РОЗДІЛ 11
МІЖНАРОДНЕ ПРАВО

УДК 341:004

ПРИНЦИПИ ОБМЕЖЕННЯ ВЕДЕННЯ КІБЕРВІЙНИ В МІЖНАРОДНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

PRINCIPLES OF LIMITATION OF CYBERWAR IN INTERNATIONAL INFORMATIONAL SPACE

Камчатний М.В.,
аспірант кафедри міжнародного права
Національного юридичного університету імені Ярослава Мудрого

Статтю присвячено дослідженню принципів обмеження ведення кібервійн суб'єктами міжнародного права з використанням інформаційно-комп'ютерних технологій. У статті досліджено наявні принципи обмеження ведення війни, можливість та доцільність їх застосування до кібервійн. Розглянуто основні підходи до формування нових обмежувальних принципів у сучасному кіберпросторі. Автор вперше в українській доктрині аналізує питання обмеження суб'єктів міжнародного права у методах та засобах ведення кібервійни, порівнює наявні принципи обмеження ведення війни, трансформує їх задля застосування щодо актів у кіберпросторі.
Ключові слова: кібервійна, інформаційна війна, принципи міжнародного права, міжнародне гуманітарне право, право збройних конфліктів, кіберпростір, кібератака, міжнародна інформаційна безпека.

Статья посвящена исследованию принципов ограничения ведения кибервойн субъектами международного права с использованием информационно-компьютерных технологий. В статье исследованы существующие принципы ограничения ведения войны, возможность и целесообразность их применения к кибервойне. Рассмотрены основные подходы к формированию новых ограничительных принципов в современном киберпространстве. Автор впервые в украинской доктрине анализирует вопрос ограничения субъектов международного права в методах и средствах ведения кибервойны, сравнивает существующие принципы ограничения ведения войны, трансформирует их для применения в отношении актов в киберпространстве.
Ключевые слова: кибервойна, информационная война, принципы международного права, международное гуманитарное право, право вооруженных конфликтов, киберпространство, кибератака, международная информационная безопасность.

The article is devoted to the study of the principles of restricting the conduct of cyberwars by subjects of international law with the use of information and computer technologies. The article examines the existing principles of restricting war, the possibility and feasibility of their application to cyberwars. The main approaches to the formation of new restrictive principles in modern cyberspace are considered. For the first time in Ukrainian doctrine the author analyzes the issue of limiting the subjects of international law in the methods and means of conducting cyberwar, compares the existing principles of the restriction of war, transforms them for the application for acts in cyberspace.
Key words: cyberwar, information war, principles of international law, international humanitarian law, law of armed conflicts, cyberspace, cyberattack, international information security.

Постановка проблеми. Проблематика ведення кібервійн, яка значно загострилася у світлі вчинених останнім часом численних кібератак та кібероперацій, свідчить про гостру необхідність пошуку міжнародно-правової основи щодо взаємодії між суб'єктами міжнародного права у кіберпросторі. Оскільки поява нового простору, що постійно збільшується, дала можливість проводити державам та іншим суб'єктам свою власну політику у ньому, то, відповідно, з'являється і необхідність регулювання, контролю та обмежень меж такого впливу, вироблення принципів, які б обмежували держави у розв'язанні кібервійн.

Для держав, міжнародних організацій та вчених міжнародників вже абсолютно очевидною є можливість ведення кібервійни у міжнародному інформаційному просторі. Оскільки для міжнародного права цей вид простору є новим, наявні міжнародно-правові норми щодо ведення війни у такому просторі повною мірою не враховують специфіку відносин, що складаються. Так само, незважаючи на досить великий спектр вчинених кібератак проти держав, нині звичаєві норми міжнародного права, які б дали змогу краще зрозуміти правову природу явища «кібервійна», перебувають лише на стадії свого формування.

Проте, спираючись на відсутність універсальних або регіональних норм міжнародного права щодо ведення кібервійни, чи можна вважати, що вони є абсолютно неврегульованими міжнародним правом? На нашу думку, відповідь тут має бути виключно позитивна.

Якщо ми зазначаємо, що кібервійна можлива, що вона має відповідати нормам міжнародного права, то, відповідно, мають бути і певні міжнародно-правові обмеження щодо ведення таких кібервійн. Нині міжнародне право у частині регулювання проведення кібероперацій, вчинення кібератак та ведення кібервійн перебуває у стадії постійної розробки.

