УДК 341: 343.34: 316.774

ПРАВОВИЙ АНАЛІЗ ВИКОРИСТАННЯ КІБЕРПРОСТОРУ У ВОЄННИХ ЦІЛЯХ

Грицун О. О.

Здобувач кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

Науковий керівник: кандидат юридичних наук, доцент І. М. Забара.

Анотація. *У статті досліджуються міжнародні ініціативи в рамках Організації Об'єднаних Націй щодо врегулювання проблеми використання державами кіберпростору у воєнних цілях та регіональний підхід, запропонований державами-членами Шанхайської Організації Співробітництва. Крім того, у статті аналізуються концептуальні та термінологічні розбіжності у теоретичних підходах науковців різних країн щодо визначення понять «інформаційна війна», «кібервійна» та «операції у кіберпросторі», їх особливості та розбіжності у змістовних підходах до розуміння цих понять. Також, у статті надається короткий огляд міждержавних ініціатив щодо погодження термінології у сфері міжнародної інформаційної безпеки. Основна частина статті присвячена аналізу застосування норм міжнародного права до ведення державами бойових дій у кіберпросторі, зокрема питанням класифікації операцій у кіберпросторі з точки зору норм jus ad bellum, а також можливості застосування положень Статуту Організації Об'єднаних Націй до врегулювання поведінки держав у кіберпросторі.*

Ключові слова: *інформаційна війна, кібервійна, операції у кіберпросторі, інформаційно-комунікаційні технології, міжнародне право.*

Постановка проблеми. На сьогодні поняття забезпечення міжнародної інформаційної безпеки та підтримання міжнародного миру та стабільності нерозривно пов'язані. Поширення нових інформаційно-комунікаційних технологій спричинили їх масштабне застосування не лише в цивільній, а і в воєнній сферах. Держави все більше уваги приділяють питанням розробки операцій у кіберпросторі як оборонного, так і наступального характеру, що відображено у національних доктринах інформаційної безпеки держав. Варто наголосити, що концепції правового забезпечення міжнародної інформаційної безпеки знаходяться лише на стадії формування та погодження в рамках Організації Об'єднаних Націй та низки регіональних організацій, а загроза використання кіберпростору для ведення бойових дій цілком реальна та потребує негайного правового врегулювання.

Мета статті – дослідити основні наукові підходи до розуміння понять «інформаційна війна» та «кібервійна», а також проаналізувати основні підходи та труднощі у тлумаченні і застосуванні існуючих норм міжнародного права до регулювання питань ведення бойових дій у кіберпросторі.

Аналіз останніх досліджень та публікацій. Окремі теоретичні підходи до розуміння понять «інформаційна війна» та «кібервійна» висвітлені в роботах Стрельцова А. О., Комова С. А., Кершишніга Г., Шмітта М., та Річарда А. Питання застосування норм міжнародного права до ведення бойових дій у кіберпросторі досліджувались у роботах Дреге К., Олдрич Р., Браунлі Я., та Хетеуей А. Проте, на даний момент не існує єдиного підходу до розуміння цих понять та існують складнощі із інтерпретацією та тлумаченням існуючих

положень міжнародного права у контексті його застосування до проведення бойових операцій у кіберпросторі. Тому, ці питання потребують подальшого аналізу та наукової розробки.

Основні результати дослідження. Навряд чи буде перебільшенням твердження, що у 21-му сторіччі суспільство повністю залежить від інформаційно-комунікаційних технологій, що застосовуються у всіх без винятку сферах суспільного життя. Найбільше занепокоєння світового співтовариства викликає можливість застосування інформаційно-комунікаційних технологій у цілях, несумісних із підтриманням міжнародного миру та безпеки. Підтвердженням цього тезису є той факт, що Група урядових експертів з питань досягнень у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки (ГУЕ), спеціально створена в рамках Організації Об'єднаних Націй (ООН), включила до розділу своєї доповіді, що стосується загроз, ризиків та вразливих місць міжнародної інформаційної безпеки, положення про те, що існуючі та потенційні загрози в сфері інформаційної безпеки, беззаперечно, є найбільш серйозною проблемою 21-го сторіччя. В доповіді наголошується на тому, що держави розробляють інформаційно-комунікаційні технології в якості інструментів ведення війни та розвідки, а також для застосування їх в політичних цілях [1, с. 6].

