УДК 341.48/.49

ЯЦИШИН М.Ю., старший викладач кафедри міжнародного права
Навчально-наукового інституту міжнародних відносин
Національного авіаційного університету

ВИКОРИСТАННЯ СИЛИ У КІБЕРПРОСТОРІ В РАМКАХ МІЖНАРОДНОГО ПРАВА

Анотація. *У статті досліджується питання міжнародно-правової кваліфікації кібервоєн. Розглядається співвідношення понять "кібератака", "кібернапад", "кіберзлочин" та "кібервійна", на підставі чого автор пропонує власні дефініції. Детально аналізуються підстави застосування норм міжнародного гуманітарного права і міжнародного кримінального права до кібервоєн. Досліджується проблеми поширення дії основних принципів міжнародного права у кіберпросторі. Автор акцентує увагу на кваліфікаційних ознаках, відповідно до яких акти кібервійни можуть бути визнані злочином агресії.*

Ключові слова: *кібервійна, кіберзлочинність, інформаційно-комунікаційні технології, злочин агресії, основні принципи міжнародного права.*

Summary: *The article deals with the issues of international legal qualification of cyberwar. The correlation between the concepts of "cyberattack", "cybercrime" and "cyberwar (cyberwarfare)" is considered. On this basis, the author offers his own distinctions. The reasons for applying international humanitarian law and international criminal law norms to cyberwar are analyzed in detail. The article deals with the problem of extending the basic principles of international law in cyberspace. The author focuses on the cyberwar qualifications, according to which such acts can be recognized as a crime of aggression.*

Keywords: *cyberwar, cybercrime, information and communication technologies, crime of aggression, principles of international law.*

Аннотация. *В статье исследуется вопрос международно-правовой квалификации кибервоен. Рассматривается соотношение понятий "кибератака", "кибернападение", "киберпреступление" и "кибервойна", на основании чего автор предлагает собственные дефиниции. Детально анализируются основания применения норм международного гуманитарного права и международного уголовного права касательно кибервоен. Исследуется проблема расширения сферы действия основных принципов международного права в киберпространстве. Автор акцентирует внимание на квалификационных признаках, согласно которым акты кибервойны могут быть признаны преступлением агрессии.*

Ключевые слова: *кибервойна, киберпреступность, информационно-коммуникационные технологии, преступление агрессии, основные принципы международного права.*

Постановка проблеми. Виходячи із основних принципів міжнародного права, зокрема мирного вирішення спорів та незастосування сили і погрози силою, а також цілей, проголошених Статутом ООН, міжнародне співтовариство зобов'язане вживати всіх необхідних засобів для запобігання та усунення загрози миру. Тому, одним з пріоритетів для міжнародного права є підтримання і захист миру, що неможливо без заборони та виключення війни як засобу ведення національної політики. За таких умов міжнародне нормотворення повинно вчасно реагувати на виклики сучасності, в тому числі на зародження тенденцій до виникнення нових асиметричних джерел сили, серед яких і кібернетичні можливості впливу [1, с. 10].

Резолюцією Генеральної Асамблеї ООН A/RES/55/29 від 11 грудня 2000 року "Роль науки і техніки в контексті міжнародної безпеки і роззброєння" міжнародне співтовариство висловило занепокоєння тим, що застосування науки і техніки можливе і у воєнних цілях, що може значною мірою сприяти удосконаленню та модернізації сучасних систем зброї, зокрема зброї масового знищення. Генеральна Асамблея ООН також з тривогою відзначала, що науково-технічні досягнення можуть бути використані з метою посилення гонки озброєнь, придушення національно-визвольних рухів та позбавлення окремих осіб і народів основних прав [2].

Як слушно зазначав, М. Тухачевський в "Питаннях сучасної стратегії" (1926 р.): "Відповісти на запитання – який характер буде мати уся майбутня війна – неможливо, бо мірою свого розвитку війна змінює свої форми, свій характер і передбачити їх заздалегідь неможливо" [3]. Таким чином, разом із розвитком суспільних відносин слід відзначити і трансформацію міжнародних спорів, які тепер вирішуються не типовими методами та засобами.