Стан опрацювання. У своїх працях зазначеної проблематики фрагментарно торкалися такі українські вчені: Д. Дубов, А. Войцехівський, О. Мережко, Ю. Разметаєва. Серед закордонних вчених свої роботи присвячували: Дж. Карр (J. Carr), М. Лібіцкі (M. Libicki), Х. Лін (H.Lin), М. Магомедов, Т. Рід (T. Rid), Е. Філіол (E. Filiol), В. Хайнтшель вон Хайнег (W. Heintschel von Heinegg), Г. Шинкарецька, М. Шмідт (M. Schmitt) та ін. Більшість авторів підкреслює необхідність створення актів, які б сприяли розумінню правил впровадження власної зовнішньої політики суб'єктами міжнародного права у кіберпросторі.

Виклад основного матеріалу. Першим важливим елементом для з'ясування або визначення обмежень щодо ведення кібервійн є поняття «кіберпростір». Як і багато інших понять, «кіберпростір» не має єдиного відображення у доктрині міжнародного права. Проте вчені-міжнародники виокремили головні ознаки, що характеризують цей новий вид простору. Найбільш влучно поняття «кіберпростір» наведено М. Шміттом: «Кіберпростір – це середовище, що формується за допомогою фізичних і нефізичних компонентів, які характеризуються використанням обчислювальної техніки й електромагнітного спектру, з метою зберігати, змінювати і обмінюватися даними з використанням комп'ютерних мереж» [1]. Ми бачимо, що кіберпростір – це певне середовище, що складається з сукупності комп'ютерних мереж. Відповідно, з метою забезпечення міжнародної безпеки і запобігання розв'язанню кібервійн необхідно зрозуміти, до яких саме норм міжнародного права мають звертатися учасники міжнародних правових відносин у кіберпросторі.

Увага порушеному питанню приділяється у рамках ООН, починаючи з 1998 р. Кожного року Генеральна Асамблея готує резолюції «Досягнення в сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» [2]. Ці документи сприяють підвищенню уваги держав необхідності врегулювання відносин між ними у кіберпросторі, яка посилюється.

Найпершим серед всіх можливих принципів обмеження ведення кібервійни, має бути принцип, що закріплений у Договорі про відмову від війни як засобу національної політики 1928 р. Держави у своїй геополітичній діяльності мають відмовитися від використання кібертехнологій як політичного тиску або навіть нападу на своїх опонентів [3]. Так само, як у XX ст. країни зобов'язувалися відмовитися від використання традиційних озброєнь, цей принцип має використовуватися за аналогією.

Незважаючи на те, що у ст. 2(4) Статуту ООН зазначено, що всі члени Організації Об'єднаних Націй «утримуються в їхніх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і будь-яким іншим чином, несумісним з цілями «Об'єднаних Націй», можливість ведення кібервійни нині є абсолютно реальною [4]. Тож ми будемо зважати на те, що кібервійна можлива, тому потребує встановлення принципів обмежень її розгортання. Але чи можна вважати кібератаки застосуванням сили? Вважається, що розвиток технологій досяг такого рівня, коли кібернетичні операції мають потенціал для завдавання великих соціально-економічних збоїв, не завдаючи при цьому фізичної шкоди, як правило, пов'язаної зі збройними конфліктами [5]. Кібероперації за своєю природою не є кінетичними і не використовують те, що в загальному розумінні можна розглядати як «зброю». Тому може скластися враження, що конфлікт, який складається лише з кібероперацій, не буде вважатися збройним. Проте кібератаки та кібероперації можуть мати вагомі руйнівні наслідки для об'єктів критичної інфраструктури, а також спричиняти жертви (включно і серед мирного населення). Саме через це, на нашу думку, до проявів актів кібервійни варто застосовувати норми міжнародного права.

Міжнародне право збройних конфліктів утворюють два основних складових елементи: jus ad bellum та jus in bello. Перше, яке також має назву право війни, регулює ситуації, коли держави можуть застосовувати силу як інструмент власної національної політики. Що стосується jus in bello, або міжнародне гуманітарне право, то воно покликане на регулювання питань того, як може бути застосована військова або інша сила, а також проти кого вона може бути використана. Право війни прагне підтримувати мирні відносини у міжнародному співтоваристві шляхом встановлення певних суворих критеріїв щодо того, коли держави можуть вийти за межі мирних заходів, таких як дипломатія, економічні санкції. Варто відзначити право зробити це в порядку самооборони, коли суб'єкт зіткнувся зі «збройним нападом», або його право прийти на допомогу іншій державі, яка захищається (колективна самооборона) [6].

