The author of the article focuses on the scientific analysis of certain definitions of the concept of «restriction of the rights to freedom of movement and free choice of place of residence», taking into account the specific historical realities of independent Ukraine.

Keywords: free choice of place of residence, freedom of movement, restrictions on the right to freedom of movement and free choice of place of residence, human rights.

Пташник І.Р.

МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВЕДЕННЯ КІБЕРВІЙН В 21 СТОЛІТТІ

УДК. 341.1./.8

Актуальність теми дослідження. На сьогодні уряди, вчені та бізнес прагнуть винайти та розробити технології, які нададуть перевагу людству в економічній та соціальних сферах. Розробки в комунікаційних сферах та в галузі інформатики (особливо актуально стосовно технологічного розвитку кіберпростору) не є виключенням в цьому відношенні. Проте варто пам'ятати, що нові технології спричиняють виникнення небезпек, особливо, якщо такі технології використовуються під час збройних конфліктів. Так, найбільших дискусій на сьогодні отримало питання, чи можуть норми міжнародного гуманітарного права поширюватись на випадки здійснення кібератак під час збройних конфліктів.

У багатьох країнах, таких як США, Ізраїль, Франція, Великобританія, Нідерланди, Німеччина, Росія, Індія, Іран, Пакистан, Австралія, Південна і Північна Корея вже давно з'явилися структури у збройних силах, які відповідають за ведення «кібервійни».

Варто відзначити недостатній ступінь дослідження даної тематики серед вітчизняних та зарубіжних науковців, що, враховуючи на існуючі загрози національній безпеці України, робить дану тему як ніколи актуальною.

Перш ніж розпочати характеристику поняття «кібервійна», варто звернутись до положень Женевських конвенцій 1949 року, які закріпили поняття «міжнародний збройний конфлікт» та «неміжнародний збройний конфлікт»». Так, ЖК 1949 в спільній статті 2 вказує на необхідність наявності всіх випадків оголошеної

війни чи будь-якого іншого збройного конфлікту, що може виникнути між двома чи більше Високими Договірними Сторонами, навіть якщо стан війни не визнаний однією з них; випадки часткової або повної окупації території Високої Договірної Сторони, навіть якщо цій окупації не чиниться жодний збройний опір [1]. Під неміжнародним збройний конфліктом спільна стаття 3 ЖК 1949 року розуміє збройний конфлікт, який не має міжнародного характеру та виникає на території однієї з Високих Договірних Сторін [1].

Аналізуючи положення міжнародного гуманітарного права варто зазначити, що поняття «війна» не має правового закріплення в жодному з відомих міжнародно-правових інструментів.

Додаткові складнощі викликає термінологічна плутанина. По-перше, як в засобах масової інформації, так і в науковій літературі дуже широко використовується поняття «інформаційні війни», яке бентежить, тому що застосовується воно не тільки до конфліктів, а й до пропаганди та роботи ЗМІ. Безумовно, до інформаційних війн, які полягають, наприклад, в навмисній дезінформації населення в певних політичних цілях, міжнародне гуманітарне право не має ніякого відношення. Воно може бути застосовано тільки до класичних збройних конфліктів, пов'язаних із застосуванням певного роду сили.

Проте, не дивлячись на те що кіберконфлікти представляють собою особливі ситуації, консультативним рішенням Міжнародного суду ООН, було підтверджено, що принципи міжнародного гуманітарного права регулюють всі види, методи і засоби ведення війни, які коли-небудь з'являлися, існують на даний момент або з'являться в майбутньому. Також варто пам'ятати, що принцип гуманності - основа МГП - безумовно можна застосувати і до кіберпростору.

Повертаючись до аналізу кібератак та кібервійни з точки зору міжнародного гуманітарного права варто зазначити наступне.