Ще одним підтвердженням зростаючої мілітаризації кіберпростору є дослідження, проведене Джеймсом А. Льюїсом та Катріною Тімлін в рамках Інституту ООН з питань роззброєння (ЮНІДІР) щодо оцінки національних доктрин держав у сфері кібербезпеки та кібервійни. У дослідженні держави розподілено на дві категорії: держави, що відносять питання інформаційної безпеки до військової доктрини та держави, що стоять на позиції розгляду питань інформаційної безпеки з точки зору цивільного підходу. Варто звернути увагу на те, що вищезазначене дослідження проводилось двічі – у 2011 та 2012 роках. Відповідно до дослідження 2011 року, 68 із 193 держав-членів ООН мають національні доктрини інформаційної безпеки. Серед них 32 держави включили поняття кібервійни до своїх національних стратегій, а питання інформаційної безпеки віднесено до компетенції воєнних відомств, в той час як у 36 державах питаннями інформаційної безпеки віднесено до відання цивільних відомств та організацій [2, с. 3]. Проте, дослідження, проведене у 2012 році засвідчило надзвичайно швидке зростання національних доктрин інформаційної безпеки серед держав-членів ООН. Так, станом на 2012 рік їх кількість зросла до 114, з яких 47 доктрин відносять питання інформаційної безпеки до військового аспекту, а 67 мають виключно цивільні програми. На особливу увагу заслуговує той факт, що відповідно до проведеного дослідження кількість держав, що створили чи планують створити спеціальні військові формування з питань кібербезпеки зросла за рік із 12 до 27 держав [3, с. 1-2]. Автор наголошує, що не виключено, що й інші держави створюють такі підрозділи чи нарощують наступальні можливості у кіберпросторі, не надаючи такої інформації у загальний доступ. Саме тому, зростаюча роль військового аспекту міжнародної інформаційної безпеки є предметом обговорення міждержавних переговорів як на регіональному, так і на глобальному рівнях.

Інформаційно-комунікаційні технології створили можливість для проведення широкого кола різних комп'ютерних та електронних атак, які відрізняються не лише засобами, методами та наслідками від традиційних атак, а й, в першу чергу, середовищем їх застосування – кіберпростором. Крім того, велике занепокоєння світового співтовариства викликає той факт, що міждержавний конфлікт у кіберпросторі може спричинити виникнення звичайного збройного конфлікту між державами.

Інформаційна безпека пов'язана із загрозою використання інформаційно-комунікаційних технологій однієї держави з метою впливу чи атаки на інформаційно-комуніка-

ційні технології іншої держави, що може спричинити виникнення міждержавної напруги та ситуації, що загрожує міжнародному миру та безпеці. Особливу занепокоєність викликають наступні три загрози: вплив та пошкодження інформаційних ресурсів та телекомунікаційних систем іншої держави, використовуючи інформаційно-комунікаційні технології; навмисний вплив на життєво важливі інфраструктури іншої держави; та підрив функціонування економічних і соціальних систем держави, а також здійснення психологічної маніпуляції населення іншої держави з метою дестабілізації суспільства [4, с. 7-8].

Варто наголосити, що наразі не існує єдиного концептуального та термінологічного підходу до розуміння ведення бойових дій у кіберпросторі. Науковці різних країн використовують різні терміни: «інформаційна війна», «кібервійна», «інформаційні операції», «кібератаки», «кібернетична війна», «використання інформаційної зброї».