Оскільки ми визначили, що кібератака може розглядатися через призму права війни і, відповідно, прирівнюватися до збройного нападу, доречно звернутися до ст. 51 Статуту ООН, в якій зазначається: «Статут у жодному разі не стосується невід'ємного права на індивідуальну або колективну самооборону, якщо станеться збройний напад на Члена Організації, доти, поки Рада Безпеки не вживе заходів, необхідних для підтримки міжнародного миру і безпеки». Водночас у міжнародному гуманітарному праві термін «атака» використовується як категорія військових операцій. Ст. 49 (1) 1977 року Додаткового протоколу I до Женевських конвенцій 1949 р. визначає «атаки» як «акти насильства щодо супротивника, або під час нападу або в обороні» [7].

Попри відсутність у міжнародному праві прямого нормативного регулювання питань, пов'язаних із веденням кібервійн, норми чинного міжнародного права можуть бути застосовані під час вчинення кібератак. Хоча варто зазначити, що вони мають відповідати певним критеріям, щоб потрапляти безпосередньо під регулювання норм саме міжнародного права.

М. Шмідт зазначає, що всі збройні атаки є застосуванням сили, проте не всі застосування сили є

збройним нападом [6, с. 286]. Тут варто звернути увагу на те, що суб'єкти міжнародного права можуть зіштовхнутися з ситуацією, коли вчинена проти них кібератака буде за своїми масштабами та наслідками недостатньою для того, аби вважатися збройним нападом, а тому держава-жертва такої атаки буде неспроможна застосувати своє право на контрзаходи, гарантоване Статутом ООН. Тому у держави залишається право відповісти на таку атаку дипломатичними протестами, економічними санкціями або вчинити таке кібервтручання, яке буде вважатися законними контрзаходами. Держава також може звернутися та передати справу на розгляд Ради Безпеки ООН, яка має унеможливлювати загрозу миру та запобігати актам агресії [4].

Погляд на акти кібервійни через призму права війни та міжнародного гуманітарного права приводить до схожих висновків. Найголовнішим тут є те, що питання кібервійни можуть бути регульованими нормами міжнародного права, попри відсутність прямих посилань у нормах. Через високу небезпеку актів кібервійни вони регулюються гуманітарним правом, бо у результаті кібервійни можуть загинути люди (включно із цивільним населенням), кібератаки можуть спричинити повне чи часткове знищення об'єктів, які в подальшому вплинуть як на стан здоров'я, так і на життя населення, що від таких об'єктів залежать. Міжнародне гуманітарне право покликане, в першу чергу, захищати життя та здоров'я цивільного населення [8]. Під час збройних конфліктів завжди виникає небезпека атак на об'єкти критичної інфраструктури, коли супротивник має на меті вивести останні з ладу або повністю знищити їх, щоб отримати певну стратегічну перевагу. Руйнування таких об'єктів часто ставить під загрозу безпеку цивільного населення.

Зважаючи на вищезазначене, важливим є визначення об'єктів критичної інфраструктури. Залежно від держави, розуміння та нормативне закріплення терміна «критична інфраструктура» може відрізнятися. Наприклад, «Акт Патріота» (Patriot Act) США подає таке визначення: «Критичні інфраструктури – це системи і ресурси, фізичні або віртуальні, настільки значимі для США, що їх руйнування або порушення нормальної роботи здатне підірвати військово-політичну безпеку держави, економічну стабільність, здоров'я громадян і суспільний порядок, або спричинити кілька вищевказаних факторів у будь-якій комбінації» [9]. В Україні Постановою Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» надається таке визначення терміна: «Критична інфраструктура – сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку й оборону, природне середовище, призвести до значних фінансових збитків та людських жертв» [10]. Порівнюючи два наведених підходи до розуміння критичної інфраструктури, ми бачимо, що у США до таких об'єктів відносять і віртуальні системи чи ресурси. Такі об'єкти утворюють так звану критичну інформаційну інфраструктуру, що є певною новелою, оскільки у міжнародному гуманітарному праві (а саме у Женевських конвенціях про захист жертв війни) не застосовується поняття «критична інфраструктура», проте ним захищається цивільний персонал, що там працює, а також накладається заборона здійснювати атаки на такі об'єкти, якщо вони не є військовими (не використовуються з військовою метою), або перебувають не в межах території, де точаться бойові дії, або не охороняються військовими. Значної уваги в праві збройних конфліктів надається захисту цивільних об'єктів: «Цивільні об'єкти не мають бути об'єктом нападу або репресалій» [8].

