АКТУАЛЬНІ ПИТАННЯ МІЖНАРОДНОГО ПРАВА

УДК 341.211:341.233

КАМІНСЬКИЙ І. І.,

аспірант кафедри міжнародного права та міжнародних відносин Національного університету «Одеська юридична академія»

КОНЦЕПЦІЯ ДЕРЖАВНОГО СУВЕРЕНІТЕТУ В КОНТЕКСТІ ЗАСТОСУВАННЯ КІБЕРСИЛИ

Анотація. У статті досліджується питання здійснення державами своїх суверенних прав у кіберпросторі. Автор намагається встановити правову природу останнього, щоб з'ясувати, чи є можливість розглядати принцип невтручання, який тісно пов'язаний із концепцією державного суверенітету, як міжнародно-правову підставу заборони застосування кіберсили.

Ключові слова: державний суверенітет, незбройна сила, застосування кіберсили, принцип невтручання.

Постановка проблеми. Очевидно, що інформаційно-цифрова сфера здійснює значний вплив на життєдіяльність як людей, так і всієї біосфери на планеті, а також визначає рівень розвиненості окремих країн, регіонів та всього світового співтовариства. Безумовно, одним із найгостріших питань, що постало у зв'язку з розвитком кіберсфери, є належне забезпечення кібербезпеки, адже останнім часом збільшилась кількість кіберінцидентів, які завдали значної шкоди потерпілим державам. Наприклад, кібератаки в Естонії в 2007 р. спричинили тимчасову зупинку роботи деяких урядових і приватних структур [1]. У 2010 р. іранський ядерний центр став об'єктом нападу за посередництвом комп'ютерного «черв'яка» *Stuxnet*, що викликало втрату контролю над його центрифугами [2].

У контексті концепції незбройної сили (сукупності засобів впливу, які не є зброєю) названі заходи пропонується іменувати кіберсилою. З прикладів помітно, що застосування кіберсили є неправомірним, адже пору-

шує міжнародний правопорядок та завдає шкоди потерпілим державам. Однак не є очевидним, яка саме імперативна норма міжнародного права повинна бути основою заборони застосування незбройної сили взагалі й кіберсили зокрема.

Аналіз останніх досліджень і публікацій. Окремі питання здійснення державою суверенітету в кіберпросторі досліджувались Е. Єнсеном, М. О'Коннел, Д. Сілвером, В. фон Хайнегом, Ф. Хінслі, В. Шарпом та іншими вченими. Водночас з огляду на порівняну новизну виділення незбройної сили та її видів, зокрема й кіберсили, варто констатувати незначне зацікавлення проблематикою державного суверенітету в контексті застосування кіберсили.

Метою статті є встановлення особливостей здійснення державами суверенних прав у кіберпросторі.

Виклад основного матеріалу дослідження. У доктрині порівняно тривалий час спостерігаються суперечки щодо віднесення заборони застосування кіберсили до предметного кола ч. 4 ст. 2 Статуту ООН, яка закликає держави у своїх міжнародних відносинах утримуватись від погрози силою або її застосування. Труднощі з правильною кваліфікацією таких діянь доповнюються тим, що поки що жодна держава не вживала будь-яких дій і не займала чіткої правової позиції, звинувачуючи іншу державу в неправомірному застосуванні кіберсили, кваліфікуючи дії останньої або за ч. 4 ст. 2, або за іншою міжнародно-правовою нормою.

В американській доктрині міжнародного права останнім часом спостерігається переважання поглядів щодо можливого включення деяких актів неправомірного застосування кіберсили до сфери поняття «сила» за ч. 4 ст. 2, якщо такі акти володіють ознаками та спричинюють наслідки, аналогічні звичайним збройним нападам. Так, Національна дослідницька рада США на одному зі своїх засідань постановила, що кібератаки повинні розглядатись у спектрі Статуту ООН та звичаєвих принципів *jus ad bellum*, якщо їхні наслідки еквівалентні військовим атакам [3, с. 33–34].

В. Шарп пропонує широке і водночас просте правило: будь-яка кібератака, що навмисно спричинила будь-які деструктивні наслідки на суверенній території іншої держави, є неправомірним застосуванням сили в значенні ч. 4 ст. 2, тим самим негайно формуючи право на самооборону [4, с. 90–91].

Д. Сілвер вважає, що ключовим критерієм, за яким необхідно визначати, чи є застосування кіберсили збройним нападом, є «жорстокість завданої шкоди». На його переконання, кібератака виправдовує самооборону лише якщо силовими наслідками є фізичні травми чи пошкодження власності або якщо такі наслідки мають схожість із результатами збройного примусу [5, с. 90–91].

