МІЖНАРОДНЕ ПРАВО

УДК 330.8 / 342.95
DOI https://doi.org/10.32782/chern.v4.2024.15

А. Ю. Ковальчук
доктор юридичних наук, професор,
професор кафедри міжнародного права та галузевих правових дисциплін
Київського університету права Національної академії наук України
orcid.org/0000-0003-4807-2436

Б. В. Чернявська
PhD, доцент кафедри теорії та історії держави і права
Національної академії управління;
запрошений дослідник юридичного факультету
Вільного Університету Амстердаму
orcid.org/0000-0001-8263-7483

МІЖНАРОДНА ПРАВОВА ВИЗНАЧЕНІСТЬ МАСШТАБНИХ КІБЕРАТАК

Нинішня ситуація в світі приносить з собою нові виклики безпеці, що пов'язані з війнами, техногенними катастрофами, які можуть бути спричинені загрозами через здійснення масштабних кібератак. Сучасні кібератаки набули такого розмаху, що спричиняють руйнівні наслідки як і будь-яка фізична зброя на війні. В деяких країнах (Ізраїль, Китай), кібератаки розглядаються як частина військових дій, інші ж країн світу мають сформовані норми у чинному національному законодавстві щодо визначення масштабних кібератак, як злочину. У нових кримінальних інцидентах злочинці атакують різні об'єкти за допомогою новітніх технологій і залишають різноманітні сліди, які не обмежуються лише технологічними алгоритмами. Авторами відзначається тенденції до розширення методології здійснення кібератак, залучення соціальної інженерії та соціального програмування тощо. Зазначається, що в теорії міжнародного кримінального права атаки на комп'ютерні мережі (кібератаки) дедалі частіше пропонується розглядати як акти агресії, фактично наступальна військова операція. Кібератака, розглядається як акт кібергресії і визначається міжнародним злочином, кваліфікація якого здійснюється на міжнародному рівні, що спричиняє поширення режиму міжнародної юрисдикції щодо осіб відповідальних за злочинні діяння. Авторами аналізуються різні підходи у кваліфікації кібератак, робиться огляд національного законодавства деяких країн. У результаті сформовані висновоки про необхідність правового уточнення таких понять як «кібератака», «кіберзагроза», «кібергресія». Правило 30 «Талліннського посібнику з міжнародного права, застосовного до кібервійни» вказує, що кібератака – це кібероперація будь то наступального, чи оборонного характеру, у наслідок якої спричиняється поранення чи смерть людей, або пошкодження чи знищення об'єктів інфраструктури. Теорія міжнародного кримінального права стверджує, що кібератаки можна віднести до різновиду збройного нападу за умови, що такі атаки призводять до наслідків, характерних для традиційного застосування сили – тобто в основу покладаються масштаби небезпечних наслідків. До таких наслідків, пропонується віднести відключення комп'ютерів, які керують гідротехнічними спорудами та дамбами, що призводить до затоплення населених пунктів, значних руйнувань, дезорганізації військової інфраструктури та порушення економічної системи. Також, пропонується визначення кібергресії, як акт агресії, що має незбройний характер і посягають на державний суверенітет. У висновку пропонується репрезентативний досвід Канади, де кібератаки розмежовуються за чотирма видами: кібершпигунство, спонсороване державою; військові дії, де кібератаки є центральним елементом військової стратегії; кібертероризм; кіберзлочинність.

Ключові слова: безпека (кібербезпека), виклики, загроза, державна/національна безпека, кібератака, кіберсфера, міжнародне гуманітарне право, протидія загрозам, правоохоронні органи, правоохоронна діяльність.

Kovalchuk A. Yu., Cherniavska B. V. **DEFINING LARGE-SCALE CYBER ATTACKS IN INTERNATIONAL LAW**
The current global situation brings new security challenges associated with wars and man-made disasters, such as those caused by large-scale cyberattacks. Modern cyberattacks have now reached a scale that they have devastating consequences comparable to physical weapons used in traditional warfare. In some states, such as Israel and China, cyberattacks qualify as military operations. In some states, such as Israel and China, cyberattacks are considered part of military operations. However, even when cyberattacks are part of military strategies, they can still be classified as criminal acts under international law if they cause significant harm to civilian infrastructure, result in casualties, or violate principles of proportionality and distinction. In recent incidents, perpetrators have used advanced technologies to target various entities, leaving behind complex digital footprints that include both traditional technological elements and sophisticated social engineering techniques. A trend can be noted towards the expansion of cyberattack methodologies, including the use of social engineering and social programming techniques. In the theory of international criminal law, there are growing proposals to classify attacks on computer networks (cyberattacks) as acts of aggression, effectively equating them to offensive military operations. If a cyberattack is considered an act of cyber aggression and recognized as an international crime, i.e., an act criminalized at the international level, it triggers the possibility of applying international jurisdiction over individuals responsible for such criminal acts.