Екс-Президент США Обама стверджував, що: "Кіберзагрози можуть нашкодити навіть міжнародному миру і безпеці, оскільки традиційні форми конфлікту розширюються вже і на Інтернет" [4]. Хоча, міжнародне співтовариство неодноразово висловлювало занепокоєння тим, що новітні технології потенційно можуть використовуватися в цілях, несумісних із завданнями щодо забезпечення міжнародної стабільності та безпеки, і в змозі негативно впливати на цілісність інфраструктури держав, порушуючи їх безпеку як у цивільній, так і у військовій сферах (Туніська програма для інформаційного суспільства; Кодекс з захисту прав користувачів в кіберпросторі ЮНЕСКО; Резолюція ГА ООН A/HRC/20/L.13 від 29.06.2012 р.; Резолюції ГА ООН A/HRC/17/27 від 16.05.2011 р. тощо), станом на сьогоднішній день немає жодного міжнародно-правового акту, що містив би визначення "кібервійни" та забороняв її.

Результати аналізу наукових публікацій. Проблематика протидії кібервійнам є порівняно новою, але за рахунок її важливості неодноразово виділялась об'єктом наукових досліджень різних спрямувань. Серед зарубіжних авторів, що внесли значний вклад у розробку окресленої проблеми виділяємо: М. Кеттеманн (M. Kettemann), О. Хетавей (O.A. Hathaway), Дж. Андрес (J. Andress), С. Вінтерфілд (S. Winterfield), Дж. Валух (Jozef Valuch), О. Гамулак (Ondrej Hamulak). Серед вітчизняних фахівців з міжнародного права різні аспекти міжнародно-правової протидії інформаційним та кібернетичним війнам висвітлювали І.М. Забара, О.О. Мережко, А.В. Пазюк.

Найбільш ґрунтовним дослідженням сучасного міжнародного кримінального права є підручник за редакцією Герхарда Верле "Принципи міжнародного кримінального права". Слід відзначити також підрозділ "Злочинність у кіберпросторі: міжнародно-правовий дискурс" у підручнику "Теорія та практика міжнародного права" за редакцією професора Н.А. Зелінської, виданого у 2017 році.

Незважаючи на інтерес вчених до окремих аспектів проблеми протидії кібервійнам, питання міжнародно-правової кваліфікації кібернетичних актів досі залишається дискусійним.

Метою статті є комплексне дослідження міжнародно-правового регулювання застосування сили у кіберпросторі, а завданнями – визначення поняття та кваліфікаційних ознак кібервійни відповідно до норм сучасного міжнародного права.

Її новизна полягає в тому, що вперше у вітчизняній доктрині здійснено комплексне дослідження, в результаті якого надано авторський погляд на питання кваліфікації застосування сили у кіберпросторі як злочину за міжнародним правом.

Виклад основного матеріалу. Поняття “кібервійни” (cyberwar) не є новим, однак єдине узагальнене його визначення відсутнє. У доктрині та практиці міжнародного права паралельно застосовуються такі терміни як: “бойові дії у кіберпросторі” (cyberwarfare), “кібератака” (cyberattack), “кіберзлочинність” (cybercrime). Варто погодитись з автором статті “Коли кіберзлочин є актом кібервійни?” Тоні Бредлі (Tony Bradley), що існують значні відмінності у застосуванні термінів “кіберзлочинність”, “кібервійна”, “кібершпіонаж”, “кібер-хактивізм” та “кібертероризм”, що окрім теоретичної дискусії спричиняє ускладнення процесу визначення, який рівень правоохоронних органів необхідно застосовувати щодо конкретної атаки [5]. Дж. Андрес (J. Andress) і С. Вінтерфілд (S. Winterfield) також стверджують: “Визначити, що таке кібервійна, досить важко. Фактично, обидві дефініції – “кібер” і “війна” – є предметом дискусій” [6].

Ускладнює ситуацію безсистемне використання термінів “кібервійна”, “інформаційна війна”, “гібридна війна” засобами масової інформації як синонімів. Єдиних підходів до розуміння понять “інформаційна війна” та “гібридна війна”, так званих технологій “м’якої сили” сьогодні не існує. За допомогою них вчені часто пояснюють зміни у способах та веденні воєнних дій, які характеризуються поєднанням нетипових для класичного міжнародного права засобів, зокрема інформаційних. В умовах глобального інформаційного простору, з одного боку, весь світ має змогу слідкувати за “полем бою”, а з іншого – відбувається серйозне спотворення у висвітленні подій державами-учасниками конфлікту, в першу чергу, агресором. Однак, на нашу думку, ототожнення названих явищ з кібервійною є необґрунтованим, а їх аналіз виходить за рамки предмету представленого дослідження.