Міхель Н. Шмітт пропонує наступне визначення інформаційної війни: «вид інформаційних операцій, тобто заходи, спрямовані на здійснення впливу на інформацію та інформаційні системи противника з метою захисту власної інформації та інформаційних систем» [5, с. 122]. До таких операцій він відносить будь-які заходи, спрямовані на виявлення, модифікацію, знищення чи передачу даних, що зберігаються в комп'ютері, підлягають комп'ютерній обробці чи пересиланню за допомогою комп'ютера. Також, до таких операцій можна віднести психологічні операції, воєнні хитрощі, електронну війну та фізичний напад на комп'ютерні мережі [6, с. 53]. Він зауважує, що вищезазначені заходи принципово відрізняються від інших методів нанесення шкоди своїм об'єктом, яким в даному випадку виступає інформація та можуть застосовуватись як в мирний час, так і під час військових конфліктів.

У більш вузькому розумінні інформаційна війна – це «інформаційні операції, що проводяться під час виникнення кризи чи конфлікту з метою досягнення чи сприяння досягненню конкретних цілей щодо конкретного супротивника» [6, с. 22]. Тобто, основною відмінністю такого розуміння інформаційної війни є її застосування виключно під час кризи чи конфлікту. Таке розуміння інформаційної війни часто використовується науковцями при дослідженні питань застосування норм міжнародного гуманітарного права до операцій у кіберпросторі. В даному контексті деякі із них використовують термін «кібернетична війна», під якою розуміють «засоби та методи ведення війни, що є операціями в інформаційному просторі і які можна розглядати в якості збройного конфлікту чи які ведуться в контексті збройного конфлікту відповідно до змісту норм міжнародного гуманітарного права» [7, с. 7].

В широкому сенсі під терміном «кібервійна» часто розуміють «будь-яке вторгнення з використанням кіберпростору, незалежно від сфери такого вторгнення чи виконавця» [8, с. 100]. Георг Кершішніг розглядає термін «кібервійна» як «геополітичний воєнний конфлікт між державами, що відбувається у кіберпросторі, включаючи конфлікти до яких залучені недержавні суб'єкти, відповідальність за дії яких лежить на державах» [9, с. 84]. На його думку кібервійна поєднує у собі дії як оборонного, так і наступального характеру, а також дії, пов'язані із виявленням та припиненням кібершпигунства. Багато науковців умисно обмежуються використанням терміну «кібервійна», таким чином виключаючи із предмету дослідження психологічні операції.

У воєнній доктрині, також, часто використовується поняття «інформаційні операції», що потенційно становлять одну із найбільш руйнівних форм сили. Ці операції в основному спрямовані на порушення функціонування ключових військових, промислових та адміністративних об'єктів противника, його критично важливих систем, а також на маніпулювання інформацією та здійснення психологічного впливу на політичне та воєнне ке-

рівництво іншої держави, військових та цивільне населення, в першу чергу, з використанням інформаційно-комунікаційних технологій [10, с. 37].

Спільне дослідження Інституту Захід-Схід та Інституту з проблем інформаційної безпеки МДУ імені М. В. Ломоносова під назвою «Російсько-американський базовий перелік критичних понять у сфері кібербезпеки» стало однією із спроб погодження термінології та напрацювання спеціального глосарію з перекладом ключових термінів на дві мови – англійську та російську у сфері міжнародної інформаційної безпеки. Відповідно до першої редакції глосарію від 2011 року «кібервійна» – це «найвища ступінь кіберконфлікту між державами, під час якої держави застосовують кібератаки проти кібер-інфраструктур противника як частину воєнної кампанії. Кібервійна може бути оголошена формально однією чи всіма конфліктуючими сторонами або існувати de facto» [11, с. 30]. Варто звернути увагу на те, що в глосарії використовується виключно приставка «кібер-» і жодного разу ми не знаходимо в перекладі «інформаційна». Це пов'язано із різними підходами до змістовного наповнення цих понять. З точки зору науковців Російської Федерації термін «інформаційна» має більш широке значення, оскільки інформація має дві характеристики: змістовну та технічну, а термін «кібер» охоплює лише її технічний аспект. Американські ж вчені не заперечують проти інших аспектів інформації, але вважають її поза межами предмету регулювання.

