РОЗДІЛ 11
МІЖНАРОДНЕ ПРАВО

УДК 327.432(477):351.848.2
DOI https://doi.org/10.32782/2524-0374/2023-11/152

КІБЕРАТАКИ РФ НА УКРАЇНУ – ВОЄННИЙ ЗЛОЧИН

RUSSIAN CYBERATTACKS ON UKRAINE – A WAR CRIME

Бондаренко І.Д., к.ю.н.,
доцент кафедри кібербезпеки
Національна академія Служби безпеки України

Шестаков В.І., д.т.н., доцент,
заступник директора
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій
Національної академії Служби безпеки України

В статті розглядається застосування міжнародного гуманітарного права до кібератак. Здійснено визначення правового змісту кібератак, які здійснюються в контексті міжнародного збройного конфлікту. Охарактеризовано динаміку розвитку наукової думки щодо можливості застосування міжнародного гуманітарного права до кіберпростору. Міжнародне гуманітарне право забороняє атаки на цивільне населення і цивільні об'єкти. Стверджується, що ця заборона поширюється на кібератаки, попри той факт що відповідні норми були сформовані задовго до початку використання кіберпростору у воєнних цілях. Обґрунтовано, що кібератаки можуть бути рівноцінними атакам кінетичною зброєю та становити воєнні злочини у випадку, якщо вони спрямовуються проти критичної інфраструктури та призводять до припинення отримання цивільним населенням відповідних послуг. Це відбувається завдяки виведенню з ладу інформаційних систем та втрати об'єктами своєї функціональності. Наведені аргументи щодо помилковості раніше пропонованої експертами концепції «фізичних наслідків», згідно якої критерієм відповідності кібератак поняттю «атака» за міжнародним гуманітарним правом вважалося виключно спричинення нею руйнувань, загибелі чи поранення людей. Розглянуто факти кібератак на критичну інфраструктуру України, у здійсненні яких звинувачуються російські хакери зі складу спецслужб рф та підконтрольних ним хакерських угрупувань. Охарактеризовано правові підстави поширення юрисдикції Міжнародного кримінального суду на ситуацію в Україні. Визначено перспективи розслідування відповідних кібертак як воєнних злочинів Прокурором Міжнародного кримінального суду.

Ключові слова: атака, злочин, кібератака, критична інфраструктура, міжнародний збройний конфлікт, Міжнародний кримінальний суд, розслідування, спецслужба, хакер, шкідливе програмне забезпечення.

The article examines the application of IHL to cyberattacks. It is devoted to the determination of the legal content of cyber attacks, which are carried out in the context of an international armed conflict. Scientific opinion evolution regarding applying of IHL to cyberspace is characterized. IHL prohibits attacks on civilians and civilian objects. It is argued that this prohibition applies to cyberattacks, even though IHL was not originally designed to address cyberwarfare. It is proved that cyber-attacks on civilian objects can be equivalent to attacks with kinetic weapons and constitute war crimes if they are directed against critical infrastructure and lead to termination of relevant services to the civilian population. This happens due to the failure of information systems leading to objects loss of functionality. Arguments are given regarding the unjustification of the concept of "physical consequences" previously proposed by experts, according to which the compliance criterion of cyberattacks with the concept of "attack" under international humanitarian law was considered to be exclusively the destruction, death or injury caused by it. The facts of cyberattacks on ukrainan critical infrastructure, which russian hackers from the special services and hacker groups controlled by them are accused of, are considered. Challenges of applying IHL to cyber domain are discussed.The legal grounds for extending the jurisdiction of the International Criminal Court on the situation in Ukraine are described. The prospects of the investigation of relevant cyber attacks as war crimes by the Prosecutor of the International Criminal Court are defined.

Key words: attack, crime, cyber attack, critical infrastructure, international armed conflict, international criminal court, investigation, secret service, hacker, malware.

Постановка проблеми. Міжнародне гуманітарне право (далі – МГП) встановлює низку обмежень, яких зобов'язані дотримуватися держави під час збройних конфліктів. Вони покликані мінімізувати людські страждання і грунтуються, зокрема, на принципах вибірковості та пропорційності. Одним із обмежень є заборонена атак на цивільні об'єкти, які не є воєнними цілями. Це є злочином за Римським статутом Міжнародного кримінального суду (далі – МКС). Постає питання, чи поширюються відповідні заборони на кібератаки так само як і на атаки кінетичною зброєю.

Слід зазначити, що чинні джерела міжнародного права створені задовго до того як кіберпростір став використовуватись як сфера протиборства. Крім того, міжнародний договір щодо правил поведінки держав у кіберпросторі так само як і практика МКС у цій сфері відсутні. Зазначене стало передумовою винекнення так-званої «сірої зони» правової невизначеності, за якої протягом останнього десятиліття відбулася стрімка мілітаризація кіберпростору, низкою країн були створені кібервійська, а в їх доктринальних документах почав широко використовуватися термін «кібернетичні операції».