В основі розуміння феномену кібервійни, на наш погляд, лежить співвідношення понять – кібервійна, кібератака чи кібероперація, а також кіберзлочин. На практиці їх досить складно розрізнити, в тому числі відповідно кваліфікувати. Для вирішення термінологічної дискусії можна скористатись підходом, запропонованим Ендрю Стормсом (Andrew Storms), фахівцем з інформаційних технологій та безпеки. На його думку, при неможливості розмежування наведених вище понять, слід видалити префікс “кібер” і застосовувати ті ж рішення, які повинні бути використанні в класичному кримінальному праві [5]. Крім цього, як стверджує автор, важко уявити будь-який акт кібервійни, який також не буде порушенням чинних законів. У цьому сенсі кібервійна завжди є кіберзлочином, але не кожен кіберзлочин може бути визнаний актом кібервійни.

Український вчений О.О. Мережко зазначає, що у міжнародному праві немає чітких критеріїв, за допомогою яких можна було б відокремити акти звичайного комп’ютерного хуліганства від таких нападів, які завдяки своїй серйозності мають характер збройного нападу на державу, або є початком збройної агресії проти певної держави [7, с. 151].

Відповідно до норм сучасного міжнародного права, а саме Додаткового протоколу до Женевських конвенцій від 12.08.1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол І від 08.06.1977 року), в період збройних конфліктів нападами визначаються: “акти насильства щодо противника незалежно від того, здійснюються вони під час наступу чи оборони” (ст. 49) [8]. Названий протокол поширює свою дію на будь-які напади та об’єкти, незалежно від території, на якій вони здійснюються або розташовуються (на суші, у повітрі чи на морі). Звичайно, у 1977 р. кіберпростір ще не існував і не міг бути формально врахованим у положеннях зазначеної статті.

Виникає логічне питання, як можна кваліфікувати у міжнародному праві акти насильства, що здійснюють в кіберпросторі з метою наступу чи оборони. Відповідно до Таллінського посібника із застосування міжнародного права до кібервійни, опублікованого у 2013 році групою спеціалістів з міжнародного права на замовлення Спільного центру НАТО з обміну передовим досвідом у сфері кіберзахисту (NATO Cooperative Cyber Defence Centre of Excellence): "кібератака є кібероперацією, наступальною чи оборонною, внаслідок якої передбачається завдання шкоди або заподіяння смерті людям, пошкодження чи знищення об'єктів" [9]. Посібник, водночас, не має жодної юридичної сили і може використовуватися як довідниковий і рекомендаційний матеріал.

Джозеф Валух (Jozef Valuch) та Ондрей Гамулак (Ondrej Hamulak) в книзі "Застосування сили проти України та міжнародного права" стверджують, що не всі операції та дії в кіберпросторі можна кваліфікувати як кібератаки [10, с. 217-219] . При цьому автори не надають уточнюючого переліку чи класифікації відповідних кібероперацій. Згідно з Таллінським посібником "кібероперація являє собою застосування сили у випадку, коли її масштаб та наслідки можуть зрівнятись з не кіберопераціями, досягаючи рівня застосування сили" [9].

Однак, наведені визначення не дають змогу виділити всі необхідні кваліфікаційні ознаки кібернападу. Не визначаються, зокрема необхідні умови суб'єктного складу – хто та проти кого може їх здійснювати. Діяти у кіберпросторі мають змогу не лише окремі особи, групи осіб чи організації (у тому числі і терористичні), але й держави чи коаліції держав. Особливо вигідно "розмиваються" кордони між війною та миром. Фактично вчинені "кібернетичні атаки" можуть здійснюватися окремо або в поєднанні з іншими нападами та загрожувати суверенітету і безпеці держави. В рамках проведеного дослідження виділяємо три можливі суб'єктних складів кібернетичних нападів:

1) атака здійснюється фізичними або юридичними особами, їх об'єднаннями чи державами проти фізичних чи юридичних осіб або їх об'єднань;

2) атака здійснюється фізичними та юридичними особами, а також їх об'єднаннями самостійно чи за участі (сприяння, фінансування) держави проти держав чи міжнародного правопорядку;

3) атака здійснюється збройними силами або спеціальними підрозділами держави проти інших держав чи міжнародного правопорядку;

У першому та другому випадках матимуть місце факти вчинення кіберзлочинів. Наслідками таких атак може бути нанесення значної шкоди або навіть спричинення смерті людей, пошкодження чи знищення окремих об'єктів. В цьому контексті також важливо відзначити, що в результаті таких атаки можуть бути виведені із ладу навіть об'єкти критичної інфраструктури з масштабними і серйозними наслідки.