У 2014 році було опубліковано нову розширену редакцію глосарію, яка на противагу попередній містить визначення безпосередньо «інформаційної війни». Розробники глосарію під цим терміном розуміють «найвищу ступінь інформаційного конфлікту між державами, коли інформаційні операції проводяться державними структурами для досягнення воєнно-політичних цілей» [12, с. 35].

На сьогодні єдиним конвенційним визначенням поняття «інформаційна війна» є визначення закріплене в Угоді між урядами держав-членів Шанхайської Організації Співробітництва про співробітництво в сфері забезпечення міжнародної інформаційної безпеки та двох додатках до неї. Відповідно до Додатку 1 до вищезазначеної конвенції «інформаційна війна» – це «протистояння між двома чи більше державами в інформаційному просторі з метою нанесення збитку інформаційним системам, процесам і ресурсам, критично важливим та іншим структурам, підриву політичної, економічної та соціальної систем, масового психологічного впливу на населення для дестабілізації суспільства та держави, а також з метою змусити державу приймати рішення в інтересах ворогуючої сторони» [13].

Не можна оминути увагою концепцію Конвенції про забезпечення міжнародної інформаційної безпеки, що була представлена в Лондоні у 2011 році на Конференції з питань кіберпростору. Не дивлячись на те, що запропонована концепція суттєво розширила коло воєнно-політичних загроз в інформаційному просторі, визначення поняття «інформаційна війна» повністю збігається із визначеннями, запропонованими у Конвенції держав-членів ШОС [14].

Що стосується питання застосування норм міжнародного права до ведення бойових дій у кіберпросторі, то тут міжнародна наукова спільнота однозначно погоджується із тим, що норми міжнародного права застосовуються і до діяльності держав у кіберпросторі. Ця думка була відображена у доповіді ГУЕ ООН, заслуханій під час проведення 65-ї сесії Генеральної Асамблеї ООН. У доповіді наголошується, що міжнародне право, зокрема Статут ООН повинен застосовуватись та має важливе значення для підтримання миру та стабільності, а також створення відкритого, безпечного, мирного та доступного інформаційного середовища [15, с. 8].

Відкритим залишається питання, яким саме чином ці норми повинні застосовуватись з огляду на відмінності кіберпростору від звичайних театрів бойових дій. Зазначимо, що у кіберпросторі не має географічної прив'язки, тому на держави може бути вчинено напад без фізичного вторгнення на їх територію, а атаки можуть бути спрямовані із будь-якої точки земної кулі.

Невирішеним однозначно з точки зору jus ad bellum залишаються питання, чи можна вважати операції у кіберпросторі застосуванням сили чи загрози силою відповідно до статті 2 (4) Статуту ООН і за яких обставин. А також, чи можна вважати операції у кіберпросторі збройним нападом відповідно до статті 51 Статуту ООН і чи виникає у постраждалих держав право на самооборону.

У статті 2 (4) Статуту ООН чітко визначено, що «усі члени ООН утримуються у своїх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і якимось іншим чином, несумісним із цілями ООН» [16]. Проте, у міжнародному праві немає чіткого визначення, які саме дії держав можна вважати застосуванням сили відповідно до положень цієї статті. Тому, думки науковців розділились: одна частина вважає, що стаття 2 (4) Статуту ООН прямо забороняє лише застосування військової сили, а інші наполягають на тому, що ця стаття, також, забороняє заходи політичного та економічного примусу. І відповідно виникає питання, яким чином можна кваліфікувати операції у кіберпросторі відповідно до заборони, визначеної Статутом ООН.