Different approaches to the qualification of cyberattacks are analyzed and the national legislations of several states are reviewed. The conclusion highlights the need for legal clarification of terms such as "cyberattack," "cyber threat," and "cyber aggression." Rule 30 of the Tallinn Manual on International Law Applicable to Cyber Warfare states that a cyberattack is a cyber operation, whether offensive or defensive, that results in injury or death of persons, or damage or destruction of infrastructure.

The theory of international criminal law suggests that cyberattacks can be classified as a type of armed attack if they result in consequences similar to those caused by traditional use of force – namely, the scale of harmful consequences. This includes disabling computers controlling hydro-technical facilities and dams, leading to flooding of populated areas, significant destruction, disruption of military infrastructure, and impairment of the economic system. The proposed definition of cyber aggression is an act of non-armed aggression that infringes on state sovereignty, characterized by the use of force against a target. Non-violent operations, such as information-psychological cyber operations (using social engineering methods) or cyber espionage, are not considered acts of aggression. A representative example from Canada is discussed, where cyberattacks are categorized into four types: state-sponsored cyber espionage, military operations where cyberattacks are central to strategy, cyberterrorism, and cybercrime. In conclusion, there is an urgent need for international legal frameworks to clearly define and classify various forms of cyberattacks and to establish jurisdictional guidelines for prosecuting such acts as international crimes.

Key words: security, challenges, threats, state/national security, cyberattack, cybersecurity, cyberspace, international humanitarian law, threat response organization, law enforcement agencies, law enforcement activities.

Постановка проблеми. Сучасні масштабні кібератаки набули такого розмаху, що спричиняють руйнівні наслідки як і будь-яка фізична зброя на війні. У нових кримінальних інцидентах злочинці атакують різні об'єкти за допомогою новітніх технологій і залишають різноманітні сліди, які не обмежуються лише технологічними алгоритмами. Трендом 2023–2024 року стає поширення залучення великих мовних моделей для просування власних інтересів і вчинення кібератак та розширення методології соціальної інженерії та соціального програмування. Згідно зі звітом VERIZON [1] про розслідування порушень даних за 2023 рік, атаки за допомогою методів соціальної інженерії спричиняють 17% усіх порушень даних і 10% випадків кібербезпеки, що робить соціальну інженерію одним із трьох найпоширеніших векторів кібератак. Такі атаки спрямовані на співробітників організації, щоб змусити їх розкрити особисту інформацію. Якщо зловмисникам вдасться зламати паролі співробітників, що захищають корпоративні ресурси, вони можуть отримати несанкціонований доступ до критично важливих даних і систем організації.

Враховуючи залежність сучасного життя від інформаційно-комунікаційних систем, у наслідок щоденного функціонування майже всіх аспектів суспільного життя у кіберпросторі, розробка різноманітних заходів його захисту набуває глобального значення й стимулює науковий пошук вирішення визначеної проблеми. Цифрова трансформація суспільних відносин і широке поширення кібератак у всьому світі призводять до матеріальних, організаційних і репутаційних втрат. У цьому аспекті кібератаки, на інформаційні системи та критичну інфраструктуру багатьох доктринах забезпечення національної безпеки окремих держав, розглядаються як акти кіберагресії, що загрожують не лише національним інтересам, а й міжнародному правопорядку [2; 3; 4]. Кібератаки є найбільш небезпечними, коли вони загрожують критичній національній інфраструктурі, енерго- та водопостачання, великої кількості життям і здоров'ю людей. Їх загрозу підживлює зростаюча оцифровка соціальних послуг, мінливий характер технологій, складність ланцюгів поставок і низьку обізнаність суспільства з кібербезпекою. Критичні системи можуть містити вразливості «нульового дня» – слабкі місця, про які розробники та користувачі не знають, і якими користуються хакери (і іноді державні суб'єкти) для створення «чорних дверей» у системах, надаючи їм привілейований незаконний доступ. За останні роки стрімкого розвитку інформаційних технологій сформовано цілий тіньовий ринок готового шкідливого програмного забезпечення, спеціалістів, що розробляють шкідливий код за запитом клієнта, хакерських об'єднань, що виконують замовлення на конкретні кібератаки чи отримання даних та інші «послуги». Кожний вид атаки має значну варіативність та чисельні механізми реалізації. Тому кожен випадок є унікальним, як і його правова кваліфікація.

