,* 18.01.2022) <https://yur-gazeta.com/dumka-eksperta/kiberataka-na-ukrayinu-yaki-visnovki-zokrema-pravovi-maemo-zrobiti.html> (accessed: 19.03.2024).
10. 'Kiberzlochyny mozhut pidpadaty pid yurysdyktsiiu MKS – prokuror Khan' (*Ukrinform*, 22.01.2024) <https://www.ukrinform.ua/rubric-world/3816924-kiberzlocini-mozut-pidpadati-pid-urisdikciu-mks-prokuror-han.html> (accessed: 19.03.2024).

Theses

11. Kipybida S P, 'Gaps in International Humanitarian Law Regarding the Creation and Deployment of International Volunteer Cyber Armies" (Utica University, graduate work 2022).

Websites

12. Connell M, Vogler S, 'Russia's Approach to Cyber Warfare' (CNA, 2017 March) <https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf> (accessed: 19.03.2024).
13. Khan K, 'Technology Will Not Exceed Our Humanity' <https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity> (accessed: 19.03.2024).
14. 'Kiberataky, artyleriia, propahanda. Zahalnyi ohliad vymiriv rosiiskoi ahresii' (*Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy,* 17.01.2023) <https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi> (accessed: 19.03.2024).

Liliia Nevara

INTERNATIONAL LEGAL RESPONSIBILITY FOR CYBERATTACKS DURING ARMED CONFLICT THROUGH THE PRISM OF INTERNATIONAL HUMANITARIAN LAW

Abstract. The relevance of the topic is substantiated by the rapid use of cyberspace for committing serious international crimes. States have reached a consensus that cyberspace is a new area requiring international legal regulation to prevent cybercrime and establish international criminal liability. The dependence of society and the armed forces on digital technologies and digital infrastructure leads to a growing number of cyberattacks in armed conflicts and hybrid wars. Such challenges require new approaches to countering cyberattacks. International humanitarian law can be used to reveal the criteria by which a cyberattack can be interpreted as an act of war and to consider the application of the principles of international humanitarian law to cyberwarfare.

The article analyzes the right to self-defense under Article 51 of the UN Charter in response to a cyberattack. The author substantiates whether a cyberattack can be considered an armed attack. The author examines the applicability of the basic principles of international humanitarian law jus in bello to cyberattacks. Cyberattacks can have the same effect as armed attacks. They can lead to human rights violations, destruction of critical infrastructure, loss of life and property. Cyberspace is an operational zone of military operations along with land, sea, and air. NATO states have identified cyberattacks as a major modern hybrid threat.

The article analyzes expert opinions, scientific opinions, and international acts that disclose and establish the limits of liability for cyberattacks. The International Criminal Court's jurisdiction over crimes caused by cyberattacks, which constitute war crimes, has been examined. The proposal to extend the application of the Rome Statute of the ICC to cyberspace is studied. The growing intensity and frequency of cyber operations also emphasizes the importance of developing and improving the ICC's own operational practices.

Today, given the rapid development of new weapons technologies, the international community has a duty to systematically assess the legality of weapons, methods and means of warfare. There is an urgent need to develop a policy for the investigation and prosecution of cyber criminals under the Rome Statute. A new view of international law is needed that takes into account the specifics of cyberspace.

Keywords: cyberattack; cybercrime; armed attack; self-defense; war crimes; responsibility; international humanitarian law; Rome Statute.