10. Savanets L., Stakhyra H. Ensuring the security of personal data on the internet: the commercial use of personal data by digital content providers. *Актуальні проблеми правознавства.* 2021. № 3. С.110-116.
11. Savanets L., Stakhyra H. Digital consumer – how to protect one in big data economy. *Актуальні проблеми правознавства.* № 3 (23). 2020. С.153–159.
12. Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review.* 2019. № 1. PP.494-620.
13. Zarsky T. Z. Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law.* 2019. № 20(1). PP.157-188.

УДК 341.312

Заставна О.П.

к.ю.н., старший викладач кафедри
міжнародного та європейського права
Західноукраїнський національний університет

КІБЕРОПЕРАЦІЇ У СВІТЛІ ПРАВА ДЕРЖАВИ НА САМООБОРОНУ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

У сучасних умовах кібероперації стали одним із ключових елементів гібридної війни та використовуються паралельно з традиційними військовими засобами. Сторони конфлікту систематично здійснюють кібератаки проти державних органів, енергетичної інфраструктури, фінансової системи, телекомунікаційних мереж та військових ресурсів з метою дестабілізації функціонування ворожої держави, порушення систем управління та створення паніки серед населення. Особливістю сучасних кібероперацій є їх поєднання з інформаційно-психологічними кампаніями та кінетичними ударами, що свідчить про трансформацію кіберпростору у повноцінний театр воєнних дій. Практика російсько-української війни демонструє, що кібератаки можуть мати масштабні

наслідки для національної безпеки держави та фактично наближатися за своїм характером і наслідками до традиційних форм застосування сили.

Метою даного дослідження є встановити, чи можуть держави посилатися на своє право на самооборону відповідно до статті 51 Статуту Організації Об'єднаних Націй (ООН) [1] у випадку здійснення кібероперацій.

Міжнародний Суд ООН у справі «Нікарагуа проти Сполучених Штатів» [2] встановив, що застосування сили буде класифікуватися як збройний напад тоді, коли такі напади досягають певного порогу. Кожен збройний напад є застосуванням сили, але не кожне застосування сили вважається збройним нападом. Лише збройні напади можуть призводити до виникнення права на самооборону.

Точного визначення поняття «зброя» не існує; загалом під зброєю розуміють інструмент, створений та використаний для завдання шкоди або позбавлення життя осіб. Міжнародний комітет Червоного Хреста (МКЧХ) зазначив, що зброя – це насильницькі засоби, які використовуються для завдання шкоди та знищення як матеріальних об'єктів, так і людей [3, с. 237-238]. Подібні елементи до визначення зброї, наданого МКЧХ, можна знайти у Керівництві HPCR з міжнародного права, застосовного до повітряної та ракетної війни (HPCR Manual). У HPCR Manual зброя описується як інструмент, що використовується для пошкодження матеріальних об'єктів та завдання шкоди людям [4, с. 49]. Суд ООН у Консультативному висновку щодо законності ядерної зброї встановив, що принципи міжнародного гуманітарного права можуть застосовуватися універсально та до всіх видів зброї – минулих, сучасних і майбутніх [5].

Більш чітке розуміння визначення зброї може допомогти встановити, чи можуть кібероперації бути класифіковані як зброя та потенційно призводити до застосування статей 2(4) та 51 Статуту Організації Об'єднаних Націй (ООН). Оскільки загальний принцип зброї полягає у тому, що вона створює ризик завдання шкоди людям та фізичному майну, можна стверджувати, що кібероперації можуть розглядатися як форма зброї. Проте для застосування до

кібероперацій статей 2(4) та 51 Статуту ООН (у відповідності до Статей про відповідальність держав за міжнародно-протиправні діяння, 2001 [6]) мають бути виконані певні критерії.

Насамперед кібероперація повинна бути приписана певній державі (принцип атрибуції). Цей критерій є однаково важливим і для інших видів нападів. Якщо державу неможливо притягнути до відповідальності, тоді держава-жертва не має права відповідати заходами самооборони. По-друге, загроза або сам акт повинні досягати певного порогу (критерій тяжкості) для того, щоб вважатися застосуванням сили. Однак саме це і є складною частиною питання, оскільки фактично не існує практики щодо того, наскільки серйозним має бути акт або загроза, щоб «відповідати цьому критерію».