Кібератаки стали невідємною компонентою збройної агресії рф проти України. З 2014 року Україна зазнає безпрецедентної кількості потужних кібератак, а напередодні повномасштабного вторгнення наша держава стала найбільш атакованою країною у світі. У проведенні кібератак Україна звинувачує рф, яка для цього використовує кіберпідрозділи спецслужб, спеціально створені та контрольовані хакерські угруповання. Цілями кібератак є, переважно, об'єкти критичної інфраструктури невоєнного характеру, зокрема, енергетичної сфери, порушення функціонування яких безпосередньо завдає шкоду цивільному населенню.

Практичні приклади кібератак рф на Україну яскраво демонструють уразливість інфраструктур, критичну залежність соціуму від їх сталого функціонування. На міжнародному рівні актуалізується дискусія щодо необ-

хідності перегляду правового змісту кібератак як елементу збройного конфлікту, меж дозволеності їх застосування. Зокрема, виникає перспектива визнання кібератак воєнним злочином. Для нашої держави це передбачає можливість притягнення російських хакерів та організаторів їх злочинної діяльності до кримінальної відповідальності саме як воєнних злочинців. В глобальному ж розумінні значущість цього питання виходить далеко за межі російської збройної агресії проти України: наразі можуть бути сформовані правила поведінки держав у кіберпросторі, сам факт існування яких безперечно сприятиме міжнародного миру та стабільності.

Аналіз останніх досліджень і публікацій. Проблема визначення міжнародно-правового змісту кібератак в контексті міжнародного збройного конфлікту є недостатньо розробленою. Протягом останніх двох років зміни безпекової ситуації у світі сприяли суттєвому перегляду міжнародними інституціями своїх поглядів щодо можливості застосування МГП до кіберпростору, що пояснює втрату актуальності частиною наукових публікацій із даної тематики. Серед робіт українських вчених, які становлять науковий інтерес, слід виділити працю К. В. Юртаєвої [1], яка досліджувала питання феномену кібернайманства та існуючі до 2022 року тенденції щодо відповідальності за кіберзлочини, вчинені під час міжнародного збройного конфлікту, та В. В. Музики [2], яка у 2021 році захистила дисертацію на здобуття наукового ступеня доктора філософії з тематики атрибуції кібератак, а також Г. В. Фещукова [3], який у своїй статті окреслив проблеми застосування МГП до кібероперацій. Найбільш актуальними дослідженнями у зазначеній сфері є роботи іноземних вчених-юристів, зокрема: Geers K. [4], Freeman L. [5], Chan Yoon Onn [6].

Мета статті: визначити правові підстави та перспективи кримінального переслідування організаторів і виконавців кібератак рф на критичну інфраструктуру України у Міжнародному кримінальному суді.

Виклад основного матеріалу. 24 березня 2022 року Прокурор МКС Карім Хан у своєму зверненні до Ради Безпеки ООН визнав факт міжнародного збройного конфлікту на території України, що триває з 20.02.2014, та повідомив, що є «розумні підстави вважати, що на території України вчиняються злочини, які підпадають під юрисдикцію МКС». Прокурором МКС було прийнято рішення про початок розслідування ситуації в Україні з 21.11.2013 (пов'язав це із потенційними злочинами розгону Євромайдану, що стало «початком нинішньої ситуації»). Зазначене розслідування охоплює «будь-які минулі та теперішні звинувачення у воєнних злочинах, злочинах проти людяності чи геноциді, скоєних на будь-якій частині території України будь-якою особою». Цьому передувало так-зване «попереднє вивчення» ситуації протягом 2014–2020 років [7].

У межах розпочатого розслідування юрисдикція МКС поширюється на територію України попри той факт, що наша держава не є учасником МКС (не ратифікувала Римський статут, хоча раніше підписала його; має зобов'язання ратифікувати у рамках асоціації з ЄС). Це є можливим, оскільки, спираючись на п. 3 ст. 15 Римського статуту, Україна визнала юрисдикцію МКС ad hoc на підставі заяв Верховної Ради України 2014 і 2015 років (щодо можливого вчинення злочинів проти людяності під час Майдану; злочинів проти людяності та воєнних злочинів на всій території України, включно з Кримом і Донбасом, з 20.02.2014 по теперішній час, без фінальної дати). 03.05.2022 внесено змін до КПК України, відповідно до яких Прокурору МКС було надано безпосередню можливість проводити розслідування на території нашої держави. Ініціатором розслідування МКС ситуації в Україні, яка не є його державою-учасницею, відповідно до процедури, передбаченої у таких випадках Римським статутом, виступив сам Прокурор МКС та окремі країни-члени, що до нього звернулися (42 країни, безпрецедентна кількість в історії суду).