Кібернетична війна (кібер-війна) означає масштабну координовану цифрову атаку на уряд іншим урядом або великими групами громадян. Це є дія держави для проникнення в комп'ю-

тери чи мережі інших країн з метою заподіяння шкоди або порушення. Термін «кібер-війна» також може використовуватися для опису нападів між корпораціями, терористичними організаціями або просто нападами осіб, яких називають хакери [2]. Якщо детальніше проаналізувати поняття кібер-війна, то варто дослідити суть його складових, якими є поняття «кіберпростір» та «війна». Слово «кібер» походить від слова кібернетика, що, в свою чергу, є похідним від грецького слова *kybernetike*, яке дослівно перекладається як «мистецтво управління». За визначенням Міжнародного союзу електрозв'язку, **кіберпростір** – це фізичний і нефізичний простір, що складається з комп'ютерів, комп'ютерних систем, мереж та комп'ютерних програм, комп'ютерних даних, контенту, даних трафіку та користувачів. Оскільки правового визначення поняття «війна» на сьогодні немає, то її варто розглядати як форму вирішення конфлікту між суб'єктами міжнародного права (державами, міжнародними організаціями), що реалізується у формі боротьби з використанням насильницьких методів і засобів для досягнення певних цілей.

Основними рисами кібервійни на сьогодні є:

- Відсутність чітко вираженого «агресора». Якщо у випадках «класичних» збройних конфліктів сторони конфлікту можна чітко прослідкувати, то у випадку здійснення кібератак це практично не можливо, оскільки, зазвичай, географічним джерелом кібератаки є зовсім не та держава, якій така атака може бути об'єктивно вигідною;
- Особливість ведення атак – це їх швидкість, яка скорочує час між початком т.зв. агресії та наслідками, а також неможливість спрогнозувати момент їх завершення.
- Відсутність видимих руйнувань.
- Особливі засоби ведення атак – «кіберзброя», яка не обов'язково знищує об'єкт атаки, а через певний набір команд, змінює існуючі алгоритми функціонування системи й активізує потрібні реакції.
- Час вчинення заборонених дій – на відміну від «класичних» збройних конфліктів, які можуть вчинятись виключно у воєнний час, кібератаки можуть бути вчинені як в мирний, так і в військовий час.

Повертаючись до можливості застосування міжнародного гуманітарного права під час кібератак, то варто звернути увагу, що думки сучасних вчених розділились. Так, одні вважають, що не важливо, які методи ведення війни застосовуються - цифрові або кінетичні. Сам факт початку застосування цих методів і, як наслідок, досягнення певного порогу насильства, на думку цих авторів, можуть служити достатньою підставою для визнання наявності збройного конфлікту, наприклад, якщо за допомогою кіберзброї виводиться з ладу система навігації, в результаті чого порушується робота аеропортів, зіткнення літаків. Є й інша думка з цього приводу, яка полягає в тому, що для кіберзброї повинен бути встановлений більш високий поріг інтенсивності: такі операції повинні проводитися постійно, а шкода від її застосування повинна бути значною. Звісно ж, що це думка не цілком заснована на положеннях міжнародного гуманітарного права, оскільки якщо ми говоримо про міжнародний збройний конфлікт, то для його констатації досить і одиничного випадку застосування сили, щоб громадянське населення отримало передбачений договором захист, а дії держав підлягали скрупульозній оцінці на предмет відповідності критеріям пропорційності та іншим обмеженням [3].

Можна констатувати що на сьогодні не існує жодного юридично обов'язкового міжнародного документа, який би в повній мірі регулював відносини в сфері використання кіберпростору. В 2017 році відбулась презентація «Таллінської книги 2.0: міжнародне право, що застосовується до кібер-операцій» (*Tallinn Manual 2.0: International Law Applicable to Cyber Operations*), яка акцентує увагу на особливості дієвих кібер-діянь, які сьогодні утворюють більшість кібер-нападів. Примітно, що за чотири роки назва книги змінювалася з «кібер-війни» на «кібер-операції», що відображає, що в сучасних країнах кібернапади найчастіше не дотягують до «порогу» за яким міжнародне право зазвичай оголошує їх офіційним актом війни. Аналізуючи положення документу варто відзначити, щл Таллінська книга має ряд недоліків:

- Сфера правового регулювання невиправдано звужена тільки відносинами військового часу - *jus ad bellum або jus in*

bello. Це означає, що зі сфери гуманітарного права викреслена найцікавіша частина, а саме запобігання кібервійни.