Не дивлячись на те, що трактування поняття застосування сили в міжнародному праві на сьогодні досить широке і може включати й інші форми примусу, все ж більшість науковців схиляється до ототожнення поняття застосування сили із застосуванням саме військової сили [17, с. 11]. Проте, це не означає, що така заборона поширюється лише на застосування кінетичної, хімічної, біологічної або ядерної зброї. Зокрема, Міжнародний Суд ООН, розглядаючи питання законності погрози та використання ядерної зброї, у своєму консультативному висновку зазначив, що заборона поширюється на застосування сили, незалежно від того яка зброя застосовувалась [18, с. 7]. Враховуючи такий підхід Міжнародного Суду ООН, операції у кіберпросторі потраплятимуть під заборону статті 2 (4) Статуту ООН у випадку, якщо їх застосування призведе до наслідків, які можна прирівняти до наслідків від застосування кінетичної, хімічної, біологічної чи ядерної зброї [19, с. 924]. Беззаперечно, до таких операцій відносяться ті їх види, що спрямовані на нанесення травм, призводять до втрати життя чи руйнування об'єктів інфраструктури, незалежно від того, чи завдають вони фізичного руйнування, функціональної шкоди, чи поєднують обидва випадки [20].

Труднощі виникають із кваліфікацією операцій у кіберпросторі, що не завдають великої матеріальної шкоди та не призводять до травм чи втрати життя. Деякі науковці наполягають на узагальненій кваліфікації таких операцій як інших форм примусу. Це твердження є досить суперечливим, оскільки передбачає виключення кібероперацій із парадигми використання сили та прирівнює їх до економічної чи політичної агресії. Кібератаки занадто багатогранні та занадто непередбачувані для того, щоб підпадати під класифікацію нелетальної зброї або засобів примусу, тому необхідно чітко розмежувати різні види кібератак відповідно до їх наслідків [9, с. 112]. В цілому, на даний момент немає консенсусу щодо кваліфікації кібератак з точки зору статті 2 (4) Статуту ООН, як немає і критеріїв їх розмежування. Відсутність правових норм та державної практики у цій сфері свідчить про те, що операції у кіберпросторі залишаються посередині між заходами застосування сили та іншими заходами примусу, і у разі виникнення суперечки кваліфікуватимуться окремо для кожного випадку [18, с. 9-12].

Ще одним із найважливіших питань забезпечення міжнародної інформаційної безпеки є гарантоване статтею 51 Статуту ООН право держав на індивідуальну чи колективну самооборону у разі збройного нападу. Закономірно виникає питання: чи можна прирівнювати операції у кіберпросторі до поняття збройного нападу?

Серед науковців сформувалось три основних підходи щодо вирішення цього питання. Перший ґрунтується на визначенні засобів вчинення кібероперацій. Його прихильники наполягають на тому, що самі по собі атаки у кіберпросторі не можуть бути визнані актами збройного нападу відповідно до статті 51 Статуту ООН, оскільки під час їх здійснення не використовується військова зброя. Відповідно до цього підходу кібератаки можна визнати актами збройного нападу тільки у випадку застосування звичайної військової зброї під час їх проведення [21, с. 845]. Проте, особливою відмінністю кібератак від інших видів зброї є саме їх можливість спричиняти значну шкоду без використання звичайних видів зброї.

Прихильники іншого підходу наполягають на тому, що актом збройного нападу можна вважати будь-які операції у кіберпросторі, основною ціллю яких є життєво необхідні комп'ютерні системи. Тобто, чи нанесено у результаті кібератаки збитку, достатнього, щоб виправдати застосування заходів самооборони у відповідь [21, с. 846-847]. Противники такого підходу наголошують на тому, що держави зможуть використовувати його з метою санкціонування силових заходів самооборони і конфлікт у кіберпросторі цілком ймовірно зможе перерости у повноцінний міждержавний конфлікт.

Третій підхід був запропонований професором М. Шміттом та є найбільш поширеним серед наукової спільноти. М. Шмітт пропонує розмежувати операції у кіберпросторі на акти збройного нападу та інші заходи примусу відповідно до наслідків, які вони спричинюють. У свою чергу ці наслідки він класифікує за наступними критеріями: серйозність – ступінь пошкодження чи збитків; оперативність – швидкість поширення негативних наслідків; спрямованість – прямий ефект чи необхідності додаткових факторів; здатність до проникнення; вимірюваність – передбачуваність певного рівня руйнування; передбачувана легітимність – когнітивний підхід до сприйняття легітимності тих чи інших дій [19, с. 936].