Важливо наголосити, що юрисдикція МКС не заміщує, а доповнює національну. Вона поширюється на територію України у міжнародно-визнаних кордонах 1991 року щодо визначених у Римському статуті злочинів, зокрема, воєнних, вчинених особами будь-якого громадянства з 21.11.2013. Наразі значна кількість воєнних злочинів, вчинених громадянами рф, розслідується правоохоронними органами України за статтею 438 Кримінального кодексу України «Порушення законів та звичаїв війни». Окремі з них можуть бути передані до МКС, зокрема, стосовно вищого воєнно-політичного керівництва рф, оскільки, на відміну від національного права, Римський статут (ст. 27) визначає, що юрисдикція МКС поширюється на всіх осіб, незалежно від їхнього статусу, займаної посади чи імунітету [8]. Слід також зазначити, що у 2017 році після заяв Прокурора МКС про вірогідні злочини, вчинені військовослужбовцями рф на території України, росія направила Генеральному секретарю ООН письмове повідомлення про вихід з під юрисдикції МКС. Але це не обмежує повноваження МКС щодо громадян рф, лише процедурно з неї знімаються зобов'язання співпрацювати з МКС та видавати підозрюваних (які, натомість, мають бути затримані на території решти 124 країн-членів та виданні МКС).

Серед форм об'єктивної сторони складу злочину «Порушення законів та звичаїв війни», передбаченого ст. 438 КК України, є «застосування засобів ведення війни, заборонених міжнародним правом» та «інші порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України». Це, зокрема, атаки на цивільні (невоєнні) об'єкти та на цивільне населення. Так Конвенцією про закони і звичаї війни на суходолі та додатком до неї встановлено, що «Забороняється будь-яким способом атакувати чи бомбардувати незахищені міста, селища, житлові будинки чи споруди» [9], а Додатковим протоколом I до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів, визначено: «для забезпечення поваги й захисту цивільного населення та цивільних об'єктів сторони, що перебувають у конфлікті, повинні завжди розрізняти цивільне населення й комбатантів, а також цивільні й воєнні об'єкти та відповідно спрямовувати свої дії тільки проти воєнних об'єктів» [10].

Порушення відповідних заборон є злочином згідно Римського статуту МКС (підпункти «i» «ii», «iv», «v», «xx» пункту «b» частини 2 статті 8): «навмисні атаки на цивільне населення як таке або окремих цивільних осіб, які не беруть безпосередньої участі у воєнних діях»; «навмисні атаки на цивільні об'єкти, тобто об'єкти, які не є воєнними цілями»; «умисне скоєння атаки, коли відомо, що така атака стане причиною випадкової загибелі чи каліцтва цивільних осіб чи шкоди цивільним об'єктам або великої, довгострокової та серйозної шкоди довкіллю, що буде явно несумісною з конкретною і безпосередньо очікуваною загальною воєнною перевагою», «атака на незахищені та такі, що не є воєнними цілями міста, села, житла чи будівлі або їх обстріл із застосуванням будь-яких засобів», «застосування зброї, боєприпасів та техніки, а також методів ведення війни такого характеру, що спричиняє надмірні ушкодження або непотрібні страждання або які є невибірковими за своєю суттю з порушенням норм міжнародного права збройних конфліктів, за умови, що така зброя, такі боєприпаси, така техніка та такі методи ведення війни є предметом всеосяжної заборони та включені до додатка до цього Статуту шляхом поправки відповідно до відповідного положення, викладеного у статтях 121 та 123» [8].

Значна кількість зухвалих і грубих порушень вищезазначених вимог щодо неприпустимості атак на цивільні об'єкти та цивільне населення були здійснені із застосуванням ракетно-артилерійського озброєння, дронів-камікадзе, тощо і наразі всебічно розслідуються як воєнні злочини українськими правоохоронними органами та на міжнародному рівні. Але для відповідних атак окрім так званої «кінетичної» зброї рф активно застосовує і інший інструментарій, а саме потужні та технічно складні кібератаки, зокрема, на об'єкти критичної інфраструктури невоєнного призначення.

У практиці МКС кібератаки ніколи не розслідувалися, не досліджувалися як «напад» в контексті міжнародного збройного конфлікту, та не розглядалися як воєнний злочин. Відповідно і в Україні такі діяння розслідувалися за ст. 361 КК України як звичайний комп'ютерний злочин приватної особи, тобто безвідносно до факту їх використання як засіб ураження в контексті міжнародного збройного конфлікту. Така ситуація пов'язана із декількома факторами.

По-перше, відсутній профільний міжнародний договір, який би визначав правила поведінки держав у кіберпросторі. Слід наголосити, що Генеральною Асамблеєю ООН з 1998 року було ухвалено 5 резолюцій, що закликали держави розробити такі правила (№ 53/70 у 1998 р., № 58/293 у 2004 р., № 59/62 у 2005 р., № 68/243 у 2013 р., № 76/246 у 2021 р.) та було створено три незалежні «Групи експертів з питань міжнародного права та кіберпростору», які мали здійснити розробку відповідної конвенції (GGE-1 у 2001 р., GGE-2 у 2006 р., GGE-3 у 2016 р.) Але, як зазначав у своїй науковій роботі американський дослідник кібервійни Kenneth Geers, через різне бачення державами питань допустимості використання сили та міжнародної юрисдикції у кіберпросторі зазначений міжнародно-правовий акт так і не був прийнятий [6, с. 47–136].