Критерій «порогу», встановлений Міжнародним Судом ООН у вже згаданій справі «Нікарагуа». Водночас у науковій літературі існує широкий спектр поглядів щодо співвідношення між поняттям збройного нападу та застосуванням сили у розумінні статті 2(4) Статуту ООН, включаючи акти агресії.

Відповідно до одного підходу, «збройний напад» та/або «агресія» розглядаються як окремі форми порушення заборони погрози силою або її застосування [7, с. 165-183; 8, с. 108-120]. Саме цю позицію підтримує критерій тяжкості, сформульований Міжнародним Судом ООН. Інший підхід виходить із того, що будь-яке порушення заборони, встановленої статтею 2(4) Статуту ООН, становить збройний напад або агресію [9, с. 795-796]. Вагомі аргументи на користь такого підходу випливають із Резолюції 3314 (XXIX) Генеральної Асамблеї ООН щодо визначення агресії. Стаття 1 Додатка до Резолюції 3314 визначає агресію як «застосування сили державою проти суверенітету, територіальної цілісності або політичної незалежності іншої держави чи будь-яким іншим способом, несумісним зі Статутом Організації Об'єднаних Націй» [10]. З такої точки зору, на думку Роман Квєцєнь (Roman Kwiecień, 2016) імперативний характер може бути притаманний не лише забороні збройного нападу чи агресії, але й самій забороні, закріпленій у статті 2(4) Статуту ООН

[11, с. 27].

Сам Міжнародний Суд ООН відмовився визнавати «менш тяжкі форми» застосування сили збройним нападом та чітко підтвердив цю позицію у рішенні у справі «Oil Platforms» [12]. Інститут міжнародного права у згаданій вище Резолюції щодо застосування збройної сили 2007 року повторили позицію Суду: «Збройний напад, який породжує право на самооборону, повинен досягати певного рівня тяжкості. Дії, пов'язані із застосуванням сили меншої інтенсивності, можуть бути підставою для застосування контрзаходів відповідно до міжнародного права» [13].

Кібероперації можуть становити застосування сили, однак існує ймовірність того, що вони не досягнуть необхідного рівня тяжкості для визнання їх збройним нападом. У такому випадку очевидно, що відповідь щодо права на самооборону буде негативною. Кібероперації можуть мати тенденцію постійно опинятися у так званій «сірій зоні», тобто серед атак, які завдають шкоди державі, але не є достатньо серйозними для застосування статті 51.

Міжнародне право застосовується до кіберпростору так само, як і до традиційних сфер міжнародних відносин; кібератаки не перебувають «поза правом», а держави несуть відповідальність за дії в кіберпросторі – це основні тези Талліннських посібників – експертного дослідження, підготовленого міжнародною групою фахівців під егідою NATO у Таллінні. Перше видання посібників, стосувалося застосування міжнародного права до «кібервійни», згодом було доповнене версією 2.0, що зосереджувалася на ширшому питанні застосування міжнародного права до «кібероперацій» [14].

Щодо збройних нападів, Міжнародна група експертів також одностайно погодилася з тим, що деякі кібероперації можуть бути «достатньо тяжкими», щоб кваліфікуватися як збройний напад, що відповідає Консультативному висновку Міжнародного Суду ООН щодо ядерної зброї, у якому зазначалося, що «вибір засобів нападу не має значення для питання, чи кваліфікується операція як збройний напад» [14, Rule 71].

Дінштейн зазначав що «правові принципи звичаєвого *jus ad bellum* залишаються незмінними незалежно від того, чи є збройний напад кінетичним чи кібернетичним» [15, с. 280]. «Усі збройні напади (які виправдовують індивідуальну та колективну самооборону відповідно до статті 51) повинні оцінюватися за однаковими критеріями незалежно від того, яка зброя використовується» [16, с. 41].

На жаль, чинне міжнародне право надає дуже мало конкретних критеріїв для оцінки масштабу та наслідків. Водночас Таллінські посібники зазначають, що «кібероперація, яка спричиняє серйозні тілесні ушкодження або смерть значної кількості осіб, чи завдає значної шкоди або руйнування майну», досягає порогу збройного нападу [14, Rule 71]. «Використання будь-якого засобу […], яке призводить до значної загибелі людей та/або масштабного знищення майна, повинно вважатися таким, що відповідає умовам збройного нападу» [16, с. 41].