Гаазька конвенція про закони і звичаї суходільної війни 1907 р. встановила заборону на бомбардування та будь-які атаки незахищених міст, селищ, житла і будівель. У додатку до Конвенції «Положення про закони та звичаї сухопутної війни» також підтверджується заборона на напади або репресалії щодо цивільних об'єктів. Ст.ст. 27, 28 Положення забороняється здійснення будь-яких ворожих актів, спрямованих проти історичних пам'яток, творів мистецтва або місць відправлення культу, які становлять культурну або духовну спадщину народів [11]. Забороняється використовувати голод серед цивільного населення як метод ведення війни. Неприпустимо піддавати нападу або знищувати, вивозити або приводити у непридатний стан об'єкти, необхідні для виживання цивільного населення (запаси продовольства, запаси питної води та споруди для її постачання, посіви, іригаційні споруди тощо). Оскільки нині можливості впливу на перелічені об'єкти розширилися завдяки інформаційно-комп'ютерним технологіям, можна говорити про застосовність норм МГП навіть до сучасних видів втручань – кібератак.

Також не варто забувати про безліч наявних об'єктів як військового, так і невійськового призначення, які можуть бути уражені за допомогою інформаційно-комп'ютерних технологій. Серед них такі, що можуть фактично бути поза межами театру воєнних дій або навіть далеко поза межами територій, де розгортається кібервійна. До таких об'єктів можна віднести морські та авіаційні судна. Системи навігації, що застосовуються на цивільних суднах, зазвичай не мають спеціальних засобів захисту від високоорганізованого зовнішнього втручання. Це може призвести до ситуацій, коли керування або навігація судном опиниться під зовнішнім контролем із боку суб'єкта, що веде кібервійну. Як результат, навіть без застосування зброї можуть постраждати цивільні особи, завдана матеріальна шкода державі. Такі об'єкти, безумовно, мають залишатися поза межами ведення кібервійни та оберігатися міжнародним правом.

Складніше визначатися безпосередньо з об'єктами інформаційної інфраструктури, тобто такими, які не мають фізичного відображення.

Цивільні інформаційні ресурси і системи не мають відмітних знаків (як такі, наприклад, що застосовуються МКЧХ або ООН), що потенційно підвищує їх вразливість і знижує ступінь захисту. Водночас така відмінність не має робити подібні цифрові об'єкти метою незаконного втручання в їх діяльність.

Крім того, звертаючись до Додаткового протоколу І до Женевських конвенцій від 12 серпня 1949 р., а саме до ст. 36, ми бачимо, що навіть попри відсутність прямого закріплення кіберзброї як інструменту вчинення атак у міжнародному інформаційному просторі, на такі атаки може і має поширюватися дія міжнародного гуманітарного права. Названою статтею передбачено, що створення та розроблення новітніх видів озброєння, засобів або методів ведення війни держава має визначати, чи потрапляє їх застосування під заборони, зазначені у Протоколі [7].

Варто зазначити, що, як і у класичному розумінні ведення війни згідно з нормами міжнародного гуманітарного права, кібервійна теж може мати подібні до неї ознаки. До них, в першу чергу, належить поняття «театр війни» та «театр воєнних дій». Нормами МГП визначається, що театром війни є певна ділянка суші чи морського простору, де можуть вестися бойові дії, в той час як театром ведення воєнних дій є певна територія, де такі дії проводяться фактично, проводяться військові операції [12]. Такі поняття є доречним застосовувати і під час кібервійни. Міжнародне гуманітарне право діє безпосередньо у визначених ситуаціях та на певній території конфлікту, ним встановлюються спеціальні зони, де ведення бойових дій обмежується чи забороняється, створюються нейтральні території. Нормативне закріплення таких обмежень щодо території розгортання кібервійн дасть змогу зменшити негативний широкий вплив на критичну інфраструктуру та цивільне населення під час такого стану. Оскільки реальних меж в інформаційному просторі не існує, це положення має трактуватись як таке, що застосовується до об'єктів, які під'єднані до кіберпростору та перебувають у межах таких обмежень застосування військової сили. Надзвичайно важливим тут є невтручання у системи життєзабезпечення цивільного населення, залишення у безпеці медичних установ та інших важливих об'єктів, які керовані за допомогою комп'ютерних технологій.

Кібервійна як акт впливу на внутрішню політику держав, безумовно, має бути обмежена нормами міжнародного права. Оскільки кібервійна потенційно може мати дуже серйозні наслідки для об'єктів військових, а також об'єктів цивільної інфраструктури, то держави, задля запобігання розгортання кібервійн, які водночас можуть супроводжуватися війнами класичними, мають утриматися від погрози силою або її застосування в межах кіберпростору. Як вже зазначалося вище, незважаючи на відсутність закріплення у міжнародно-правових актах прямої заборони на використання кіберзброї, такі види озброєння вже існують, постійно розробляються й удосконалюються. Відсутність нормативного регулювання – лише питання часу та досягнення консенсусу на міжнародній арені. Своє визнання небезпеки ведення кібервійни держави de facto визнають, приймаючи національне законодавство у сфері кібербезпеки. Свою готовність до ведення наступальних або оборонних операцій у кіберпросторі суб'єкти міжнародного права визнають, створюючи спеціальні державні формування, що відповідають за проведення кібероперацій (їх організацію або відвернення, або подолання наслідків). Серед таких держав США, КНР, Росія, Індія, Велика Британія, Німеччина та багато інших. Важливо зазначити, що у більшості країн, де такі формування ініціюються, вони створюються на базі Міністерств оборони держав, що, безумовно, свідчить про майбутній характер та розвиток цього напряму державної діяльності [13].