Ступінь наукової розробки. Іноземні вчені й практики, а також законодавчі акти окремих країн виокремлюють поняття кібератаки і кваліфікують їх в залежності від наслідків та масштабів негативних подій від їх вчинення (Lilienthal G., & Nehaluddin A.):

– кібератаки публічної дії, спрямовані на ураження комп'ютерних та інформаційно-телемунікаційних систем державних органів, міжнародних організацій, великих підприємств, державних реєстрів, об'єктів критичної інфраструктури та інших [5];

– кібератака індивідуальної дії, спрямовані на заволодіння майном або інформацією певної особи, групи осіб або підприємства.

Щодо правової визначеності «кібератаки» як злочину і акту публічної дії, сформувалося два підходи:

– визначення кібератаки, як злочину у національному законодавстві;

– національним законодавством, не визначена «кібератака» як злочин, а розглядається як міжнародний злочин передбачений нормами міжнародного гуманітарного права (Римський статут, декларації ООН й інші міжнародні правові акти).

Ціль статті. Зробити огляд чинного законодавства окремих країн, а також міжнародного правового визначення кібрзагроз, кіберагресії, кібератаки. В умовах сучасної актуалізації кібервійн, правова визначеність відіграє суттєву роль у протидії розповсюдження кібератак.

Викладення основного матеріалу. Більшість країн Світу визначили кібератаки у національному законодавстві як злочин, разом з тим, вчені з різних країн, вказують на проблеми, що виникають з надмірною правовою визначеністю й колосальною різницею між формулюванням самої дії у кіберпросторі. Така теза обґрунтовується поступовим зростанням різноманітності форм, методів здійснення кібератак. Кіберзлочинність носить транскордонний характер відповідно, протидіяти їх злочинам у межах однієї країни, навіть передбачивши самі суворі кримінальні переслідування стає дедалі важче. Окрім того, обмежене розуміння технологій, задіяних у кібератаках часто є проблемою для розробки організаційно-правових заходів з протидії кібератакам.

У Великобританії кібератака, визначається як злочин публічної та індивідуальної дії. У Законі «Computer Misuse Act 1990», в статті 3 визначені основні кібератаки, у тому числі і DDoS-атаки, які носять індивідуальний характер. «Кібератаки – це злочин, що охоплює хакерські дії організацій і осіб, які знають, що їх дії завдадуть, або можуть завдати серйозної шкоди, і мають намір настання шкоди. Правопорушення також може бути скоєно через необачність». Статтею 3ZA Закону «Computer Misuse Act 1990» передбачено відповідальність за несанкціоновані дії, що викликають або створюють ризик серйозної шкоди. Зазначена норма спрямована на припинення посягань на об'єкти критично важливої національної інфраструктури (залежно від мотивів виконавця також може бути застосоване антитерористичне законодавство)[6]. Кібератаки розглядаються як дуже небезпечні агресивні дії, через загрозу стабільності та здоров'ю суспільства та громадськості. Максимальний термін покарання становить 14 років, або довічне ув'язнення, якщо дія вчинена з усвідомленням того, що вона може завдати значних збитків добробуту людей або національній безпеці країни [6]. У США основи кібербезпеки визначені у Computer Fraudand Abuse Act [7], там же передбачена відповідальність за кібератаки. Provision sof the Computer Fraud&Abuse Act 18 U.S.C. § 1030: «проникнення в комп'ютер (наприклад, злом) урядового комп'ютера, 18 USC 1030(a)(3); посягання на комп'ютер (наприклад, хакерство), що призводить до доступу до певної урядової, кредитної, фінансової чи комп'ютерної інформації, 18 USC 1030(a)(2); пошкодження урядового комп'ютера, банківського комп'ютера або комп'ютера, який використовується або впливає на міждержавну чи зовнішню торгівлю (наприклад, черв'як, комп'ютерний вірус, троянський кінь, бомба уповільненої дії, атака на відмову в обслуговуванні та інші форми кібератак, кіберзлочинність або кібертероризм), 18 USC 1030(a)(5); вчинення шахрайства, невід'ємною частиною якого є несанкціонований доступ до комп'ютера уряду, банківського комп'ютера або комп'ютера, який використовується або впливає на міждержавну чи зовнішню торгівлю, 18 USC 1030(a)(4); погроза пошкодити державний комп'ютер, банківський комп'ютер або комп'ютер, який використовується або впливає на міждержавну чи зовнішню торгівлю, 18 USC 1030(a)(7); торгівля паролями для урядового комп'ютера, або якщо торгівля впливає на міждержавну чи зовнішню торгівлю, 18 USC 1030(a)(6); доступ до комп'ютера для здійснення шпигунства, 18 USC 1030(a)(1) [8].