Разом із тим, особливого статусу набувають протиправні дії осіб, що підтримуються чи фінансуються державами. Прикладом такої атаки була загроза зловмисного програмного забезпечення Stuxnet, яке розроблено для того, щоб завдати шкоди фабриці зі збагачення урану в Ірані. Stuxnet був створений, щоб пошкодити фізичне обладнання, яке контролюється комп'ютерами. Він використовував програмні модулі, що були націлені на виконання певного завдання шкідливого програмного забезпечення. У Талліннському посібнику визначається, що кібератака з використанням шкідливого програмного забезпечення Stuxnet може бути визнана "озброєним нападом" [9]. Жертви таких атак мають право завдати удару у відповідь з метою самозахисту. Хакери, що беруть участь у конфлікті між державами, автоматично набувають статусу комбатантів.

У третьому випадку, коли атака здійснюється збройними силами або спеціальними підрозділами держави проти інших держав чи міжнародного правопорядку, на нашу думку, обґрунтовано буде говорити про міжнародний кібернетичний напад. А за умов системності таких атак – міжнародний кібернетичний конфлікт (cyberwarfare). Антонович П.І. у статті "Про сучасне розуміння терміну кібервійна", визначає кібернетичну війну як систематичну боротьбу в кіберпросторі між державами (групами держав), політичними групами, екстремістськими і терористичними та ін. угрупованнями, яка проводиться в формі атакуючих та оборонних дій [11, с. 90]. При чому, автор наголошує на системності такої боротьби, тобто цілісності, послідовності, єдності, підпорядкованості заданій меті дій агресора, які поєднуються з іншими діями. Стів Ренджер (Steve Ranger), надаючи визначення бойовим діям у кіберпросторі (cyberwarfare), вказує на ознаку розміру завданої шкоди: "це цифрова атака, яка є настільки серйозною, що може прирівнюватись до фізичної атаки" [12].

Отже, постає наступне дискусійне питання, чи може окремий кібернетичний напад бути визнаним кібервійною, за умови що він призводить до особливо значних негативних наслідків. Також чи можуть визнаватись кібернетичною війною систематичні кібернапади, що не призводять до тяжких наслідків, але здійснюються систематично і цілеспрямовано? Наприклад, DOS-атаки на комп'ютерні системи державних органів Естонії, що здійснювались протягом квітня 2007 року. Однак, ці питання також залишаються відкритими для наукової дискусії, зважаючи на відсутність міждержавного консенсусу.

Важливим в контексті проведеного дослідження є підхід запропонований колективом американських авторів в роботі "Право кібератак" щодо розмежування "кібератаки", "кіберзлочину" та "кібервійни" (cyberwarfare) [13]. В праці визначається, що на відміну від кіберзлочинів, які є порушеннями кримінального права з використанням комп'ютерних технологій і вчиняються недержавними суб'єктами, кібератаки здійснюються для виведення з ладу комп'ютерної мережі з політичних мотивів чи національної оборони. Натомість кібервійна, на думку авторів, є кібератакою, наслідки якої прирівнюються до "озброєного нападу" або здійснюються в умовах озброєного конфлікту. У публікації до кібератак відносяться три види діянь – DOS-атаки, поширення неправомірної інформації та проникнення в комп'ютерну систему, що перебуває під захистом. Однак, всі названі види відносяться до кіберзлочинів. У такому випадку, можна визначати будь-який кіберзлочин кібератакою за умови, що він здійснюється з мотивів політики чи національної оборони.

Міжнародне гуманітарне право та правила і звичаї ведення війни застосовуються під час озброєних конфліктів, як міжнародного, так і неміжнародного характеру. Апеляційна палата Міжнародного кримінального трибуналу по колишній Югославії надала наступне визначення озброєному конфлікту в своєму рішенні від 02.10.1995 року: "озброєний конфлікт відбувається у тих випадках, коли військова сила застосовується державами або коли здійснюється тривале військове насильство між урядами та організованими озброєними групами чи між такими групами всередині однієї держави" [14]. Виходячи із цього положення, на нашу думку, дія міжнародного гуманітарного права може поширюватись і на кібернетичні конфлікти за умови їхньої відповідності таким критеріям, як: 1) кібернетичні засоби впливу будуть кваліфікуватись як військова сила або військове насильство; 2) вони будуть здійснюватися державами або організованими озброєними групами.