Що стосується загальних принципів, вони, швидше за все, стають актуальними, коли виникають суперечки між державами з певних питань у кіберпросторі. Наприклад, у відомому випадку на заводі Хожув Постійна палата міжнародного правосуддя ухвалила, що порушення зобов'язання в міжнародному праві обов'язково призводить до виникнення зобов'язання зробити репарації, принцип було повторено Комісією з міжнародного права у тексті проекту Статей про відповідальність держав за міжнародно-протиправне діяння [14]. Таким чином, якщо операції держави у кіберсфері порушують суверенітет іншої держави і завдають останній шкоди, держава, що їх вчинила, буде зобов'язана зробити репарації на користь останньої. Як зазначає М. Камишанський, так званий «хожувський принцип» продовжує виконувати свою функцію із врегулювання наслідків міжнародно-протиправних діянь [15]. Аналогічним чином, суди можуть розглядати справи частково на основі справедливих міркувань. Таке рішення може бути доцільним, наприклад, у разі, коли предметом розгляду є кіберінфраструктура, яку поділяють між собою держави [16]. Чітко закріплена відповідальність за вчинення актів кібератак або ведення кібервійни також має слугувати як певний обмежувальний елемент для суб'єктів міжнародного права, щоб зазначені діяння не вчиняти.

Окремим надзвичайно важливим принципом, що має обмежити кібератаки як складові елементи ведення кібервійни, має стати принцип невтручання у справи, які входять до внутрішньої компетенції держав. Цей важливий принцип має знайти своє віддзеркалення щодо кіберпростору, оскільки нині цей простір не є повною мірою контрольованим нормами міжнародного права (а правильніше буде зазначити, майже не контрольований), а отже, залишає для більш розвинених у кібернетичному сенсі держав великий простір для втручання. Масштаби втручання у внутрішні справи держав залежать лише від бажання сторони, що вчиняє кібератаки, а інтенсивність – виключно від рівня розвитку кібертехнологій сторін. Важливо зазначити, що певні види кібератак є відкладеними у часі, тобто навіть після виявлення державою-жертвою незаконного втручання у питання внутрішньої компетенції іншої держави та ліквідацію усіх знайдених загроз, певна

частина з них може бути трансформована та залишатися в інформаційно-комп'ютерних мережах держави-жертви. Акти кібервійни не завжди мають на меті виведення з ладу певних об'єктів критичної інфраструктури, а тому можуть навмисно ретельно приховуватися. Нині, попри порівняно високій рівень розвитку кібертехнологій, кібероперації мають надзвичайно високий рівень латентності, а проблема атрибуції певному суб'єкту міжнародного права вчинення кібератаки залишається однією з найбільш актуальних.

Відповідно до Декларації про принципи міжнародного права, всі народи мають право вільно визначати без втручання ззовні свій політичний статус і здійснювати свій економічний, соціальний і культурний розвиток, і кожна держава зобов'язана поважати це право відповідно до положень Статуту ООН [17]. Події під час президентських виборів у США, коли на сервери офісу демократичної партії були вчинені деякі кібератаки, продемонстрували гостру необхідність визнання цього принципу у кіберсфері. Центральне розвідувальне управління, Федеральна служба безпеки та Агентство з національної безпеки США підготували звіт, в якому наведені звинувачення у втручанні у внутрішні справи держави, продемонстровані напрями інформаційного впливу на президентські вибори у державі, наведені зразки пропаганди з метою маніпулювання суспільною свідомістю громадян США [18]. Після оприлюднення наведеного звіту між РФ та США були задіяні взаємні заходи дипломатичного впливу, а також запроваджено ряд санкцій. Оприлюднена версія звіту не включала повний перелік висновків державних агенцій США, а також у ньому не було наведено достатніх доказів прямого втручання держави у внутрішні справи. Проте результати взаємного обміну протестами та санкціями між названими суб'єктами свідчать про існування, а відповідно, і визнання певних відносин між ними у кіберпросторі. У зв'язку з недостатністю оприлюднених фактів цей стан не можна назвати кібервійною, проте майбутні відносини між РФ та США продемонструють напрям розвитку цих відносин і, можливо, створять перший прецедент врегулювання протистояння у кіберпросторі міжнародно-нормативним шляхом.