Це лише кілька прикладів країн, де національним законодавством передбачено відповідальність за кібератаки, незалежно від масштабів наслідків й об'єкта атаки. Важливо зауважити, що закони і міра відповідальності можуть різнитися в кожній країні в залежності від реальних загроз, а також загальної цифровізації усіх сфер держави.

Разом з тим, виникає й нова проблема, яка обумовлюється необхідністю розширення меж повноважень правоохоронних органів для забезпечення встановлених правил, що нерозривно призводить до проблеми пошуку балансу між дотриманням свобод громадян у цифровому просторі та забезпеченням загальної кібербезпеки. Так, наприклад, у Великій Британії та США навіть при детальній правовій визначеності, й передбаченій кримінальній відповідальності за кібератаки, наголошують про труднощі, що супроводжують процес доказування такого злочину, це пов'язано у першу чергу з тим, що є значний відсоток непомічених атак, які дозволяють хакерам стежити за клієнтами певний час. Дослідження динаміки й різноманітності кібератак [9] вказує на збільшення інтенсивності кібератак, які вчиняються невизначеними суб'єктами, на елементи програмного забезпечення, що належить корпораціям, чиї продукти, як правило, вбудовані в ланцюги поставок критичної інфраструктури. Такий захід спричиняє значні негативні наслідки, але вчиняється з метою дискредитації крупних постачальників програмного забезпечення. Так саме імітуються кібератаки, з метою підкреслення власного іміджу, як структури яка здатна створити надійне програмне забезпечення. Таким чином, стати лідером на

економічному ринку програмних послуг. Одним із найбільш складних аспектів є те, як уряди, наймані хакери та корпорації взаємодіють у розробці та використанні технологій, це додатково створює складнощі у кваліфікації й доказуванні даного злочину. Так наприклад, *Pegasus,* дуже складне шпигунське програмне забезпечення, спочатку було розроблено ізраїльською фірмою, яка створює технологію для «запобігання та розслідування» тероризму та злочинності. *Pegasus* також використовувався урядами для стеження за внутрішніми опонентами, які не мають відношення до тероризму чи злочинності, включаючи політиків, журналістів і активістів. Вірус Stuxnet став відомим у 2010 році як перша програма зловмисників, скерована проти підприємств важливої інфраструктури, як от станції з вироблення електроенергії. Фахівці з антивірусної компанії Symantec повідомили, що вірус надходив на підприємства хвилями, часом уже через 12 годин після написання нової версії. Походження цього вірусу остаточно не відомо, разом з тим, він вперше став відомим коли його застосували з метою нападу на іранську ядерну програму, включно з процесами збагачення урану у спеціальних центрифугах [10].

Chatham house досліджуючи проблему доказування кіберзлочинів, зазначає про такий метод реалізації кібератаки, як велика кількість однотипних атак вчинялися протягом кількох років на певні об'єкти у наслідку, вони спричиняли значні матеріальні та фізичні збитки, насправді ж, було встановлено, що структурно така атака виглядала як сукупність агресивних дій, що походили від величезної кількості одночасних і часто непов'язаних незначних атак [11].

Інші країни, які не визначили кібератаку, як злочин у національному кримінальному законодавстві, розглядають її як дію держави, проти іншої держави і кваліфікувати, як порушення статті 2(4) Статуту ООН: «Стаття 2(4) Статуту ООН: «Усі Члени Організації Об'єднаних Націй утримуються в своїх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і якимось іншим чином, несумісним із Цілями Об'єднаних Націй» [12]. Lilienthal G., &Nehaluddin A. (2015) обґрунтовують це тим, що сучасні соціально-економічні, геополітичні, культурні та інформаційно-технологічні процеси зумовлюють виникнення нових ризиків і загроз стабільності, правопорядку, суверенітету, територіальній цілісності та незалежності окремих держав, що, зрештою, висуває на перший план необхідність концептуально-правового осмислення статус безпеки в центрі уваги тих деструктивних проявів міжнародних відносин, які зазіхають або створюють загрозу міжнародному миру та безпеці всього людства [13; 14].