Джозеф Валух (Jozef Valuch) та Ондрей Гамулак (Ondrej Hamulak) зазначають, що міжнародне право регулює "cyberwarfare" (бойові дії в кіберпросторі) відповідно до jus

ad bellum і jus in bello, однак через особливу специфіку кіберпростору окремі норми міжнародного права не можуть застосовуватись до нього vis-à-vis, зокрема щодо проблеми юрисдикції [10]. НАТО також повністю визнає дію міжнародного права та міжнародного гуманітарного права у кіберпросторі.

Матіас Кеттеманн (Matthias Kettemann) у статті "Посилення кібербезпеки за рахунок міжнародного права" стверджує, що норми Статуту ООН, які забороняють агресію та втручання є дійсними і для міжнародного права кібербезпеки [15]. За умови відсутності універсального договору щодо кібербезпеки цю сферу, на його думку, можна врегулювати лише на основі звичаїв та основних принципів міжнародного права.

Одним із фундаментальних принципів міжнародного права є принцип суверенної рівності держав, відповідно до якого кожна держава володіє юрисдикцією та владою в межах своєї території, а відповідно і інфраструктури інформаційно-комп'ютерних технологій (ІКТ), що розташована на ній. Саме названий принцип покладає на держави відповідальність забезпечити, щоб жодних атак проти інших країн чи інституцій, які б могли порушити міжнародне право, не було організовано чи здійснено з її території [15].

В справі Corfu Channel Міжнародний суд ООН визнав, що принцип добросусідства (ст. 74 Статуту ООН) означає також зобов'язання кожної держави не дозволяти використовувати власну територію для дій, що суперечать правам інших держав [16]. Принцип "не завдавати шкоди", що був застосований в справах Trail Smelter та Lac Lanoux, отримав нормативне закріплення в Стокгольмській декларації 1972 р., а також Ріо декларації 1992 р. та існує як звичаєва норма.

Особливого значення для регулювання кіберпростору і забезпечення кібербезпеки набув принцип due diligence (належна добросовісність), що широко застосовується для боротьби з тероризмом і фінансуванням тероризму [15]. Виходячи із названих принципів можна говорити про існування зобов'язання держав inter alia попереджати кібератаки, що готуються з їхньої території, та створювати правову систему забезпечення та сприяння кібербезпеці.

У монографії "Проблеми теорії міжнародного публічного та приватного права" О.О. Мережко пропонує проект Конвенції про заборону використання кібервійни в глобальній інформаційній мережі інформаційних і обчислювальних ресурсів (Інтернет). У ст. 1 проекту надається наступне визначення: "кібервійна – використання Інтернету й пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету держави" [7, с. 152]. В проекті автор також пропонує визнати Інтернет загальною спадщиною людства, що підлягає використанню виключно в мирних цілях. Компанія Cisco також визначає кібервійну як Інтернет-конфлікт, який передбачає проникнення у комп'ютерні системи та мережі інших країн [17].

Вважаємо, дещо неточним звуження кібервійни лише щодо використання Інтернету. На нашу думку, кібернетична війна відбувається у кіберпросторі, що є однією із сутнісних ознак цього явища. Зокрема, рішення Сенату США, прийняте у 2009 році, офіційно проголошує кібернетичний простір новим середовищем (domain) ведення бойових дій та визначається доцільність його об'єднання з космічним простором в рамках виконання завдань на новому, "геоцентричному театрі воєнних дій" (Spherical Area of Operation).

В умовах неоднозначності застосування норм міжнародного права до кіберпростору держави здійснюють нарощування власних кібернетичних ресурсів. Так, окремі органи в сфері кібербезпеки створені в більшості держав світу (Франція, Великобританія, США, Німеччина, Російська Федерація, Україна та ін.). Як наслідок, на наш погляд, має місце нова стадія "гонки озброєнь". Тому окремо слід розглянути міжнародні норми, що можуть бути застосовані для регулювання засобів здійснення кібернападів чи атак – кібернетичної зброї.

ІКТ надають нові можливості для удосконалення вже існуючої зброї, а також створення нових її видів. В доктрині існують погляди про необхідність розробки міжнародної угоди про заборону окремих видів новітньої зброї. Формально така домовленість може бути прийнята як додатковий протокол до Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію.