До принципів обмеження також варто віднести наявний у міжнародному праві принцип пропорційності, що стосуватиметься масштабу вчинення кібератак. Він дасть змогу унеможливити повномасштабні розгортання кібероперацій зі зростаючою потужністю. Завдяки такому обмеженню можна уникнути ситуації, коли взаємний обмін кібератаками переросте у кібервійну або збройний конфлікт у класичному його розумінні (оскільки, зважаючи на певні ознаки, яким відповідають кібератаки, їх результат можна характеризувати як результат застосування зброї).

З огляду міжнародного гуманітарного права, до обмежень ведення кібервійн теж варто застосувати деякі принципи, наведені Правом Женеви. Наприклад, принцип розрізнення, який є закріпленим в ст. 48 Додаткового протоколу 1977 р. до чотирьох Женевських конвенцій 1949 р.: «Сторони конфлікту мають в усі часи розрізняти цивільне населення і комбатантів, цивільні й військові цілі і, відповідно, скеровувати свої дії тільки проти військових цілей. Цей принцип чітко демонструє, що норми міжнародного гуманітарного права застосовні під час ведення кібервійни. Досить легко уявити ситуацію, коли держава, що розпочинає кібервійну, порушує діяльність гідроелектростанцій, систем фільтрації та подачі води цивільному населенню, атомних електростанцій та безліч інших критично важливих об'єктів. Виведення їх з ладу ставить під загрозу життя буквально цілих міст, а з метою заподіяння істотної шкоди таким об'єктам достатньо вчинення спрямованої кібератаки на них (за умови їх безпосереднього підключення до мережі Інтернет, хоча можливі втручання навіть в об'єкти зі своєю власною відокремленою системою, як це було здійснено під час запуску STUXNET у Ірані)» [19]. Таким чином, із цього принципу логічно випливає принцип заборони атак на цивільне населення. У сучасному світі в деяких медичних установах із метою оптимізації та більш детального слідкування за станом здоров'я деяких пацієнтів створюються системи віддаленого контролю за показниками та підтримання їх життя. Очевидним є те, що всі такі дані збираються та обробляються на відокремлених серверах, доступ до яких лікарі мають за допомогою мережі Інтернет. Окрім полегшення та сприяння роботи медичного персоналу, такі технології роблять ці об'єкти вразливими перед впливом кібератак. Це також стосується військових госпіталів, де можуть бути запроваджені такі технології для контролю за станом здоров'я поранених чи хворих військовослужбовців. Тому за будь-яких умов розвитку конфлікту такі об'єкти мають залишатися поза межами розгортання кібервійни.

Відповідно до принципу територіального суверенітету, держава здійснює повну і виключну владу над своєю територією. Це так само має стосуватися і кіберпростору. Проте варто зазначити, що у кіберпросторі не існує жодних відомих кордонів. Тому виникає логічне питання: а як визначити межі суверенітету держав у кіберпросторі і чи існує він взагалі? Особливо важливе розуміння і чітке визначення цього принципу саме у контексті ведення кібервійни. Як вже зазначалося вище, нині однією з найбільш складних проблем у міжнародному праві є атрибуція діянь, вчинених у кіберпросторі суб'єктам міжнародного права. Якщо з технічними аспектами проходження сигналу через супутники у космосі, по кабелях під землею, по дну морських просторів або іншими засобами важко визначитися, використовуючи принцип територіального суверенітету, то завдяки вихідній точці такого сигналу питання атрибуції значно полегшується. Абсолютно логічним є те, що всі комп'ютерні мережі є штучно створеними людиною, а отже, кожен з їх компонентів (сервери, приймаючі установки, персональні комп'ютери та інші прилади) фізично перебуває в межах пев-

ної території. Беззаперечним є той факт, що всі ці прилади є чиїмось майном, яке належить на праві власності державі, юридичним або фізичним особам. Крім того, задля того, щоб всі ці інформаційно-комп'ютерні мережі функціонувало потрібне електричне живлення, яке теж здійснюється з певного джерела, яке об'єктивно знаходиться в межах території держави. Тому, хоча внутрішніх кордонів у кіберпросторі і не існує, проте забезпечення територіального суверенітету у ньому цілком можливе завдяки визначенню місця знаходження компонентів, що забезпечують під'єднання певних об'єктів до міжнародного інформаційного простору. Відповідно, інтеграція фізичних компонентів кіберінфраструктури, розташованої в межах території держави, в «глобальному» кіберпросторі не може бути витлумачена як відмова від здійснення територіального суверенітету. Хоча, з точки зору справжньої архітектури кіберпростору, здійснювати свій суверенітет може бути важко, а пов'язані технологічні і технічні проблеми не заважають державі здійснювати свою юрисдикцію щодо кіберінфраструктури, розташованої в районах своєї суверенної території [20]. Держави, по суті, постійно підкреслюють своє право здійснювати контроль над такою інфраструктурою, відстоювати свою юрисдикцію щодо кібернетичної діяльності на їх території, а також з метою захисту їх кіберінфраструктури від транскордонного втручання з боку інших держав або окремих осіб [21].