- Предмет правового регулювання кібервійни відрізняється від традиційних методів ведення війни. Автори документа виходили з того, що немає різниці між застосуванням бомб або ракет і комп'ютера.

- Особливості кібервійни не охоплюються традиційною структурою гуманітарного права. Застосовуючи структурні інструментарії Женевських конвенцій 1949 р. до кібервійни, автори Талліннської книги характеризують відношення кібероперації до актів шпигунства, блокади, окупації, нейтралітету та ін. об'єктів. Тим самим вони створюють набір безсистемних абстрактних побажань воюючим сторонам. Проте театр кібервійни глобальний, його учасниками є все людство, без відмінностей серед потенційних учасників.

- Перспектива подальшої роботи над законами кібервійни вбачається не в переказі Женевських конвенцій, вносячи зміни щодо кібер-лексики, а зі створення якісно нової загальної Конвенції безпеки кіберпростору, в якій, перш за все, потрібно визначити правовий стан - «кіберсвіту» і «кібервійни». Далі регламентувати сфери застосування права в кіберпросторі, по колу осіб і за видами технічних телекомунікаційних та програмних об'єктів [4].

Таким чином на сьогодні в міжнародному праві виникла проблема правового регулювання даних відносин. Кібератаки є різновидом агресії, і вони повинні бути заборонені міжнародним правом одним з двох способів: або шляхом прийняття міжнародної конвенції або доповнення поняття агресії.

Розглядаючи перший потенційний варіант доповнення елементів, що складають поняття «агресія», варто зазначити, що в Резолюції Генеральної Асамблеї ООН від 14 грудня 1974 року 3314 (XXIX) «Поняття агресії» під даним поняттям розуміється застосування збройної сили державою проти суверенітету, територіальної недоторканності або політичної незалежності іншої держави, або яким-небудь іншим чином, несумісним зі Статутом Організації Об'єднаних Націй [5]. Звісно, даний спосіб регулю-

вання правовідносин, пов'язаних із регулюванням кібератак є цілком прийнятний, однак все ж слід враховувати той факт, що дані відносини є складними і вимагають більш детального регулювання, ніж просто включення в дефініцію.

Інший варіант врегулювання даного питання передбачає прийняття спеціальної конвенції. Даний підхід видається найбільш вірним, оскільки з'являється можливість висвітлити всі проблемні моменти, пов'язані з кібератаками та інформаційною безпекою в цілому. В даний час розробка проекту конвенції здійснюється групами урядових експертів. Розглядаючи об'єктивно результати їх роботи, можна відзначити, що в даний час вдалося узгодити лише думки стосовно застосування міжнародного права до кіберпростору. Незважаючи на раціональність прийняття конвенції, варто відзначати той момент, що, швидше за все, вона не буде прийнята найближчим часом, оскільки думки багатьох провідних країн розходяться по істотним питанням регулювання кіберпростору.

Окрім того варто пам'ятати і про можливість вирішення питання правового регулювання проблемних моментів, пов'язаних з кібератаками з позиції міжнародного гуманітарного права. Стаття 36 Додаткового Протоколу до Женевських Конвенцій передбачає, що при розробці нової зброї державою, не обов'язково приймати нову конвенцію, щоб використання/заборона використання цієї зброї регулювалося міжнародним гуманітарним правом [6].

Підводячи підсумки необхідно говорити про те, що питання, пов'язане з регулюванням кіберпростору в цілому, і здійснення кібератак зокрема, є одним з найбільш гострих в сучасному світі. Найбільш раціональним врегулюванням даного питання видається прийняття конвенції, яка б відобразила всі аспекти даних правовідносин. Однак, необхідно розуміти, що в сучасній геополітичній ситуації прийняття конвенції може бути відкладено на тривалий термін, що створює проблему відсутності регулювання одного з найбільш небезпечних явищ в сучасному світі.