Міжнародне співтовариство активно здійснює дослідження в сфері новітніх озброєнь. Серед таких видів зброї, в першу чергу, слід відзначити бойові автономні роботизовані системи (БАРС), смертоносні автономні засобаи (САЗ), робототехнічні комплекси (РТК). Названі системи є прикладами автономної зброї, що може самостійно виявляти, ідентифікувати та вражати ціль за допомогою відповідних датчиків і штучного інтелекту . Хоча, використання автономних озброєних засобів передбачає існування віртуального простору, де знаходиться відповідне програмне забезпечення, здійснюються автоматизовані процеси, такі види зброї не можна вважати кібернетичними. Автономна зброя застосовуються в фізичному просторі (на суші, в повітрі, на морі).

На думку В. Каберник, кіберзброєю є найрізноманітніші технічні та програмні засоби, найчастіше спрямовані на експлуатацію вразливостей у системах передачі та обробки інформації або програмно-технічних системах (віруси типу Flame, зомбі-мережі, DOS і DDOS-атаки) [18]. П. Паганіні стверджує, що кіберзброя – це певний комп'ютерний код, який використовується або призначений для використання з метою загрози або заподіяння фізичної, функціональної або психічної шкоди структурам, системам або живим істотам [19].

Прикладом кіберзброї в більшості джерел визначається вірус Stuxnet, що описувався вище. Його особлива небезпечність полягає в тому, що він був першим вірусом, який наносив безпосередню фізичну шкоду комп'ютерним системам. Інформатизація та автоматизація багатьох процесів призвела сьогодні до широкого використання ІКТ на підприємствах, виробництві, всіх сферах промисловості, гідро- та атомних електростанціях, транспорті, в медицині тощо. А тому, як зазначає М. Камчатний, кіберзброя уже визначається летальною [20].

Застосування державою кібернетичної зброї, може розглядатись як міжнародний злочин агресії. Найбільш тяжкі міжнародні злочини – це такі міжнародні правопорушення, шо ставлять під загрозу знищення існуючого міжнародного порядку, порушують права та інтереси всього світового співтовариства, як правило вчиняються з неправомірним застосуванням збройних сил, інших неправомірних примусових заходів, ставлять під загрозу існування держави тощо [22, с. 114]. Хоча кібератаки не передбачають застосовування збройних сил у розумінні класичного міжнародного права, використання кібернетичної зброї може поставити під загрозу як національний, так і міжнародний правопорядок. Наприклад, застосування вірусів типу Stuxnet.

Діяння підпадають під дію міжнародного кримінального права, якщо воно відповідає трьом умовам: воно повинно тягнути за собою індивідуальну відповідальність та бути караним; норма, яка встановлює таку відповідальність повинна входити в систему міжнародного права; діяння повинно бути караним незалежно від того, чи включене воно в національне право чи ні [23, с. 38-39]. Злочинами за міжнародним правом є воєнні злочини, злочини проти людяності, геноцид і злочин агресії.

Як зазначається в колективному підручнику під редакцією Герхарда Верле "Принципи міжнародного кримінального права", злочин агресії перебуває "в стані невизначеності" [22, с. 39]. На думку авторів, безпосередньо за міжнародним звичаєвим правом криміналізується виключно агресивна війна (заборона війни передбачена низкою міжнародно-правових актів, серед яких Пакт Бріана-Келлога від 27 серпня 1928 року та Статут ООН). Зміст терміну "акт агресії", відповідно до ст. 39 Статуту ООН, конкретизовано Резолюцією ГА ООН 3314 (XXIX) від 14.12.1974 р., що визначає акт агресії як "застосування озброєної сили державою проти суверенітету, територіальної недоторканості чи політичної незалежності іншої держави" [23]. Злочин агресії охоплює акти меншої інтенсивності та масштабу, аніж війна [23, с. 38]. Як приклад актів агресії різні автори наводять: напад озброєних сил, блокада, надання підтримки озброєним бандам на територіях інших держав тощо. Більш детальний, хоча й невичерпний, перелік дій, що можуть бути кваліфіковані як акт агресії міститься в ст. 3 Резолюції ГА ООН 3314. Тоні Бредлі (Tony Bradley), наприклад, проводить паралель між військово-морською блокадою під час Кубинської ракетної кризи і атаки відмови в обслуговуванні (DOS-атакою) проти державної інфраструктури. За його переконанням, такі дії можуть бути бойовими і агресивними, фінансуватись державою, але не досягати значення "акту війни" [5].