Такий підхід дозволяє зрозуміти, чи досягли кібератаки рівня збройного нападу та чи можуть вони виправдати застосування збройної самооборони. Довести доречність застосування подібних методів має держава, яка вдалась до силового самозахисту. Якщо рівня збройного нападу не було досягнуто, силове вирішення проблеми може базуватись лише на Статті 39 Статуту ООН, згідно з якою подібні питання мають бути розглянуті Радою Безпеки, яка і прийме рішення про те, як реагувати на загрози миру або його порушення [9, с. 134].

Висновки. Проаналізувавши різні теоретичні підходи до розуміння війни у кіберпросторі, приходимо до висновку, що на даний момент не існує єдиного бачення понять «інформаційна війна» та «кібервійна» ні з термінологічної, ні зі змістовної точок зору. Питання ведення бойових дій у кіберпросторі досить нове для світового співтовариства і тому знаходиться лише на стадії формування концептуальних підходів до його розуміння та вирішення. Не дивлячись на це, світове співтовариство одноголосно погоджується із тим, що міжнародне право застосовується до будь-якої діяльності держав у кіберпросторі, включаючи військову діяльність. Безумовно, існує велика кількість розбіжностей у підходах до тлумачення та застосування норм міжнародного права до діяльності держав у кіберпросторі з огляду на специфіку інформаційно-комунікаційних технологій, і світовій спільноті ще доведеться визначитись із підходом до врегулювання воєнного аспекту між-

народної інформаційної безпеки, проте найважливішим є той факт, що всі без винятку держави визнають, що їх військова діяльність у кіберпросторі знаходиться не в правовому вакуумі, а регулюється чинними нормами міжнародного права.

Список використаної літератури

1. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности [Електронний ресурс] / ГА ООН Документ A/65/201. – Режим доступу: http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF.
2. Lewis J. A. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization [Електронний ресурс] / J. A. Lewis, K. Timlin. – // Режим доступу: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.
3. Lewis J. A. Cybersecurity and cyberwarfare: assessment of national doctrine and organization [Електронний ресурс] / J. A. Lewis. – Режим доступу: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.
4. Streltsov A. A. International information security: description and legal aspects [Електронний ресурс] / A. A. Streltsov. – Режим доступу: http://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf.
5. Шмитт М. Н. Электронная война: нападение на компьютерные сети и jus in bello [Електронний ресурс] / М. Н. Шмитт. – // Режим доступу: https://www.icrc.org/rus/assets/files/other/06_irrc_846_schmitt_rus.pdf.
6. Joint Doctrine for Information Operations [Електронний ресурс]. – // Режим доступу: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
7. Дрёге К. Слезай с моего облака: кибернетическая война, международное гуманитарное право и защита гражданских лиц [Електронний ресурс] / К. Дрёге. – Режим доступу: https://www.icrc.org/rus/resources/documents/article/review-2012/irrc-886- droege.htm.
8. Aldrich R. W. The International Legal Implications of Information Warfare [Електронний ресурс] / R. W. Aldrich. – Режим доступу: http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf.
9. Kerschischnig G. Cyberthreats and International Law / G. Kerschischnig // The Hague: Eleven International Publishing. – 2012. – p. 311.
10. Komov S. Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law [Електронний ресурс] / S. Komov, S. Korotkov, I. Dylevski. – Режим доступу: http://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf.
11. Rauscher K. F. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations [Електронний ресурс] / K. F. Rauscher, V. Yaschenko. – Режим доступу: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=130080.
12. Godwin J. B. III Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2 [Електронний ресурс] / J. B. Godwin III, A. Kulpin, K. F. Rauscher, V. Yaschenko. – Режим доступу: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=178418.
13. Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року [Електронний ресурс]. – Режим доступу: http://base.spinform.ru/show_doc.fwx?rgn=28340.