По-друге, за відсутності профільного міжнародного договору проведення відповідного розслідування вимагатиме вирішення цілої низки складних суперечливих питань на межі технології і права, які виникатимуть з огляду на саму природу кіберпростору, зокрема, таких його суттєвих відмінностей від фізичного світу як транскордонність, широкі можливості анонімізації, що створює перешкоди для так-званої «атрибуції» кібератак, тобто ідентифікації їх реальних виконавців.

Донедавна у межах жодного міжнародного збройного конфлікту кібернетична компонента масштабно не застосовувалася, а питання міжнародно-правового змісту кібератак залишалося теоретичним. Натомість протягом останнього десятиріччя відбулася стрімка мілітаризація кібепростору. Так, наприклад, Китаєм, США, росією першими були створені кібервійська, а усвідомлення масштабу воєнної загрози у кіберпросторі спонукало, зокрема, НАТО, ще у 2016 році визнати його «як сферу операцій, у якій Організація має захищати себе так само ефективно, як і у повітрі, на землі та на морі» [11].

За відсутності конкретних нормативно-визначених критеріїв щодо меж дозволеності застосування кіберпростору у воєнних цілях міжнародною групою експертів під егідою Центру передового досвіду з кібербезпеки НАТО (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE – неурядова, але фінансована НАТО, організація кібербезпекової спрямованості, яка розташовується у м. Таллін, Естонія) у 2013-му та 2017-му році було підготовлено посібники, які хоч і не мають юридичної сили, але містять досить детальні тлумачення та рекомендації щодо застосування міжнародного права до кібервійни та кібероперацій, відомі як «Tallinn Manual 1.0» та «Tallinn Manual 2.0» [12; 13]. Саме у останньому викладено позицію, що так-звана «кібероперація» може вважатися «атакою» згідно МГП, якщо вона: «очікується, що призведе до смерті, поранень або фізичної шкоди» або «спрямована на заподіяння такої шкоди» або «є частиною більшої атаки, яка, очікується, призведе до такої шкоди» (правило 92). За таких умов кібератака, у випадку її спрямованості на цивільні об'єкти чи цивільне населення, становить воєнний злочин (правило 101, 102) [13]. Тобто Tallinn Manual 2.0 відображає певний існуючий на той час консенсус (суто теоретичний), що кібератаки набувають правового змісту «атак» лише тоді, коли їх очікувані наслідки співрозмірні із наслідками атак кінетичною зброєю: призводять до смерті, поранень, фізичного руйнування об'єктів.

Безпрецедентно потужні та технічно складні кібератаки на критичну інфраструктуру України під час міжнародного збройного конфлікту (факт якого юридично визнаний МКС) проводилися росією, а саме кадровими співробітниками кіберпідрозділів ФСБ, ГУ ГШ ВС рф (колишнє ГРУ) та їх «proxy», тобто спеціально-створеними та підконтрольними хакерськими організаціями, зокрема, відомими під назвами: APT28 (Fancy Bear, Sofacy Group), APT29, Gamaredon, Sandworm, Турла, Заря, CyberArmyofRussia, Ember Bear, тощо, – саме так офіційно стверджувало воєнно-політичне керівництво України, низка країн-партнерів, авторитетні кібербезпекові та антивірусні компанії. Окрім оприлюднення технічних звітів та здійснення політичних заяв мали місце і юридичні дії на внутрішньо-національному рівні, а саме у США, де в 2020 році за кібератаки, зокрема на Україну, Міністерством юстиції було висунуто обвинувачення шістьом громадянам росії, яких було ідентифіковано військовослужбовцями ГУ ГШ ВС рф та учасниками хакерської групи «Sandworm» [14].

Характерним є те, що зазначені кібератаки на Україну безпосередньо не призводили до фізичного руйнування устаткування або загибелі людей, що на етапі роботи над Tallinn Manual 2.0 його авторами тлумачилося як умова набуття кібератакою правового змісту «атаки» за МГП (здійснення якої щодо цивільних об'єктів і цивільного населення є воєнним злочином). Попри це кібератаки, так само як і у випадку атаки кінетичною зброєю, виводили з ладу об'єкти критичної інфраструктури завдяки знищенню або пошкодженню штатного програмного забезпечення, припиняючи виконання об'єктом своєї основної функції, подекуди життєво-важливої для цивільного населення. Так, наприклад, знеструмлення значної кількості приватних споживачів, систем теплогенерації, лікарень відбувалося в зимовий період та безпосередньо створювало загрозу життю та здоров'ю населення.

Реальне усвідомлення небезпечності наслідків кібератак протягом останніх років сприяли суттєвому перегляду багатьма європейськими та американськими науковцями їх позиції щодо так-званого «порогу серйозності» («gravity threshold»), якому повинні відповідати кібератаки щоб становити «атаку» за МГП. Мова йде про визнання, що самі комп'ютерні дані, зокрема, в системах управління критичної інфраструктури (навіть за відсутності фактів загибелі та руйнувань) можуть бути таким об'єктом «атаки» [5].