На нашу думку, кібератаки за основними кваліфікаційними ознаками можуть прирівнюватись до дій, передбачених ст. 3b "бомбардування озброєними силами держави території іншої держави або застосування будь-якої зброї державою проти території іншої держави" [24]. Формулювання "застосування будь-якої зброї" може включати в себе розуміння "застосування кіберзброї". З іншої сторони, об'єкт злочину агресії – "проти території іншої держави" опосередковано відноситься до екстериторіального кібернетичного простору.

Для того, щоб кібервійна була кваліфікована за міжнародним правом як злочин агресії, необхідно щоб такі дії відповідали всім елементам, відповідно до Додатку II "Поправки до елементів злочинів" до Римського статуту Міжнародного кримінального суду. Оцінити ступінь порушення кібернетичними атаками Статуту ООН можна відповідно до п. 6 та 7 Додатку III "Положення про розуміння щодо поправок до Римського статуту Міжнародного кримінального суду, стосовно злочину агресії". Так, визначається обов'язковість розгляду всіх обставин кожного конкретного випадку, включаючи тяжкість відповідних актів та їх наслідки, оскільки агресія визнається найбільш серйозною і небезпечною формою незаконного застосування сили. З іншої сторони, встановлюється необхідність наявності трьох компонентів при кваліфікації факту агресії як порушення Статуту ООН: характеру, тяжкості і масштабу. Названі ознаки повинні існувати одночасно, внаслідок чого злочин можна визнати "явним" [24].

Слід наголосити на тому, що аналізоване визначення злочину агресії схвалене Резолюцією ГА ООН № 3314, має характер soft law і потребує конвенційного закріплення. Як стверджує К.А. Важна, наявність факту перетворення положень названої резолюції на звичаєві норми на сучасному етапі є дискусійним [25, с. 92].

Висновки.

Кібервійна – це значні, масштабні, цілеспрямовані та систематичні кібератаки із застосуванням кіберзброї, здійснювані збройними силами та/або спеціальними підрозділами держави проти суверенітету, територіальної цілісності, незалежності іншої держави та міжнародного миру і стабільності.

Кібератака – порушення прав і законних інтересів учасників кіберпростору за допомогою ІКТ, що здійснюються фізичними та юридичними особами за участі (сприяння, фінансування тощо) держав з політичних мотивів. Кібератаки, що фінансуються державами, але за своїм характером не є значними, масштабними та систематичними, не можуть визнаватись кібервійною. Їх можна кваліфікувати як недружні акти.

За умови, якщо кібератака включає здійснення дій, передбачених кримінальним і міжнародним правом, такі діяння можуть бути кваліфіковані як кіберзлочини та міжнародні кібернетичні злочини відповідно.

Норми сучасного міжнародного права, зокрема основні принципи міжнародного права є чинними і для кіберпростору. Це означає, існування заборони здійснювати акти агресії у кіберпросторі на підставі принципів суверенної рівності держав, незастосування сили і погрози силою, невтручання у внутрішні справи, а також спеціальних принципів – добросусідства і due diligence.

Відсутність формально вираженого консенсусу держав та доктринальна невизначеність з питання кваліфікації кібервійни за міжнародним правом залишає його відкритим для дискусії. В таких умовах відбувається процес поглиблення інформаційного протистояння між державами, мілітаризації кіберпростору, розробки кіберзброї, та нарощування кібернетичних потужностей і тактик як національного ресурсу держав. В позитивному праві не існує достатніх запобіжних засобів для захисту слабкої сторони в умовах застосування інформаційних методів впливу. А отже, єдиним виходом для держав є захист і здійснення кібернетичних атак у відповідь.

В сучасній доктрині та практиці міжнародного права існують два можливі підходи до кваліфікації кібернападів, що складають кібервійну. З однієї сторони, на них може поширюватись дія міжнародного гуманітарного права за умови їхньої відповідності таким критеріям, як: 1) кібернетичні засоби впливу будуть кваліфікуватись як військова сила або військове насильство; 2) вони будуть здійснюватися державами або організованими озброєними групами. В рамках віртуального простору розмиваються не лише кордони, а й різниця між воєнними цілями і мирними об’єктами (серед яких і культурні цінності, об’єкти критичної інфраструктури та ін.), між військовим та цивільним населенням. З іншої сторони, кібератаки можна кваліфікувати як злочин агресії за міжнародним кримінальним правом. Таке рішення повинно розглядатись в кожному конкретному випадку, оцінюючи характер, тяжкість і масштаб порушення Статуту ООН. Найбільш обґрунтованим вважаємо визнання кібервійни як акту застосування сили відповідно до Статуту ООН, а в окремих випадках – злочину агресії.