14. Проект Конвенции об обеспечении международной информационной безопасности (концепция) [Електронний ресурс]. – Режим доступу: http://www.scrf.gov.ru/documents/6/112.html.
15. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности [Електронний ресурс] / ГА ООН Документ А/68/98. – Режим доступу: http://www.mofa.go.jp/files/000016407.pdf.
16. Статут Організації Об'єднаних Націй [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/charter/chapter7.shtml.
17. Brownlie I. International Law and the Use of Force by States [Електронний ресурс] / I. Brownlie. – Режим доступу: http://chinesejil.oxfordjournals.org/content/1/1/1.full.pdf.
18. Melzer N. Cyberwarfare and International Law [Електронний ресурс] / N. Melzer. – Режим доступу: http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.
19. Schmitt M. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework [Електронний ресурс] / M. Schmitt. – Режим доступу: http://cyber.law.harvard.edu/cybersecurity/Computer_Network_Attack_and_the_Use_of_Force_in_International_Law.
20. The Tallinn Manual on the International Law Applicable to Cyber Warfare [Електронний ресурс] / NATO Cooperative Cyber Defence Centre of Excellence. – Режим доступу: https://ccdcoe.org/249.html.
21. Hathaway A. The Law of Cyber-Attack [Електронний ресурс] / A. Hathaway, R. Crootof. – Режим доступу: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers.

LEGAL ANALYSIS OF THE USE OF CYBERSPACE FOR MILITARY PURPOSES

Grytsun O. O.

Postgraduate of the International Law Department of the Institute of International Relations of Kyiv National Taras Shevcnenko University.
Scientific Supervisor: Ph. D. in Law, Ap. Igor M. Zabara.

Abstract. *The article deals with international initiatives within the framework of the United Nations on the issue of resolving the problem concerning the use of cyberspace for military purposes by states as well as the regional approach provided by the Member States of the Shanghai Cooperation Organization. In addition, the article analyzes the conceptual and terminological differences in theoretical approaches of scientists from different countries on the definition of «information war», «cyberwar» and «operations in cyberspace», their characteristics and differences in meaningful approach of understanding these concepts. The article also provides a short review of international initiatives on definition the terminology in the sphere of international information security. The main part of the article is devoted to analysis of the application of international law to the conduct of states hostilities in cyberspace, including the classification of operations in cyberspace in terms of jus ad bellum, as well as the possibility of using the Charter of the United Nations to resolve the conduct of states in cyberspace.*

Key words: *information war, cyberwar, operations in cyberspace, information and communication technologies, international law.*

Referances

1. Doklad Gruppy pravitel'stvennykh ehkspertov po dostizhenijam v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti [Electr. resurs] / GA OON Dokument A/65/201. – Regim dostupu: http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF.