Фактичним відображенням зазначених змін став запит групи юристів Центру прав людини Каліфорнійського університету в Берклі (Berkeley Human Rights Center), який було направлено відповідно до ст. 15 Римського статуту прокурору МКС одразу після оголошення ним 03.03.2022 початку розгляду справи щодо можливих воєнних злочинів, вчинених на території України. У запиті міститься юридичне обґрунтування із клопотанням «розширити сферу розпочатого розслідування, включивши до нього кібердомен поряд із традиційними театрами бойових дій (сухопутний, повітряний, морський та космічний) враховуючи приклади агресивної кіберактивності рф в Україні».

Група юристів з Берклі у своєму документі надала аргументи, що низка кібератак на Україну є яскравим прикладом їх «фізичного ефекту, порівнянного з ефектами

традиційної війни», сфокусувавшись на двох тенденційних кібератаках на об'єкти енергетики, а саме на підстанції «Прикарпаттяобленерго» у 2015 році та на підстанцію «Північна» «Укренерго» у 2016 році, звинувативши у них російське хакерське угруповання Sandworm, підконтрольне ГУ ГШ ЗС рф (колишнє ГРУ) [5]. Обидві кібератаки детально досліджені в експертному середовищі. Щодо них були підготовлені технічні звіти кібербезпековими кампаніями: ESET, Dragos, Symantec, Crowdstrike, ISSP, CyberX, FireEye, а також ICS-CERT.

Перша із зазначених кіберак була реалізована шляхом застосування до SCADA систем підприємства шкідливого програмного забезпечення «BlackEnergy», яке вивело з ладу підстанції «Добровляни», «Калуш, «Стрий», «Долина», «Татарів», що призвело до знеструмлення 225000 споживачів Івано-Франківська та населених пунктів Прикарпаття. Характерним є проведення атаки в зимовий період, а також додаткове застосування заходів посилення її деструктивного впливу шляхом синхронної TDoS атаки (перевантаження та блокування телефонних ліній) і використання програмного забезпечення «KillDisk» для знищення системних файлів, програмних засобів людино-машинного інтерфейсу (HMI), та, навіть, завантажувального сектору (boot record) рабочих станцій SCADA для унеможливлення оперативного відновлення системи.

Друга кібератака 2016 року, відома як «CrashOverride» або «Industroyer» також відбулася у грудні і спрямовувалася на об'єкт енергетики, але вже була технічно складнішою ніж попередня. Зокрема, для проникнення у мережу підприємства також застосовувалася методологія соціального інжинірингу, але використані для встановлення шкідливого коду (який надавав хакерам віддалений доступ до заражених комп'ютерів) макроси документів Microsoft Word за своєю будовою на понад 96 відсотків забезпечували приховування та ускладнення аналізу зловмисного коду і лише їх декілька відсотків виконувало функцію власне доставки коду до системи жертви.

У березні 2023 року вищезазначена група юристів Каліфорнійського університету направила до МКС другий запит стосовно розслідування як воєнних злочинів кібератак російських хакерської групи, звинувативши її також і у проведенні атаки, відомої під назвою «NotPetya», а також атаки на супутники Viasat-2 та Viasat-3 компанії Viasat напередодні повномасштабного вторгнення, що призвело до відключення Інтернету у значної кількості користувачів як в Україні, так і в низці країн ЄС.

Окрім цілей вищезазначених кібератак звертає на себе увагу специфіка, технологічна складність та небезпечність використаного інструментарію, а саме шкідливого програмного забезпечення, орієнтованого на системи промислової автоматизації типу SCADA. Наразі у світі відомо лише про 5 зразків тах засобів, 4 з яких з'явилися в період агресії проти України, а у їх розробці та застосуванні звинувачують саме рф (Triton, Havex, BlackEnergy3, Industroyer, Industroyer2) [5].

Ліндсі Фрімен (Lindsay Freeman), директорка з питань права та політики програми високих технологій Центру прав людини Берклі Каліфорнійського Університету, характеризуючи підготовлене її командою звернення до Прокурора МКС наголошувала на декількох аргументах, чому відповідні звинувачення є юридично-обґрунтованими та мають перспективи судового розслідування у межах юрисдикції МКС. По-перше, відповідні кібератаки вже є детально розслідуваними як приватними структурами, так і в межах американської судової системи. По-друге, кібератаки здійснювалися в контексті міжнародного збройного конфлікту, факт якого офіційно визнаний. По-третє, атаки мають чітку цивільну ціль, враховуючи, зокрема, той факт, що на момент їх проведення ні Західна Україна, ні Київ не були зоною бойових дій. По-четверте, кібератаки відповідають «порогу серйозності», мали безпосередні фізичні наслідки (регіональний блекаут), що спрощує визнання їх еквівалентом «фізичної» атаки згідно МГП. По-п'яте, результати кібератак для цивільного населення. В контексті кібератаки Industroyer на підстанцію «Північна» у грудні 2016 року, Ліндсі Фріман додатково акцентує, що попри той факт, що у блекаут у Києві тривав близько години, технічні розслідування показали, шкідлива програма мала забезпечити фізичне руйнування електрообладнання, яке не відбулося лише через допущену помилку конфігурації [15].