Міжнародне гуманітарне право також зобов'язує суб'єктів учасників збройного конфлікту зберігати культурні цінності. На наш погляд, цей принцип також може бути застосовним і до обмежень ведення кібервійни, оскільки технології, які застосовуються у багатьох випадках з метою зберігання деяких культурних цінностей, залежать від кіберінфраструктури.

Також більшість наявних принципів, застосовних до кібервійни, наведені у Талліннському посібнику 2013 р. Деякі з них є новелою для міжнародного права і не мають свого відображення у наявних і закріплених принципах. Цей зразок узагальненої доктрини є надзвичайно важливим задля розуміння бачення питань розвитку міжнародно-правового регулювання питань, пов'язаних із кібербезпекою. Серед наведених у посібнику уваги заслуговують наведені нижче принципи, що здатні обмежити розв'язання кібервійн.

Принцип контролю за кіберінфраструктурою. Він полягає в тому, що держава, на території якої знаходяться кіберінфраструктури, не має дозволяти використання їх зі шкідливою або незаконною метою проти іншої держави. Цей принцип тісно переплітається з принципом державного суверенітету, проте, на відміну від нього, покладає на державу пряме зобов'язання не допускати використання «свого» обладнання проти інших держав.

Ще одним зазначеним принципом є *принцип необхідності та пропорційності.* Він, в свою чергу, деякою мірою дублює за своїм змістом принцип пропорційності, проте дещо ширше розкриває значення «необхідності». Зазначається, що необхідністю є ситуація, коли треба відвернути неминучу атаку або зупинити розпочату. Цей принцип не означає, що ситуація може бути вирішена лише силою. Силові методи можуть бути використані паралельно з дипломатичними, економічними або правовими або бути замінені ними. Необхідність визначається потерпілою державою, проте визначення необхідності має бути розумним за супутніх обставин.

Сучасні технології виводять відносини між суб'єктами міжнародного права навіть за межі Землі. Космічні технології нерозривно пов'язані із застосуванням інформаційно-комп'ютерних технологій. Міжнародним правом заборонено вести будь-які бойові дії у космічному просторі [22]. Проте, оскільки досі нема нормативного закріплення щодо проведення у космосі актів кібервійни, а також через вкрай високий ступінь задіяння комп'ютерних технологій у цій сфері важливим є *принцип обмеження ведення кібервійни у космічному просторі.* Сучасні технології дають змогу перехоплювати за допомогою інформаційно-комп'ютерних систем сигнали супутників різного призначення, що створює підстави для неправомірного втручання в їх діяльність з боку недружніх суб'єктів. Таким чином, може бути створена небезпека для значної кількості об'єктів інфраструктури, а також поставлене під загрозу життя цивільного населення.

Наведені вище принципи, безумовно, мають бути застосовані у міжнародному праві як основні принципи обмеження ведення кібервійн.

Висновки. Отже, незважаючи на порівняно короткий час існування кіберпростору як нового визнаного міжнародного простору, відносини у ньому розвиваються дуже швидко. Від засобу, що давав змогу полегшити комунікацію у міжнародному середовищі, він швидко перейшов до простору, де міжнародні актори намагаються проводити власну політику. Незважаючи на відсутність чітко врегульованих міжнародних норм та правил поведінки держав та інших суб'єктів міжнародного права у кіберпросторі, більшість із них de facto визнають, що норми міжнародного права є застосовними до кібератак. Небажання суб'єктів вв'язуватися у неконтрольовану та неврегульовану кібервійну слугує додатковим стримувальним фактором на шляху вчинення кібероперацій цими суб'єктами.

Нині вже очевидною стала проблема вироблення міжнародно-правових норм, які б полегшили співпрацю суб'єктів міжнародного права у кіберсфері. Така робота ведеться паралельно як у сучасній доктрині, так і за кордоном, на національних рівнях у державах, а також у міжнародних організаціях регіонального та універсального характеру. Зрештою, міжнародним співтовариством мають бути вироблені необхідні міжнародно-правові норми, які б унеможливили або значно обмежили вірогідність використання кібервійни як засобу впливу на внутрішню політику держав. Оскільки такий принцип вже був закріплений у Договорі про відмову від війни як засобу національної політики, його можна і варто застосувати і до війни кібернетичної [3].