2. Lewis J. A. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization [Electr. resurs] / J. A. Lewis, K. Timlin. – Regim dostupu: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.
3. Lewis J. A. Cybersecurity and cyberwarfare: assessment of national doctrine and organization [Electr. resurs] / J. A. Lewis. – Regim dostupu: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.
4. Streltsov A. A. International information security: description and legal aspects [Electr. resurs] / A. A. Streltsov. – Regim dostupu: http://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf.
5. Schmitt M. N. Elektronnaya voina: napadenie na komp'yuternue seti i jus in bello [Electr. resurs] / M. N. Schmitt. – Regim dostupu: https://www.icrc.org/rus/assets/files/other/06_irrc_846_schmitt_rus.pdf.
6. Joint Doctrine for Information Operations [Electr. resurs]. – Regim dostupu: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
7. Drege C. Slezaj s moego oblaka: kiberneticheskaya voina, mezhdynarodnoe gymanitarnoe pravo i zaschita grazhdanskih lic [Electr. resurs] / C. Drege. – Regim dostupu: https://www.icrc.org/rus/resources/documents/article/review-2012/irrc-886-droege.htm.
8. Aldrich R. W. The International Legal Implications of Information Warfare [Electr. resurs] / R. W. Aldrich. – Regim dostupu: http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf.
9. Kerschischnig G. Cyberthreats and International Law / G. Kerschischnig // The Hague: Eleven International Publishing. – 2012. – p. 311.
10. Komov S. Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law [Electr. resurs] / S. Komov, S. Korotkov, I. Dylevski. – Regim dostupu: http://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf.
11. Rauscher K. F. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations [Electr. resurs] / K. F. Rauscher, V. Yaschenko. – Regim dostupu: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=130080.
12. Godwin J. B. III Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2 [Electr. resurs] / J. B. Godwin III, A. Kulpin, K. F. Rauscher, V. Yaschenko. – Regim dostupu: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=178418.
13. Ugoda mizh uryadamu derzhav-chleniv SHOS pro spivrobitnuctvo v oblasti zabezpechennya mizhnarodnoi informacijnoi bezpeku vid 16 chervnya 2009 roky [Electr. resurs]. – Regim dostupu: http://base.spinform.ru/show_doc.fwx?rgn=28340.
14. Proekt Konvencii ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (koncepciya) [Electr. resurs]. – Regim dostupu: http://www.scrf.gov.ru/documents/6/112.html.
15. Doklad Gruppy pravitel'stvennykh ehkspertov po dostizhenijam v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti [Electr. resurs] / GA OON Dokument A/68/98. – Regim dostupu: http://www.mofa.go.jp/files/000016407.pdf.
16. Statut Organizacii Ob'ednanuh Nacij [Electr. resurs]. – Regim dostupu: http://www.un.org/ru/documents/charter/chapter7.shtml.
17. Brownlie I. International Law and the Use of Force by States [Electr. resurs] / I. Brownlie. – Regim dostupu: http://chinesejil.oxfordjournals.org/content/1/1/1.full.pdf.
18. Melzer N. Cyberwarfare and International Law [Electr. resurs] / N. Melzer. – Regim dostupu: http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.
19. Schmitt M. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework [Electr. resurs] / M. Schmitt. – Regim dostupu: http://cyber.law.harvard.edu/cybersecurity/Computer_Network_Attack_and_the_Use_of_Force_in_International_Law.
20. The Tallinn Manual on the International Law Applicable to Cyber Warfare [Electr. resurs] / NATO Cooperative Cyber Defence Centre of Excellence. – Regim dostupu: https://ccdcoe.org/249.html.
21. Hathaway A. The Law of Cyber-Attack [Electr. resurs] / A. Hathaway, R. Crootof. – Regim dostupu: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers.

ПРАВОВОЙ АНАЛИЗ ИСПОЛЬЗОВАНИЯ КИБЕРПРОСТРАНСТВА В ВОЕННЫХ ЦЕЛЯХ

Грицун О. А.

Соискатель кафедры международного права Института международных отношений Киевского национального университета имени Тараса Шевченко.

Научный руководитель: кандидат юридических наук, доцент И. Н. Забара.

Аннотация. *В статье исследуются международные инициативы в рамках Организации Объединенных Наций по урегулированию проблемы использования государствами киберпространства в военных целях, а также региональный подход, закрепленный государствами-членами в рамках Шанхайской Организации Сотрудничества. Кроме того, в статье анализируются концептуальные и терминологические различия в теоретических подходах ученых разных стран касательно определения таких понятий как «информационная война», «кибервойна» и «операции в киберпространстве», их особенности и различия в содержательных подходах к пониманию этих понятий. В статье также предоставляется короткий обзор межгосударственных инициатив по согласованию терминологии в сфере международной информационной безопасности. Основная часть статьи посвящена анализу применения норм международного права к ведению государствами боевых действий в киберпространстве, в частности вопросам классификации операций в киберпространстве с точки зрения норм jus ad bellum, а также возможности применения положений Устава Организации Объединенных Наций к урегулированию поведения государств в киберпространстве.*

Ключевые слова: *информационная война, кибервойна, операции в киберпространстве, информационно-коммуникационные технологии, международное право.*