Однак наслідки розширення об'єму ч. 4 ст. 2 за межі застосування військових заходів були передбачені багато десятиліть тому Г. Кельзеном: «Якщо <…> «застосування сили» <…> тлумачилось би в широкому сенсі

цього терміна <…> Статут ООН обмежував би свободу дій її членів набагато більше, ніж будь-яке національне законодавство обмежує свободу дій його суб'єктів» [6, с. 5]. На думку М. О'Коннел, спроби вчених використати критерії застосування збройної сили в разі самооборони в умовах кібератак є важким або взагалі нездійсненним завданням. Дослідник вважає, що в цьому разі відсутні як належні засоби, так і належні наслідки, необхідні для застосування ст. 51. Окрім Статуту ООН, як акцентує увагу М. О'Коннел, Міжнародний суд у 6 справах вказував на важливість дотримання звичаєвого міжнародного права та основних принципів, що стосуються легітимного застосування сили. Для використання збройних сил у самообороні необхідно, щоб напад був збройним, значним. Також самооборона має бути пов'язана з регіоном, де мав місце напад. Застосування сили має бути останньою дією та мати успіх саме в досягненні захисту, а також має бути пропорційним завданій шкоді [7, с. 6].

П. Зінгер і Н. Шахтман висловлюють схожу думку, проте керуються не судовою практикою, а державною. Аналізуючи наслідки застосування кіберсили проти Естонії в 2007 р. та порівнюючи кібератаки проти грузинського уряду з активними російськими військовими діями в цій країні в 2008 р., вони доходять висновку, що наслідки кібератак є незрівнянними з наслідками збройного нападу. Тому вчені вважають, що неправильно та недоцільно застосовувати норми *jus ad bellum* до кіберпростору [8].

Підсумовуючи цю дискусію, необхідно вказати, що на сучасному етапі міжнародного праворозуміння й правозастосування вважається, що ч. 4 ст. 2 Статуту ООН стосується тільки випадків застосування збройної сили, тому, відповідно, не може бути використана як міжнародно-правова підстава заборони застосування незбройної сили. З огляду на характер реалізації державами заходів, що являють собою незбройний вплив, вбачається, що міжнародно-правова заборона останніх постає з іншого основного принципу міжнародного права – принципу заборони втручання в справи, які належать до внутрішньої компетенції будь-якої держави (принципу невтручання).

Водночас варто акцентувати увагу на тому, що згаданий принцип тісно пов'язаний із концепцією державного суверенітету та іншими основними принципами міжнародного права. Так, Д. Лубан зазначає: «В основі обов'язку утримуватись від втручання у внутрішні справи лежить принцип державного суверенітету, похідним від якого він і є» [9, с. 199]. Ф. Хінслі стверджував, що принцип невтручання вимагає насамперед поваги до того, що він насправді захищає, тобто до принципу державного суверенітету [10, с. 27]. Л. Оппенгейм вважав заборону втручання наслідком права кожної держави на суверенітет, територіальну цілісність і політичну незалежність [11, с. 428].

Однак з огляду на специфіку кіберзасобів природно виникає питання: чи спрямоване застосування кіберсили на порушення суверенітету потерпілої держави? Інакше кажучи, чи володіють держави суверенітетом у

кіберпросторі? Ствердна відповідь на ці питання дасть змогу розглядати кібервплив як примус, заборонений принципом невтручання, що робить останній міжнародно-правовою підставою заборони застосування кібер-сили.

Державний суверенітет є основою сучасного міжнародного правопорядку. Статут ООН підтверджує це, встановлюючи в ч. 1 ст. 2: «Організація заснована на принципі суверенної рівності всіх її членів». Хоча значення поняття «суверенітет» протягом багатьох століть слугувало причиною наукових дискусій, загальний сенс цієї категорії розуміється приблизно однаково в різних школах міжнародного права. Так, К.А. Бекяшев вважає, що суверенітет – це політико-юридичне поняття, яке відображає органічну властивість держави – верховенство на своїй території, тобто відсутність на цій території іншого суб'єкта влади, який вирішує питання правотворчості, правозастосування (у тому числі правоохорони), судочинства й незалежності в міжнародних відносинах [12, с. 56].