Ізраїль виклав свою офіційну позицію щодо застосування норм міжнародного права до атак у кіберпросторі: «звичайна погроза силою або її застосування – як державним, так і недержавним суб'єктом – застосовна в кіберсфері надає невід'ємне право на самооборону від фактичного чи неминучого застосування сили в кіберсфері, що є збройним нападом. Разом з тим, зауважується, що згідно чинного законодавства застосування сили має включати фактичне чи очікуване, пряме чи непряме, фізичне пошкодження, каліцтво чи смерть»[15]. Фундаментальні принципи міжнародного гуманітарного права (далі – МГП) застосовуються до кібероперацій, які проводяться в контексті збройного конфлікту. Кібероперації, які спричиняють звичайну втрату або погіршення функціональності інфраструктури, можуть порушити зобов'язання за міжнародним гуманітарним правом – наприклад, якщо скомпрометована інфраструктура служить для медичних цілей, атака може порушити зобов'язання поважати та захищати медичні підрозділи згідно з нормами міжнародного гуманітарного права [15]. Ізраїль не має позиції щодо точного обсягу правового захисту, наданого міжнародним правом законним інтересам суверенітету держав щодо захисту їхньої кіберінфраструктури та даних – незалежно від того, чи розташовані дані та інфраструктура на території держави чи за її межами. Але,Уряд Ізраїлю ставить під сумнів адекватність традиційного розуміння правила невтручання, під час бойових дій. Окрім того, невизначеність суб'єктів здійснення атаки, їх приналежності до урядів окремих країн, або ж недержавні хакерські угрупування не дають змогу визначити суб'єкта для міжнародної кваліфікації такого злочину. Отже, Ізраїль вважає, що поки не було достатньо поширеної державної практики чи *opinio juris*, які могли б виправдати поширення на кіберсферу звичаєвих норм міжнародного права про належну обачність, розроблених в інших сферах, Ізраїль буде вважати, це військовою дією. «Атрибуція кібератаки залишається здебільшого технічним питанням, яке не слід надмірно регулювати і згідно з міжнародним правом не існує абсолютного обов'язку повідомляти ворожу іноземну державу заздалегідь про вжиття проти неї кібер контрзаходів, враховуючи побоювання, що попереднє оголошення кібер контрзаходів може зробити контрзахід малоефективними» [15].

У Китаї кібератаки визначено як операція у кібервійні. Після того, як 31 грудня 2015 року Народно-визвольна армія Китаю створила кіберармію «Сили стратегічної підтримки» паралельно армії, флоту та авіації, останніми роками вона продовжувала зміцнювати свій потенціал у кібер-

бою. У зв'язку з цим Цай Сонгтін підкреслив, що «APT 41» має дуже великий арсенал шкідливих програм. За приблизними підрахунками, існує близько 30 активних хакерських груп з Китаю, включаючи «APT41» [16]. Відповідно, як й будь-яка операція у бойових діях розробляється стратегічно як комплекс заходів наступу так і захисту. Такий підхід застосовують й інші країни. Відповідно, заходи захисту, протидії повинні відповідати існуючим загрозам.

Деякі країни разом з відповідальністю за кібератаки передбачають ряд заходів упереджувального характеру щодо захисту критичної інфраструктури і кіберпростору. Стратегія інформаційної безпеки Японії представляє реальну небезпеку масштабних кібератак для Японії у світлі іноземних інцидентів (Сполучені Штати та Південна Корея) та функціональний зв'язок між багатьма аспектами економічної діяльності та соціального життя, з одного боку, а інформаційно-комунікаційні технології – з іншого. Стратегія також закріплює спеціальні заходи щодо протидії широкомасштабним кібератакам, які проявляються у посиленні контролю над кіберзлочинністю, міжнародній взаємодії у сфері забезпечення національних інтересів у кіберпросторі, а також активній взаємодії держави та приватного сектору.

