Єлизавета КАРЛЮГА
Одеський національний університет
імені І. І. Мечникова
економіко-правовий факультет,
2 курс магістратури, 2 група

КІБЕРАТАКА ЯК ЗБРОЙНИЙ НАПАД В КОНТЕКСТІ СТ. 51 СТАТУТУ ООН

Події, які мали місце в Естонії (2007 р.), Грузії (2008 р.), Ірані (2010 р.), Україні (2015 р.), поклали початок дискусії про застосовність концепції права на самооборону у випадку кібератаки. Як свідчить аналіз наукової

літератури, обговорення вказаної проблематики триває і дотепер, а досягнення згоди у цьому питанні здається ще далекою перспективою. Водночас, практика міжнародних відносин, як і завжди, схильна йти набагато далі, виробляючи власні підходи до вирішення тих чи інших проблем. Не є виключенням згадана сфера міжнародних відносин, де окремі держави та міжнародні організації формують та проводять самостійну політику щодо права на самооборону у відповідь на кібератаки. Такий стан міжнародних відносин, де за відсутності узгодженої міжнародно-правової бази суб'єкти міжнародного права керуються суперечливими уявленнями про правомірність застосування концепції права на самооборону в кіберпросторі, загрожує наростанням міжнародної кризи, схильної до трансформації у міжнародний збройний конфлікт.

У зв'язку з цим, як нагальна розглядається потреба в створенні єдиного підходу до визначення можливості застосування права на самооборону у випадку кібератаки. Виходячи із змісту ст. 51 Статуту ООН, першочерговим в цьому аспекті постає дослідження перспективи кваліфікації кібератаки як збройного нападу, на чому і пропонується зосередити увагу в межах цього дослідження.

Як здається, відправним пунктом для вищеокресленого напрямку вивчення слугує детермінація ознак однієї з ключових категорій права міжнародної безпеки, а саме категорії «збройний напад». Остання не знайшла свого точного визначення, а її обсяг варіюється в залежності від суб'єкта тлумачення. Так, як вказує С. Ш. Пенк, у 1945 р.автори Статуту ООН, розробляючи термін «збройний напад», мали на увазі напад регулярних збройних сил однієї держави на іншу [1, с. 3]. З позицій упорядників згаданого міжнародного договору вбачається, що визначальною ознакою збройного нападу є його здійснення державою за допомогою її регулярних збройних сил. За такого підходу, можливість визнання кібератаки збройним нападом суттєво ускладнюється, адже зазвичай вкрай важко з'ясувати хто та яким чином здійснює, «атрибутує» кібероперації [2, с. 44], не кажучи вже про безпосереднє встановлення факту використання національних збройних сил.

Протилежного висновку можна дійти, якщо розглядати збройний напад крізь призму ознак, викладених Міжнародним Судом ООН (далі – МС ООН) у рішенні по справі «Нікарагуа проти США». Як вказується у рішенні, «наразі можна вважати, що є згода щодо того, що до збройного нападу має включатися не лише акція регулярних збройних сил, що здійснюється через міжнародний кордон, але також «засилання державою або

від імені держави збройних банд, груп, іррегулярних збройних формувань або найманців, які здійснюють проти іншої держави збройні силові дії, що мають такий значний характер, що дозволяє кваліфікувати їх як фактичний збройний напад, який здійснюється регулярними збройними силами» [3, с. 103]. Така інтерпретація збройного нападу, яка характеризується відходом від традиційної прив'язки до регулярних збройних сил держави, на наш погляд, дозволяє віднести кібератаки до досліджуваної категорії. Аналогічна думка висловлюється О. В. Демідовим, який зазначає, що, незважаючи на відсутність безпосереднього зв'язку між рішенням по справі «Нікарагуа проти США» з кібероперaціями, останнє є досить важливим в контексті сьогоднішніх завдань: по-перше, із рішення слідує, що застосування сили не обмежується прямим використанням збройних сил держави і може включати інші дії, зокрема озброєння, тренування тощо; по-друге, рішення МС ООН відкриває можливість для кваліфікації як застосування збройної сили дій посередників. Обидва висновки є актуальними для кіберпростору [4, с. 110].