Інакше кажучи, суверенітет є сукупністю прав та обов'язків держав у двох сферах – внутрішньодержавній і міжнародній. У внутрішньодержавній сфері, як зазначає Дж. Кроуфорд, суверенітет забезпечує винятковість у здійсненні влади на власній території [13, с. 448]. Міжнародний суд ООН у своєму рішенні в справі про протоку Корфу від 1949 р. («Об'єднане Королівство проти Албанії») підтвердив таке розуміння суверенітету: «Під суверенітетом ми розуміємо всю сукупність прав та атрибутів, якими володіє держава на своїй території, а також у відносинах з іншими державами» [14, с. 43]. Водночас у міжнародному праві під територією, на яку може поширюватись суверенітет, розуміється вся земна куля, у тому числі сухопутні та водні простори, надра й повітряний простір над ними, а також космічний простір, у тому числі Місяць та інші небесні тіла [15, с. 439]. Просторові межі суверенітету конкретної держави визначаються її державними кордонами.

Як зазначалось, суверенітет, крім прав, передбачає наявність певних обов'язків. Це підтверджує Міжнародний суд ООН: «Суверенітет обдаровує держави правами та накладає на них обов'язки» [14, с. 43]. Зобов'язання, пов'язані із суверенітетом, включають обов'язок визнавати суверенітет інших держав, обов'язок не втручатись у сфери виключної компетенції іншої держави та обов'язок контролювати дії, що здійснюються в межах географічних кордонів [13, с. 447].

Зі свого боку під кіберпростором розуміють середовище, створене злиттям об'єднаних комп'ютерних мереж, інформаційних систем і телекомунікаційних інфраструктур, що традиційно іменуються Інтернетом та «всесвітньою павутиною» (World Wide Web) [4, с. 15]. Таким чином, кіберпростір не є визначеним місцем, це сфера поза фізичним виміром і часом.

Як зазначає В. фон Хайнег, кіберпростір характеризується анонімністю й повсюдністю, тому логічно було б прирівняти його до відкритого моря, міжнародного повітряного простору та космосу, тобто розглядати

кіберпростір як загальне надбання, або *res communis omnium* [16, с. 9]. Схожі твердження були висунуті Департаментом оборони США, де заявили: «Загальне надбання людства складається з міжнародних вод, повітряного простору, космосу та кіберпростору» [17]. Однак така категоризація призведе до очевидного висновку, що кіберпростір не підлягає суверенітету жодної держави чи групи держав. Як вказав Інститут міжнародного гуманітарного права, відмінною особливістю кіберпростору є те, що він є умовним середовищем та перебуває поза юрисдикцією будь-якої держави [18].

Водночас не можна заперечувати, що держави мають право розвивати свої кіберможливості з огляду на власні інтереси й ресурси. Держава може обрати шлях екстенсивного розвитку, як це зробила Естонія, або закрити свої «кіберкордони» від іноземного впливу, як це зробила Північна Корея. Держави зобов'язані визнавати й поважати це право та не втручатись у внутрішні справи з питань кіберполітики інших держав [19, с. 286].

Деякі вчені зауважують, що суверенітет не може застосовуватись до кіберпростору, оскільки останній є віртуальним середовищем і не належить до будь-якого суверенітету. Проте очевидно, що певний суб'єкт повинен контролювати кіберпростір, щоб він існував і функціонував, адже кіберпростір потребує фізичного устрою. Як вказують науковці, хоча жодна держава не може здійснювати суверенітет над кіберпростором *per se*, держави володіють суверенітетом над кіберінфраструктурою, розташованою на їхніх територіях, і діяльністю, пов'язаною з такою інфраструктурою [20]. Кіберінфраструктура зазвичай складається із серверів, комп'ютерів, кабелів та інших фізичних компонентів. Вони знаходяться не в кіберпросторі, а на певній державній території, тому очевидно, що держава володіє юрисдикцією й суверенітетом над цими компонентами.

Також кіберпростір не є відокремленим від суверенітету, оскільки фінансові відносини й транзакції в кіберпросторі вимагають відповідного законодавства. Інакше такі відносини були б нікчемними та сповненими ризиків для кожної зі сторін [21, с. 35].

Крім того, кіберпростір не може перебувати поза суверенітетом, оскільки державна присутність у кіберпросторі, як демонструють численні інциденти, безпосередньо впливає на її національну безпеку. Адже зараз багато держав контролюють деякі елементи своєї критичної інфраструктури (банківська й фінансова системи, транспорт, нафтові й газові магістралі, електропостачання тощо) за допомогою кіберпростору, що водночас робить їх дуже вразливими. Таке твердження підкреслюється в Національній стратегії безпеки кіберпростору США: «У мирний час вороги Америки можуть <…> готуватись до кібератаки, ідентифікуючи інформаційні системи США, визначаючи доступ до основних цілей. У воєнний час супротивники можуть <…> атакувати об'єкти критичної інфраструктури <…> або підривати громадський спокій в інформаційних системах» [22]. Оскільки ймовірність заподіяння шкоди в кіберпросторі реальна, держави не можуть залишити його без управління, а повинні знайти шлях для

здійснення контролю в кіберпросторі, щоб зменшити в ньому свою вразливість. Відповідно, як «реальний» світ вимагає державного суверенітету, щоб упорядковувати, захищати й карати різних суб'єктів, так і кіберпростір вимагає такого суверенного впливу.