Прокурор МКС прийняв до розгляду звернення групи Берклі Каліфорнійського Університету. Невдовзі з'явилася і публічна інформація від української сторони, а саме керівництва ДССЗЗІ України, що наша держава збирає докази кібератак і надає інформацію МКС з метою висунення звинувачень російським хакерам у воєнних злочинах. При цьому українське слідство акцентує на координації кібератак на критичну інфраструктуру із кінетичними операціями російської армії. Зокрема, поширені ситуації, коли «теплову електростанцію було обстріляно, і одночасно була атакована її корпоративна мережа» [16]. У 2023 році Генеральний прокурор України Андрій Костін також повідомив, що «ми підходимо до розгляду кібератак як воєнних злочинів», а начальник кібердепартаменту СБ України (ДКІБ) Ілля Вітюк заявив: «результати кримінальних проваджень СБУ щодо російських кібератак на Україну мають розглядатися Міжнародним трибуналом як воєнний злочин. Це дозволить притягнути до відповідальності вище воєнно-політичне керівництво країни-агресора, зокрема і спецслужб» [17].

У серпні 2023 року відбулася подія, важливість якої важко недооцінити з позиції МГП та практики його застосування. Карім Хан, Прокурор МКС, у виданні «Foreign Policy Analytics» опублікував статтю, в якій заявив про свій намір розслідувати кібератаки як воєнний злочин: «Спроби вплинути на критично важливу інфраструктуру… можуть призвести до негайних наслідків для багатьох, особливо для найбільш уразливих… Хоча жодне положення Римського статуту не стосується кіберзлочинів, така поведінка потенційно може відповідати елементам багатьох основних міжнародних злочинів… У рамках своїх розслідувань мій офіс збиратиме та розглядатиме докази такої поведінки» [18]. Пізніше речник Офісу Прокурора МКС підтвердив, що відповідне розуміння кібератак є офіційною позицією організації.

У [18] своїй статті Прокурор МКС безпосередньо не вказує на ситуацію в Україні, але зазначає, що «ми повинні показати, що закон здатний допомогти тим, хто опинився на передовій». Цілком очевидно, що в контексті заяв української сторони саме кібератаки рф становитимуть предмет першого відповідного розслідування.

У [18] опублікованому матеріалі також засуджується використання кібероперацій як частини «гібридної стратегії» або «сірої зони» та наголошується, що наразі між державами з'являється консенсус, що кіберпростір «не є особливою сферою, вільною від регулювань», напроти, міжнародне право «має відігравати тут чітку роль». Акцентовано увагу на історичній ролі МКС в контексті формування правил поведінки держав у кіберпросторі: «Міжнародне кримінальне правосуддя може і повинно адаптуватися до нового ландшафту…Юрисдикція МКС може стати важливою частиною колективної відповіді… МКС може стримувати порушників…, його провадження можуть допомогти пом'якшити неоднозначність гібридних стратегій…, допомогти державам та іншим органам діяти відповідно до їх чинного законодавства» [18].

Аргументуючи необхідність визнання кібератак воєнним злочином Прокурор МКС також апелює до попередньо висловленої позиції Міжнародного комітету Червоного Хреста (далі – МКЧХ), що «кібератаки мають відповідати основним принципам розрізнення та пропо-

рційності та мають бути спрямовані лише проти воєнних цілей» [18]. Слід зазначити, що у жовтні 2023 року МКЧХ опублікував більш деталізований прес-реліз, де сформовані правила для цивільних хакерів, які беруть участь у збройних конфліктах, зокрема у неоголошеній війні рф проти України (не затверджені жодним міжнародним договором, мають рекомендаційний характер). У правилах містяться заборони спрямовувати кібератаки на цивільні, зокрема медичні, гуманітарні та інші об'єкти, необхідні для виживання населення або такі, що можуть вивільнити небезпечні сили; використовувати шкідливе програмне забезпечення, яке поширюються автоматично і завдає шкоди як військовим, так і цивільним об'єктам [19].

Стаття Прокурора МКС привернула значну увагу міжнародного наукового та експертного середовища. Водночас, окрім позитивної оцінки заявлених ініціатив у фокусі вчених-юристів є ціла низка проблемних питань, вирішення яких Прокурору МКС доведеться здійснювати у межах його розслідування вперше. Зокрема, це атрибуція кібератак, визначення статусу її акторів та встановлення субординаційної підпорядкованості їх діяльності в контексті існуючого міжнародного збройного конфлікту [3]. Першочерговим же завданням буде юридичне обґрунтування відповідності кібератак «порогру серйозності» атаки згідно МГП.