Наведене дозволяє дійти однозначного висновку – до кібероперацій можуть і мають бути застосовані статті 2(4) та 51 Статуту ООН щодо права держави на самооборону, а розвиток кіберпростору потребує переосмислення традиційних підходів до застосування сили у міжнародному праві. Дослідження надало можливість виокремити наступні основні напрями:

1. Кібероперації можуть кваліфікуватися як збройний напад у розумінні статті 51 Статуту ООН за умови, що їх масштаб та наслідки досягають порогу тяжкості, співставного з традиційним застосуванням сили, зокрема у випадках загибелі людей, значного пошкодження критичної інфраструктури або суттєвої дестабілізації функціонування держави.

2. Право держави на самооборону у відповідь на кібероперації залишається обмеженим принципами необхідності, пропорційності та атрибуції, що створює суттєві практичні труднощі через анонімність кіберпростору, складність встановлення держави-відповідача та відсутність чітких критеріїв оцінки масштабу кібератак.

3. Сучасне міжнародне право визнає застосовність чинних норм jus ad bellum до кіберпростору, однак відсутність єдиного міжнародного підходу до

визначення порогу «збройного нападу» у сфері кібероперацій свідчить про необхідність подальшого розвитку міжнародної практики та уніфікації правових підходів держав.

4. Перспективним напрямом удосконалення міжнародного гуманітарного права є розроблення спеціальних міжнародно-правових норм щодо кібероперацій, зокрема визначення правового статусу кібератак на критичну інфраструктуру, критеріїв кваліфікації кібератак, що дозволять співставити їх із кінетичними атаками та критеріїв пропорційності кіберсамооборони.

ЛІТЕРАТУРА

1. Статут Організації Об'єднаних Націй від 26.06.1945 URL: https://zakon.rada.gov.ua/laws/show/995_010#Text
2. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) Judgment of 27 June 1986 (1986) ICJ Rep 14, 286 (Nicaragua case). URL: https://www.icj-cij.org/case/70
3. Jean-Marie Henckaerts and others (eds). Customary International Humanitarian Law (Cambridge University Press 2005). 689 p. URL: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf
4. Harvard School of Public Health (ed), HPCR Manual on International Law Applicable to Air and Missile Warfare (Cambridge University Press 2013) 423 p. URL: https://assets.cambridge.org/97811070/34198/excerpt/9781107034198_excerpt.pdf
5. Legality of the Threat or Use of Nuclear Weapons, (Advisory Opinion) ICJ Reports 1996 p. 226 (8 July 1996) URL: https://www.icj-cij.org/case/95
6. Responsibility of States for Internationally Wrongful Acts. 2001. URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf
7. Y. Dinstein. War, Aggression and Self-Defence (3rd ed.), Cambridge University Press, Cambridge: 2001. 300 p. URL: https://www.cambridge.org/core/books/war-aggression-and-selfdefence/C65C03F29CD58079A78CE3B917054BB1

8. Ch. Gray. International Law and the Use of Force (2nd ed.), Oxford University Press, Oxford: 2004. 355 p.
9. Randelzhofer, Article 51, in: B. Simma (ed.), The Charter of the United Nations: A Commentary (2nd ed.), Berlin: 2002. 895 p.
10. General Assembly of the United Nations. 3314 (XXIX). Definition of Agression. URL: https://docs.un.org/en/A/RES/3314(XXIX)
11. Roman Kwiecień. The Nicaragua Judgment and the Use of Force – 30 Years Later. XXXVI POLISH Yearbook of international law. 2016. pp. 21-36.
12. Case Concerning Oil Platforms (Islamic Republic of Iran v The United States of America) Judgment of 6 November 2003 (2003) ICJ Rep 161-219 (Oil Platforms case) URL: https://www.icj-cij.org/case/90
13. Institut de droit international, Session de Santiago – 2007, Present Problems of the Use of Armed Force. Selfdefence, available at: http://www.idi-iil.org/idiE/resolutionsE/2007_san_02_en.pdf
14. Schmitt N.M, Vihul L. and NATO (eds). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Second edition, Cambridge University Press 2017). 302 p. URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf
15. Dinstein Y. Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference. *International Law Studies*. 2013. pp. 276–287. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1041&context=ils
16. Roscini M. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press. 2014. 44 p. URL: https://www.academia.edu/75038388/Cyber_Operations_and_the_Use_of_Force_in_International_Law