1. *Женевська конвенція про поводження з військовополоненими від 12.08.1949. – Електронний ресурс. – [Режим доступу]: http://zakon3.rada.gov.ua/laws/show/995_153*

2. *Cyber Warfare Law and Legal Definition. – Електронний ресурс. – [Режим доступу]: https://definitions.uslegal.com/c/cyber-warfare/*
3. *М. Гаврилова «Применение международного права в киберпространстве»//ИНДЕКС БЕЗОПАСНОСТИ. - № 3 (114), Том 21. – Електронний ресурс. – [Режим доступу]: http://pircenter.org/media/content/files/13/14513439760.pdf*
4. *Право кибервойны// Гуманитарное право. - Електронний ресурс. – [Режим доступу]: https://humanlaw.ru/9-article/20-law-cyberwar.html*
5. *Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX) dated 14 December 1974. - Електронний ресурс. – [Режим доступу]: http://hrlibrary.umn.edu/instree/GAres3314.html*
6. *Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. – Електронний ресурс. – [Режим доступу]: http://zakon5.rada.gov.ua/laws/show/995_199*

Пташник І.Р. Міжнародно-правове регулювання ведення кібервійн в 21 столітті

Основною метою статті є аналіз міжнародного гуманітарного права та можливість його застосування під час кібератак. Автор аналізує положення Женевських конвенцій 1949 року, які дають пояснення поняттю «збройний конфлікт». Автором в ході дослідження запропоновано регулювати випадки ведення кібератак та кібервійн положеннями міжнародного права, що регулюють агресію.

Ключові слова: ядерна зброя, міжнародне право, міжнародна співпраця, діяльність ООН, міжнародний договір, конвенція.

Пташник И.Р. Международно-правовое регулирование ведения кибервойн в 21 веке

Основной целью статьи является анализ международного гуманитарного права и возможность его применения при кибератаках. Автор анализирует положение Женевских конвенций 1949 года, которые дают объяснение понятию «вооруженный конфликт». Автором в ходе исследования предложено регулировать случаи ведения кибератак и кибервойн положениями международного права, регулирующих агрессию.

Ключевые слова: кибероружие, международное право, международное гуманитарное право, деятельность международных организаций, международный договор, вооруженный конфликт.

Ptashnyk I.R. International legal regulation of conduction of cyber warfare in the 21st century

Today's biggest debate has been connected to the possibility of application of rules of international humanitarian law to cases of cyberattacking in armed conflicts. However, to fully understand the problem there is the need for definition and features of cyber warfare. During the research the author defines cyber war as a large-scale

coordinated digital attack on the government by another government or large groups of citizens. This is an act of the state for penetration into computers or networks of other countries for the purpose of causing harm or violation.

Today, the main features of the cyberwar are: the lack of a clearly expressed «aggressor», the peculiarity of the attacks, the absence of visible destruction, special means of attack, the time of the commission of prohibited acts.

We can state that today there is no legally binding international instrument that fully regulates relations in the area of cyberspace use. Cyberattacks are a form of aggression and they should be prohibited by international law in one of two ways: either by adopting an international convention or supplementing the notion of aggression.

While conducting a study the author analyzed the relevant provisions of four Geneva Convention 1949 and their Additional Protocol 1977; issues and provisions of Tallinn Manual 2.0. International Law Applicable to Cyber Operations.

Keywords: cyber-weapons, international law, international humanitarian law, the activities of international organizations, an international treaty, an armed conflict.

Розвадовський В.І.

ПРОБЛЕМИ КОНСТИТУЦІЙНОГО КОНТРОЛЮ І НАГЛЯДУ ЯК ЦІННОСТІ В УКРАЇНІ

УДК 342.565.2(477)

Постановка проблеми. Варто зазначити, що проблема судового захисту конституцій в Європі набула актуальності після першої, та особливо – другої світової війни. Науковці, практикуючі юристи традиційно пов'язують утвердження конституційного судочинства з формуванням спеціальних конституційних судів.

У результаті становлення України як незалежної держави органом конституційного контролю і нагляду став Конституційний Суд України, що забезпечує верховенство Конституції і здійснює її офіційне тлумачення [1]. У зв'язку з цим питання конституційного контролю і нагляду тривалий час привертає увагу суспільства, це пояснюється тим, що він має на меті правову охорону Конституції, забезпечення прозорості і правопорядку, що є досить актуальним для України.

Аналіз останніх досліджень і публікацій. Науковою основою дослідження стали праці науковців як минулого так і сучас-