Таке обгрунтування запропоноване юристами Центру Берклі у запитах до Прокурора МКС грунтується на новому тлумаченні правового змісту кібератак в контексті міжнародного збройного конфлікту. Пропонується відмовитися від концепції «фізичних наслідків» (смерті, поранень чи руйнувань) на користь концепції «наслідків втрати функціональності», яка має місце «якщо цільове обладнання або системи більше не надають послуги, для яких вони були впроваджені, як тимчасово, так і постійно, як за можливості подальшого відновлення їх функціонування, так і без такого [20].

Ця прогресивна концепція відповідає положенню, яке міститься у ст. 52 (2) Додаткового протоколу до Женевських конвенцій 1949 року, що напад можна вважати таким, що мав місце коли ціль «нейтралізована», а не повністю знищена [10]. Стосовно кібератак вона вперше була запропонована у 2021 році так-званою «Радою радників», міжнародною групою юристів, створеною відповідно до резолюції Генеральної Асамблеї ООН A/RES/73/262 під егідою Постійної місії Ліхтенштейну при ООН у відповідь на стурбованість низки держав зростаючою загрозою кібератак. У підготовленому групою звіті «Щодо застосування Римського статуту МКС до кібервійни» міститься рекомендація вважати, що «припинення функціонування критичної інфраструктури держави чи створення перешкод військовим можливостям, навіть якщо критична інфраструктура чи військова техніка фізично не знищені, може кваліфікуватися як напад відповідно до МГП» [21].

Спираючись на концепцію «наслідків втрати функціональності», група юристів Каліфорнійського Університету наголошувала, що кібератаки на критичну інфраструктуру є атаками на кожного споживача відповідних життєво-важливих послуг: «це були не просто атаки на конкретні інфраструктурні об'єкти, а на опалення, яке зігріває людей взимку; системи охолодження, які перешкоджають псуванню їжі, світлофори, що забезпечують громадську безпеку; фінансові послуги, які надають засоби для існування та підтримують обмін найважливішими товарами та послугами; медичні установи, які забезпечують життя та здоров'я населення; системи, які ізолюють небезпечні ядерні та хімічні об'єкти; а також транспорт, комунальні послуги та зв'язок, які з'єднують українську громаду в середині країни та із зовнішнім світом» [5]. Підтримуючи позицію групи Берклі, Боббі Чесні, директор Центру міжнародної безпеки та права ім. Штрауса при Школі права Техаського університету додатково аргументує, що здійснені рф кібератаки мають такий самий ефект як і «припустимо, підрив ними бомб на електропідстанціях», що однозначно становитиме воєнний злочин [11].

У своїй статті Прокурор МКС перефразовує відому цитату Альберта Ейнштейна із пересторогою, що «технології можуть стати більш важливими ніж наша людяність» та наголошує, що «безперечно, нас чекає перевірка» [15]. Але сам факт визнання ним, що дія МГП поширюється на кіберпростір, а кібератаки можуть становити воєнні злочини є історичним моментом, що визначатиме ландшафт кібервійни у нову цифрову епоху.

Висновки. Існують правові підстави для притягнення офіцерів спецслужб та політичного керівництва рф до кримінальної відповідальності за кібератаки на критичну інфраструктуру України як воєнні злочини. Наразі виникають реальні перспективи розгляду такої справи у МКС. Обгрунтування:

1. Ситуація в Україні юридично визнана Прокурором МКС міжнародним збройним конфліктом, який триває з 2014 року. До неї застосовується МГП, порушення норм якого може становити воєнні злочини.

2. Прокурор МКС у 2022 році розпочав розслідування таких потенційних злочинів. Україна, яка не є членом МКС, визнала ad hoc юрисдикцію МКС, що доповнює національну, поширюється на осіб будь-якого громадянство незалежно від наявності імунітету.

3. Окрім нападів кінетичною зброєю на цивільні об'єкти, зокрема, критичної інфраструктури (що заборонено МГП та євоєнним злочином), росію звинувачують у беспрецедентному в світовій історії застосуванню кібератак, які проводяться кадровими співробітниками її спецслужб через підконтрольні хакерські угруповання. Шістьом таким ідентифікованим хакерам висунуто кримінальні обвинувачення в США.

4. МГП безпосередньо не містить положень щодо кібернетичного простору і до кібератак раніше не застосовувалося. Але наразі формується консенсус щодо необхідності перегляду такої практики з огляду на зростаючу загрозу кібератак як елементу збройного конфлікту. Відповідне рішення розслідувати кібератаки як потенційні воєнні злочини у серпні 2023 року оприлюднив Прокурор МКС, наголосивши на історичній ролі МКС у контексті стримування розвитку гібридних стратегій та мілітаризації кіберпростору.