Принципи обмеження розв'язання і ведення кібервійн у міжнародному праві поки відтворюють чинні норми та принципи таких обмежень, що застосовувалися до війни у класичному розумінні. Проте унікальність кіберпростору все ж таки вимагає вироблення специфічного переліку правових норм та принципів, які б, зокрема, були спрямовані на обмеження можливостей держав здійснювати свою агресивну зовнішню політику із використанням кіберпростору. З'являються перші спроби закріплення таких норм нормативно, ООН приділяє значну увагу питанням кібербезпеки, спостерігається дедалі більше випадків кібервтручань, які потребують нормативного роз'яснення та правової кваліфікації, а отже, поступово вироблятимуться і звичаєві норми. Наведений у статті перелік принципів не є вичерпним, перебуває у постійній дискусії, розширенні та доповненні у колі юристів-міжнародників, а також перебуває серед основних питань порядку денного таких міжнародних організацій, як ООН, НАТО, ОБСЄ, ШОС тощо. Зрештою варто зазначити, що наукові пошуки з питань розроблення принципів обмеження ведення кібервійн у міжнародному інформаційному просторі мають бути продовжені.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare / Michael N. – Cambridge University Press.
2. Resolution Adopted by the General Assembly 53/70. Developments in the Field of Information and Telecommunications in the Context of International Security. 1999 [Електронний ресурс]. – Режим доступу : https://ccdcoe.org/sites/default/files/documents/UN-981204-ITIS.pdf
3. Договір про відмову від війни як засобу національної політики (Пакт Бріана-Келлога). Париж, 1928 р. [Електронний ресурс]. – Режим доступу : https://www.uni-marburg.de/icwc/dateien/briandkelloggpact.pdf
4. Статут ООН. Charter of the United Nations and Statute of the International Court of Justice. San Francisco – 1945 [Електронний ресурс]. – Режим доступу : https://treaties.un.org/doc/publication/ctc/uncharter.pdf
5. Classification of Cyber Conflict. Journal of Conflict & Security Law. Michael Schmitt [Електронний ресурс]. – Режим доступу : https://academic.oup.com/jcsl.
6. «Attack» as a Term of Art in International Law: The Cyber Operations Context. Michael N. Schmitt. 2012 4th International Conference on Cyber Conflict. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn.
7. Додатковий протокол I до Женевських конвенцій 1949. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_199.
8. Конвенція про захист цивільного населення під час війни. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_154.
9. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.
10. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF.
11. Положення про закони та звичаї сухопутної війни [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_222.
12. Тимченко Л.Д. Міжнародне право : підручник / Л.Д. Тимченко, В.П. Кононенко. – К. : Знання, 2012. – 631 с.
13. Who are the cyberwar superpowers? World Economic Forum. Global Agenda. [Електронний ресурс]. – Режим доступу : https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/
14. Chorzow Factory Case, 1928 PCIJ., (ser. A) No. 13, at 28.
15. Камышанский М.М. Влияние дела о фабрике в Хожуве (1928 г.) на становление принципа международно-правовой ответственности / М.М. Камышанский // Форум права. – 2015. – № 2. – С. 83–89 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/j-pdf/FP_index.htm_2015_2_15.pdf.
16. Michael N. Schmitt and Liis Vihul. The Nature of International Law Cyber Norms. Tallinn Paper No. 5 Special Expanded Issue, 2014.
17. Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций. Принята резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 года.
18. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. 6 January 2017.
19. Андрєєва О.М., Мусієнко К. Кіберзброя та аналіз її деструктивної діяльності на прикладі впливу вірусу нового покоління STUXNET на іранську ядерну програму. Перспективи відносин України зі США, РФ, ЄС і НАТО в посткризовому світі, 2011 – С. 29–34.
20. Territorial Sovereignty and Neutrality in Cyberspace. Wolff Heintschel von Heinegg. 89 INT'L L. STUD. 123 (2013). Volume 89.
21. See DoD Strategy for Operating in Cyberspace, supra note 9. See also U.S. Depart-ment of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the Na-tional Defense Authorization Act for Fiscal Year 2011, Section 934, at 7–8 (2011), available at http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20 Section%20934%20 Report_For%20webpage.pdf [hereinafter Cyberspace Policy Report]; THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECU-RITY, AND OPENNESS IN A NETWORKED WORLD 12–15 (2011), [Електронний ресурс]. – Режим доступу : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
22. Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла. [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/995_480.