Стратегія кібербезпеки Канади від 2010 року [17] описує суспільну небезпеку сучасних кібератак, яка полягає в настанні серйозних наслідків для приватних і суспільних інтересів (зокрема, підрив електричних мереж, збій роботи водоочисних споруд, збої в роботі телекомунікаційних мереж, підвищення собівартості продукції, порушення конфіденційності, втрата інтелектуальної власності тощо). У Стратегії пропонується розмежувати всі кібератаки за чотирма видами: кібершпигунство, спонсороване державою; військові дії, де кібератаки є центральним елементом військової стратегії; кібертероризм; кіберзлочинність.

Отже, аналіз стратегій у сфері боротьби з кіберзлочинами на сучасному етапі свідчить, як про спільні, так і про відмінні особливості концептуальних, доктринальних та прикладних підходів до кваліфікації визначених злочинних діянь у даній сфері, що обумовлено різним баченням пріоритетів у сфері інформаційної безпеки держав-учасниць їх інституційною спроможністю, й різний рівень їх інформаційного розвитку. Окрім того, кібератаки, як вид кіберзагроз, у сучасних умовах розвитку інформаційно-цифрового середовища розглядаються в багатьох доктринах національної безпеки як нові виклики, що загрожують не лише національним інтересам, а й міжнародному правопорядку. Тобто, у масштабі цей злочин носить наддержавний характер.

Уточнення потребує й міжнародні положення й акти щодо кваліфікації кібератак. Резолюція Генеральної Асамблеї ООН «Визначення агресії» 1974 року надає юридичне визначення агресії (стаття 1), а також неповний перелік актів агресії (стаття 3). На перший погляд, буквальне тлумачення цих актів не дозволяє зробити висновок про можливе розглядання кібератаки як акту агресії, оскільки мова йде про традиційне застосування збройної сили. Однак, необхідно розуміти той факт, що цей перелік не є вичерпним, і Рада Безпеки ООН може визначити, що інші акти є агресією згідно з положеннями Статуту ООН (ст. 4). Розуміючи розмах розвитку і поширення інформаційно-телекомунікативних технологій європейськими експертами разом з НАТО розроблено «Талліннський посібник з міжнародного права, застосовного до кібервійни 2.0» (2013) [18]. У Талліннських вказівках щодо застосування правових норм міжнародного права до військових операцій у кіберпросторі визначено, що застосування сили може охоплювати дії, вчинені в кіберпросторі, і призводити до наслідків, порівнянних з наслідками традиційного використання збройні сили. Тобто, на міжнародному рівні спостерігається тенденція визнавати використання атак на комп'ютерні мережі актом агресії й терору [18]. Правило 30 Талліннського посібнику з міжнародного права, застосовного до кібервійни вказує, що кібератака – це кібероперація будь то наступального чи оборонного характеру, яка, як обґрунтовано очікується, спричинить поранення чи смерть людей, або пошкодження чи знищення об'єктів. Це визначення однаково застосовується до міжнародних і неміжнародних збройних конфліктів. Поняття «атака» є поняттям, яке являє собою основою для ряду конкретних обмежень і заборон у праві збройних конфліктів. Наприклад, цивільні особи та цивільні об'єкти не можуть піддаватися «нападу» (Правило 32). Це правило встановлює визначення, яке спирається на визначення, яке міститься в статті 49(1) Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року: ««Напад» означає акти насильства щодо противника незалежно від того, здійснюються вони під час наступу чи під час оборони. Положення цього Протоколу, що стосуються нападів, застосовуються до всіх нападів незалежно від того, на якій території вони здійснюються, включаючи національну територію, яка належить стороні, що перебуває в конфлікті, але є під контролем супротивної сторони». Положення цієї статті застосовуються до будь-яких воєнних дій на суші, у повітрі або на морі, які можуть завдати шкоди цивільному населенню або цивільним об'єктам, що розміщені на суші. Вони також застосовуються до всіх нападів з моря або з повітря на об'єкти,