5. Розслідування кібератак, зокрема російських, на критичну інфраструктуру України за відсутності чіткої міжнародно-правової регламентації використання кіберпростору в контексті збройних конфліктів буде пов'язано із необхідністю вирішення низки юридичних проблем. Однією із ключових є встановлення відповідності кібератак так-званому «порогу серйозності» (gravity threshold) «атаки» за МГП.

6. Ця проблема може бути вирішена шляхом відмови від раніше запропонованої експертами концепції «фізичних наслідків» (а саме смерті, поранень чи руйнувань) як критерію відповідності кібератаки атаці згідно МГП на користь концепції «втрати функціональності», за якої таким критерієм визнається не фізичне знищення цілі, а її нейтралізація, в результаті якої інформаціна система об'єкта перестає забезпечувати надання послуг, критичних для нормальної життєдіяльності населення.

ЛІТЕРАТУРА

1. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал.* 2012. № 12. С. 409–414.

2. Музика В. В. Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення : дис. … д-ра філософії : 081 / Нац. ун-т. «Одеська юридична академія». Одеса, 2021. 219 с.

3. Фещуков Г. В. Застосування МГП по відношенню до кібероперацій, що проводяться під час збройних конфліктів. *Юридичний науковий електронний журнал*. 2023. № 9. С. 437–439.
4. Geers K. Strategic cyber security : Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2011. 169 p.
5. The Gravity of Russia's Cyberwar against Ukraine. *OpinioJuris* : веб-сайт. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russias-cyberwar-against-ukraine/ (дата звернення: 01.08.2023).
6. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine). *Blog of the European Journal of International Law* : веб-сайт. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-the-international-criminal-court-and-its-implications-for-ukraine-some-preliminaryreflections/ (дата звернення: 01.08.2023).
7. Information for victims. *International Criminal Court* : веб-сайт. URL: https://www.icc-cpi.int/victims/ukraine (дата звернення: 01.11.2023).
8. Римський статут Міжнародного кримінального суду. *Міністерство юстиції України* : веб-сайт. URL: https://minjust.gov.ua/m/mijnarodniy-kriminalniy-sud (дата звернення: 01.11.2023).
9. Що стосується захисту жертв збройних конфліктів неміжнародного характеру : Додатковий протокол до Женевських конвенцій від 9 чер. 1977 р. URL: https://zakon.rada.gov.ua/laws/show/995_200#Text (дата звернення: 01.11.2023).
10. Що стосується захисту жертв міжнародних збройних конфліктів : Додатковий протокол до Женевських конвенцій від 8 чер. 1977 р. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text (дата звернення: 01.11.2023).
11. NATO Cyber defence. *North Atlantic Treaty Organization* : веб-сайт. URL: https://www.nato.int/cps/en/natohq/topics_78170.html (дата звернення: 01.11.2023).
12. Tallinn Manual on the International Law Applicable to Cyber Warfare. *Nowandfutures* : веб-сайт. URL: https://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf (дата звернення: 01.11.2023).
13. Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare. *Cambridge University* : веб-сайт. URL: https://assets.cambridge.org/ 97811071/77222/frontmatter/9781107177222_frontmatter.pdf (дата звернення: 01.11.2023).
14. US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit. *Wired* : веб-сайт. URL: https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/ (дата звернення: 01.11.2023).
15. 15. The Case for War Crimes Charges Against Russia's Sandworm Hackers. *Wired* : веб-сайт. URL: https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/ (дата звернення: 01.11.2023).
16. Ukraine enters uncharted territory with request to investigate Russian cyberattacks as war crimes. *The Hill* : веб-сайт. URL: https://thehill.com/policy/cybersecurity/3833793-ukraine-enters-uncharted-territory-with-request-to-investigate-russian-cyberattacks-as-war-crimes/ (дата звернення: 01.11.2023).
17. Міжнародний трибунал може розглядати кібератаки РФ на Україну як військовий злочин. *Служба безпеки України* : веб-сайт. URL: https://ssu.gov.ua/novyny/mizhnarodnyi-trybunal-maie-rozghliadaty-kiberataky-rf-na-ukrainu-yak-voiennyi-zlochyn-illia-vitiuk (дата звернення: 01.11.2023).
18. Technology Will Not Exceed Our Humanity. *Digitalfrontlines* : веб-сайт. URL: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/: (дата звернення: 01.11.2023).
19. BBC News. Rules of engagement issued to hacktivists after chaos. *BBC* : веб-сайт. URL: https://www.bbc.com/news/technology-66998064: (дата звернення: 01.11.2023).
20. Ukraine symposium – accountability for cyber war crimes. *The Lieber Institute for Law & Warfare at West Point* : веб-сайт. URL: https://lieber.westpoint.edu/about/lieber/ (дата звернення: 01.11.2023).
21. The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare Prepared by the Permanent Mission of Liechtenstein to the United Nations. *The Global Institute for the Prevention of Agression* : веб-сайт. URL: https://crimeofaggression.info/the-campaign/the-council-of-advisers-on-the-application-of-the-rome-statute-to-cyberwarfare/ (дата звернення: 01.11.2023).