Використана література

1. Антипенко В.Ф. Проблеми ефективності міжнародного права. *Проблеми ефективності міжнародного права*: матер. тез. міжн. наук.-практ. конф., м. Київ, 29 бер. 2013 р. Київ, 2013. С. 9-11.

2. Про використання науково-технічного прогресу в інтересах світу і на благо людства: Декларація ГА ООН від 09 грудня.1975 р. URL: https://undocs.org/ru/A/RES/3384(XXX)

3. Требін М. П. “Гібридна” війна як нова українська реальність. *Український соціум.* 2014. URL: http://nbuv.gov.ua/UJRN/Usoc_2014_3_13

4. International Strategy for Cyberspace, 2011. URL: https://obamawhitehouse.archives.gov /sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

5. Bradley T. When is a Cybercrime an Act of Cyberwar? URL: https://www.pcworld.com/ article/250308/when_is_a_cybercrime_an_act_of_cyberwar_html

6. Andress J., Winterfeld S. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. URL: http://index-of.es/Hack/Cyber%20Warfare.pdf

7. Мережко О.О. Проблеми теорії міжнародного публічного і приватного права. Київ: Юстиниан, 2010. 320 с.

8. Додатковий протокол до Женевських конвенцій від 12.08.1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол I від 08.06.1977 р.). URL: http://zakon.rada.gov.ua/laws/show/995_199

9. The Tallin Manual on International Law applicable to Cyber Warfare Prepared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. URL: http://csef.ru/media/articles/3990/3990.pdf

10. Sayapin S., Tsybulenko E. The use of force against Ukraine and International Law. *Springer*. Netherlands, 2018. 465 p.

11. Антонович П.И. О современном понимании термина “кибервойна”. *Вестник академии военных наук*. 2011. № 2(35). С. 89-96

12. Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict. URL: https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-on line-onflict

13. Hathaway O.A. The Law of Cyber-attack. URL: https://law.yale.edu/system/files/doc uments/ pdf/cglc/LawOfCyberAttack.pdf

14. United Nations International Criminal Tribunal for the former Yugoslavia. URL: http://www.icty.org/case/tadic/4

15. Matthias C. Kettemann. Ensuring Cybersecurity through International Law. URL:https://www. jstor.org/stable/26296737?read-now=1&refreqid=excelsior%3A6fb9e65c043f51fa573028c4c61c9e93 &seq=4#page_scan_tab_contents

16. Summary of relevant aspects of Corfu Channel case (Merits). URL: https://www.iilj.org/wp-content/uploads/2016/08/Summary-of-and-extract-from-Corfu-Channel-Case-United-Kingdom-v-Alb ania.pdf

17. Cisco. Що таке кібервійна? URL: https://static-course-assets.s3.amazonaws.com/Cyber Sec2/uk/index. html#1.4.1.1

18. Каберник В. В. Центр военно-политических исследований. *Кибервойна и кибероружие*. URL: http://eurasian-defence.ru/?q=node/3115

19. Pierluigi Paganini. Cyber Weapons. April 3, 2012. URL:http://securityaffairs.co/wordpress/ 3896/intelligence/cyber-weapons.html

20. Камчатний М. Заборонені засоби ведення кібервійни. URL: http://pgp-journal.kiev.ua/ archive/2017/9/44.pdf

21. Задорожній О.В., Буткевич В.Г., Мицик В.В. Конспект лекцій з основ теорії міжнародного права. Київ: Либідь. 2001. С. 114-115.

22. Верле Герхард. Принципы международного уголовного права: учебник / пер. с англ. С. В. Саяпина. Одеса: Фенікс; Москва: ТрансЛит, 2011. 910 с. С. 38-39.

23. Определение агрессии: утверждено резолюцией 3314 (XXIX) Генеральной Ассамблеи ООН от 14 декабря 1974 года URL: http://www.un.org/ru/documents/decl_conv/conventions/aggres sion. shtml

24. Резолюція RC/Res.6: прийнята консенсусом на 13-му пленарному засіданні 11 червня 2010 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=50984&pf35401 =301758

25. Важна К.А. Визначення агресії у сучасному міжнародному праві: матеріали наук.-практ. конф. *Україна і світ,* м. Київ, 19 квіт. 2016 р. *Україна і світ:* науковий журнал (Факультет журналістики і міжнародних відносин Київського національного університету культури і мистецтв). Київ: КНУКіМ, 2016. Вип. 1. С. 84-92.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~