що розміщені на суші, але не торкаються будь-яким чином норм міжнародного права, застосовуваних у період збройних конфліктів на морі або в повітрі» [19]. Згідно з цим загальноприйнятим визначенням, саме використання насильства проти цілі відрізняє напади від інших військових операцій. Ненасильницькі операції, такі як психологічні кібероперації або кібершпигунство, не вважаються атаками. «Акти насильства» не слід розуміти обмежено, лише як дію, яка вивільняє кінетичну силу. У зв'язку з цим зауважується, що хімічні, біологічні чи радіологічні атаки зазвичай не мають кінетичного впливу на визначену ціль, але загальновизнано, що вони є атаками з точки зору закону. Суть поняття полягає в наслідках які викликані певними діями. Щоб кваліфікуватись як акт насильства, дія має призвести до значних негативних наслідків. Наслідки кібероперації, а не її характер, загалом визначають обсяг терміну «атака»; «насильство» слід розглядати в сенсі наслідків насильницьких дій і не обмежується лише самими діями. Наприклад, кібероперація, яка змінює роботу системи, що контролює електричну мережу, і призводить до пожежі, відповідає таким вимогам, за масштабом наслідків. Оскільки наслідки руйнівні, операція є нападом. Тип непрямої шкоди, кваліфікує дію як напад, існують нюанси щодо її застосування. Правила пропорційності говорять про «втрату цивільних осіб, поранення цивільних осіб, пошкодження цивільних об'єктів або їх поєднання». Правила, що стосуються захисту навколишнього середовища, посилаються на «широко поширену, тривалу та серйозну шкоду», а захист дамб і атомних електростанцій визначено в термінах «серйозних втрат серед цивільного населення».

Атака, яка була успішно перехоплена і не призвела до реальної шкоди, все одно є атакою за правом збройних конфліктів. Таким чином, кібероперація, яка зазнала поразки за допомогою пасивних засобів кіберзахисту, таких як брандмауери, антивірусне програмне забезпечення та системи виявлення або запобігання вторгненням все ж кваліфікується як атака, якщо за відсутності такого захисту це могло б спричинити необхідні наслідки. Кібероперації можуть бути невід'ємною частиною більш широкої операції, яка є атакою. Як приклад, кібероперація може бути використана для вимкнення захисту цілі, яка згодом піддається кінетичній атаці. У такому випадку кібероперація є одним із компонентів операції, яка кваліфікується як кібератака. Закон про збройні конфлікти щодо атак повністю поширюється на такі кібероперації [18]. Головний прокурор Міжнародного кримінального суду (МКС) Карім А. А. Хан виділяє «кібератаку» як міжнародний злочин відповідно до Римського статуту. Обґрунтовуючи свою думку положеннями Талліннського посібника з міжнародного права 2.0 (2013) [20]. Карім А. А. Хан зазначає, що Римський статут хоча прямо не криміналізує таку поведінку, разом з тим, кібератаки можуть становити порушення, оскільки вони «потенційно відповідають елементам багатьох основних міжнародних злочинів. Прокурор вважає встановлену правову базу Римського статуту достатньо широкою та гнучкою, щоб боротися з кіберзлочинами, не вимагаючи запровадження нових правил або розширення діючих норм для цього. На його думку, Талліннський посібник передбачає, що «розумне очікування» травм, смерті чи руйнування є ключовою умовою справжньої «кібератаки». Вимога фактичної шкоди, таким чином, теоретично може виключати ситуації, коли веб-сайти урядових установ зіпсовані або заповнені розподіленими атаками на відмову в обслуговуванні (DDoS) як «частина загальної кампанії переслідувань і деморалізації громадськості», якщо фізичної шкоди не завдано. Такі занепокоєння потенційно висвітлюються в остаточному звіті Ради радників із застосування Римського статуту Міжнародного кримінального суду до кібервійни, на який посилається Карім А. А. Хан. У звіті міститься кілька важливих рекомендацій: по-перше, відповідно до Статті 52(2) API, що напад можна вважати таким, що відбувся, коли ціль «нейтралізована», а не знищена відразу. Таким чином, у контексті кіберпростору стверджується, що «порушення або припинення функціонування критичної інфраструктури держави чи створення перешкод військовим можливостям, навіть якщо критична інфраструктура чи військова техніка фізично не знищено, може кваліфікуватися як напад відповідно до МГП. По-друге, у звіті маються поради вважати «цивільні дані законом захищеним об'єктом». Таким чином, націлювання на інформацію про персональні дані може кваліфікуватися як масштабна кібератака. На підтримку цієї точки зору у звіті наведено важливий приклад націлювання на особисті медичні дані пацієнтів, які зберігаються в цивільному чи військовому госпіталі, видалення яких серйозно підірвало б допомогу, яку можна надавати хворим і пораненим.