Інший підхід до визначення категорії «збройний напад» пов'язується із дефініцією самого терміну «зброя». Одним з представників такого підходу можна вважати доктора філософії І. Кузігу, яка у відповіді на питання, чи є кібератака збройним нападом, спирається на тлумачення понять «озброєний», «зброя». Як наслідок, вчена підсумовує, що зброєю може бути визнана будь-яка річ, яка призначена або використовується для заподіяння матеріальної шкоди або вбивств. Звідси, якщо кібертехнології використовуються для завдання тілесних ушкоджень, фізичної шкоди або вбивств, їх слід розглядати як «зброю» [5, с. 6], а напад з використанням кібертехнологій – збройним. На користь такого необмежувального підходу до визначення «номенклатури» зброї та можливості кваліфікації кібератак як збройних нападів свідчать висновки МС ООН, згідно яких положення ст. 2(4) і ст. 51 Статуту ООН «не стосуються конкретної зброї…Вони застосовуються до будь-якого застосування сили, незалежно від застосованої зброї» [6, с. 4, 22].

Дещо схожим на вищезазначений уявляється останній підхід, відповідно до якого під збройним нападом розуміється будь-яке діяння в залежності від його масштабу та завданих наслідків. Базисом для розвитку цього підходу постало вже згадуване рішення МС ООН по справі «Нікарагуа проти США» [3, с. 103]. Так, прихильники підходу «на основі наслідків» стверджують, що кібератаки, скоєні з наміром заподіяти матеріальні руй-

нування, поранення та/або смерть, аналогічні тим, що здійснюються за допомогою класичної зброї, та мають розглядатися як збройний напад [7, с. 74]. Протилежна думка висловлюється П. Сінгером та Н. Шахтманом, які резюмують, що наслідки кібератак неможливо порівняти з наслідками реальних збройних нападів. На підтвердження своїх висновків дослідники приводять аналіз наслідків кібератак, здійснених проти Естонії, та порівнюють останні з наслідками кібератак, спрямованих проти Грузії і «поєднаних із справжніми ракетами та бомбами у супутній війні» [8].

Окремим аспектом, що розвивається в межах підходу визначення збройного нападу з позицій масштабу та наслідків діяння, є визнання кібератаки збройним нападом в залежності від її спрямованості на завдання шкоди об'єктам критичної інфраструктури [5, с. 8]. В цьому разі необхідно визначити, чи було завдано шкоди об'єктам критичної інфраструктури. Однак, з огляду на те, що дефініція поняття «об'єкт критичної інфраструктури» позбавлена загальноприйнятого визнання, то зрозуміло, що кваліфікація кібератаки як збройного нападу набуває казуального характеру.

Таким чином, на підставі вищевикладеного, можемо зазначити наступне. Потенціал визнання кібератаки збройним нападом згідно з контекстом ст. 51 Статуту ООН перебуває у прямій залежності від трактування самого терміну «збройний напад». Водночас, на сьогодні єдина, усталена інтерпретація вказаного поняття відсутня, що породжує суперечливі підходи до кваліфікації кібератак. У зв'язку з цим та з огляду на «патологічне» відставання міжнародно-правового регулювання кібервідносин, необхідним здається, насамперед, визначити та закріпити на рівні міжнародного договору ознаки, яким має відповідати діяння, аби бути правомірно розціненим як збройний напад.

Список використаних джерел:

1. Pank S. C. What is the scope of legal self□defense in International Law? Jus ad bellum with a special view to new frontiers for self□defense. Aarhus
2. Denmark. Juridik Institut. RETTID. 2014. Specialeafhandling 19, (2014). 47 p.
3. Huang Z. The Attribution Rules in the ILC's Articles on State Responsibility: A Preliminary Assessment of Their Application to Cyber-Operations. *Baltic Yearbook of International Law Online*. 2015. Vol. 14. P. 41–54.
4. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of 27 June 1986 // I. C. J. Reports 1986.

5. Гаврилова М. С., Демидов О. В., Козик А. Л., Стрельцов А. А. Применение международного права в киберпространстве. *Индекс безопасности.* 2015. № 4 (115). С. 99–116.
6. Couzigou I. The Challenges Posed by Cyber Attacks to the Law on Self-Defence. European Society of International Law, 10th Anniversary Conference. Vienna, 4–6 September 2014. Conference Paper № 16/2014. 16 p.
7. Legality of the Threat or Use of Nuclear Weapons. ICJ Advisory Opinion of 8 July 1996. URL: https://www.icj-cij.org/public/files/case-related/95/095–19960708-ADV-01–00-EN.pdf (дата звернення: 08.11.2021).
8. Dinniss H. H. Cyber Warfare and the Laws of War. Cambridge : Cambridge University Press, 2012. 331 p.
9. Singer P. W., Shachtman N. The Wrong War, Foreign Policy 21st Century Defense Initiative. Brookings. 2011. URL:https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/ (дата звернення: 08.11.2021).

Науковий керівник: Нігреєва О. О., кандидат юридичних наук, доцент кафедри загальноправових дисциплін та міжнародного права Одеського національного університету імені І. І. Мечникова.