Висновки. Сучасні збройні конфлікти є гібридними, що виражаються у використанні різноманітних форм і засобів ведення війни, а кіберзброї надається ключове значення в контексті реалізації концепції та стратегії ведення кібервійни. Як у міжнародній практиці так і у теорії міжнародного кримінального права склалося кілька підходів у сфері міжнародно-правового визначення кібератаки та кіберагресії. Природа збройних нападів зазнає закономірних змін у зв'язку з активним використанням засобів інформаційних технологій проти об'єктів інформаційно-критичної інфраструктури інших дер-

жав. Теорія міжнародного кримінального права стверджує, що кібератаки можна віднести до різновиду збройного нападу за умови, що такі атаки призводять до наслідків, характерних для традиційного застосування сили. До них пропонується віднести відключення комп'ютерів, які керують гідротехнічними спорудами та дамбами, що призводить до затоплення населених пунктів, руйнування інформаційної безпеки, дезорганізації військової інфраструктури та порушення економічної системи не менше, ніж пряме використання збройних сил. З іншого боку, також висловлюються позиції щодо кваліфікації кібератак як незбройних форм агресії. Втручання у внутрішні справи держави чи посягання на державний суверенітет на сучасному етапі може здійснюватися за допомогою кібератаки, яка за певних умов може бути кваліфікована як акт агресії, що має незбройний характер. При цьому необхідно розуміти, що правова сутність агресії, як злочину проти міжнародного миру виражається не стільки в об'єктивному аспекті (застосування збройної сили однією державою проти іншої), скільки в контекстному елементі, що діє як особлива ознака міжнародного злочину (крім ознак складу злочину). Контекстуальним елементом міжнародного злочину є певна умова, яка повинна супроводжувати вчинення самого діяння і це зумовлює його найвищу суспільну (міжнародну) небезпеку.

Література

1. Top 10 Best-Known Cybersecurity Incidents and What to Learn from Them (2024). URL: https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches

2. Blanck L. R. (2013). International Law and Cyber Threats from non-states Actors. International Law Studies, 89(406), 406-409.

3. Country Wiki. Octopus Cybercrime Community. (Вікі-профілі надають огляд політики країни щодо кіберзлочинності та електронних доказів). URL: https://www.coe.int/en/web/octopus/country-wiki

4. Російські кібероперації «Аналітика за перше півріччя 2023 року. Зміна тактик, цілей і спроможностей хакерських груп уряду рф. та контрольованих ним угруповань». Аналітичний звіт. URL: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi

5. Кіберзлочинність: актуальна судова практика (2022) // Liga zakon.URL:https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika

6. Computer Misuse Act 1990.URL: https://www.legislation.gov.uk/ukpga/1990/18/contents

7. Закон про комп'ютерне шахрайство та зловживання (CFAA). URL:https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

8. Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws. URL: https://www.everycrsreport.com/reports/97-1025.html#_Toc401151140

9. The 5 5—Russia's cyberstatecraft (2022). Atlantic Council.URL: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-russias-cyber-statecraft/

10. Stuxnet – перша цифрова зброя-вірус? URL: https://www.bbc.com/ukrainian/news/2011/02/110215_stuxnet_virus_oh

11. Whatis a cyberattack? Chathamhouse. URL: https://www.chathamhouse.org/2022/02/what-cyber-attack

12. Статут ООН. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf

13. Lilienthal, G., &Nehaluddin, A. (2015). Cyber-attackas Inevitable KineticWar. ComputerLaw&SecurityReview, 31(3), 390-400. URL: https://repo.uum.edu.my/id/eprint/18674/

14. History of Cyber Warfare and the Top 5 MostNotoriousAttacks.URL: https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare

15. Israel, Cyber attacks and International Law (2020).URL: https://www.lawfaremedia.org/article/israel-cyberattacks-and-international-law

16. 紅色網戰：中國駭客組織發起網路攻擊鏈，台灣百處基礎設施如何防備？ URL:https://www.twreporter.org/a/prochina-hackers-cyberattack-taiwan-critical-infrastructure

17. Canada's Cyber Security Strategy. For a stronger and more prosperous Canada. (2010). URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/canadaNCSS.pdf

18. Талліннський посібник з міжнародного права, застосовного до кібервійни, 2013. URL:https://csef.ru/media/articles/3990/3990.pdf

19. 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

20. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine): Some Preliminary Reflections (and its implications for Ukraine): Some Preliminary Reflections (2023). URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-the-international-criminal-court-and-its-implications-for-ukraine-some-preliminary-reflections/