Висновки. Очевидно, що держави не можуть здійснювати суверенітет над кіберпростором як віртуальним середовищем, тому що він як об'єкт внутрішньодержавного й міжнародно-правового регулювання є юридичною фікцією, «місцем», яке не існує в об'єктивному світі. Водночас було доведено, що держави володіють суверенними правами щодо об'єктів своєї кіберінфраструктури, а також обов'язками контролювати цю інфраструктуру та попереджати випадки її умисного використання з метою завдати шкоди іншим державам. Інакше кажучи, формально концепція державного суверенітету поширюється тільки на фізичну територію держави, проте може виходити за межі поняття територіального контролю. Так, Р. Бакен зазначає: «Державний суверенітет захищає від зовнішніх втручань право держави здійснювати певну політику та приймати рішення щодо внутрішніх і зовнішніх питань» [23, с. 223]. Очевидно, що такі питання можуть стосуватись кіберпростору та бути пов'язаними з ним, тому не варто заперечувати зв'язок державного суверенітету з кіберпростором.

Література:

1. Hackers Take Down the Most Wired Country in Europe [Електронний ресурс]. – Режим доступу : http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.
2. Stuxnet worm "targeted high-value Iranian assets" [Електронний ресурс]. – Режим доступу : http://www.bbc.com/news/technology-11388018.
3. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities. – Washington : The National Academies Press, 2009. – 367 p.
4. Sharp W.G. Sr. Cyberspace and the Use of Force // W.G. Sharp Sr. – Falls Church : Aegis Research Corp., 1999. – 234 p.
5. Silver D. Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter / D. Silver // International Law Studies. – 2002. – Vol. 76. – P. 73–97.
6. Kelsen H. General International Law and the Law of the United Nations / H. Kelsen // Van der Molen J. The United Nations: Ten Years' Legal Progress / J. Van der Molen, W. Pompe and J. Verzijl (eds). – The Hague : Nederlandse Studentenvereniging voor Wereldrechtsorde, 1956. – P. 4–6.
7. O'Connell M. Cyber Security and International Law / M. O'Connell // International Law Meeting Summary. – 2012. – № 17. – P. 5–7.
8. Singer P. The Wrong War: The Insistence on Applying Cold War Metaphors to CyberSecurity Is Misplaced and Counterproductive / P. Singer, N. Shachtman [Електронний ресурс]. – Режим доступу : http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman.
9. Luban D. Just War and Human Rights / D. Luban // Beitz C. International Ethics / C. Beitz et. al. (eds.). – New Jersey : Princeton University Press, 1985. – P. 195–202.

10. Hinsley F.H. Sovereignty / F.H. Hinsley. – 2nd ed. – Cambridge : Cambridge University Press, 1986. – 268 p.
11. Jennings R. Oppenheim's International Law. Vol. 1: Peace / R. Jennings, A. Watts. – 9th ed. – London : Oxford University Press, 1992. – 2887 p.
12. Международное право : [учебник для бакалавров] / отв. ред. К.А. Бекяшев. – М. : Проспект, 2015. – 350 с.
13. Crawford J. Brownlie's Principles of Public International Law / J. Crawford. – 8th ed. – Oxford : Oxford University Press, 2012. – 888 p.
14. Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania) // Separate opinion of Judge Alvarez. – 1949. – 9 April. – P. 39–48.
15. Международное право / отв. ред. : В.И. Кузнецов, Б.Р. Тузмухамедов. – М. : НОРМА – ИНФРА-М, 2010. – 720 с.
16. Von Heinegg W.H. Legal Implications of Territorial Sovereignty in Cyberspace / W.H. von Heinegg // 4th International Conference on Cyber Conflict / C. Czosseck, R. Ottis, K. Ziolkowski (eds.). – Tallinn : NATO CCD COE Publications, 2012. – P. 7–19.
17. Strategy for Homeland Defense and Civil Support (June 2005). US Department of Defense [Електронний ресурс]. – Режим доступу : http://www.wslfweb.org/docs/usg/homeland.pdf.
18. Sanremo Handbook on Rules of Engagement (September 2009). International Humanitarian Law Institute [Електронний ресурс]. – Режим доступу : http://www.iihl.org/wp-content/uploads/2015/12/ROE-HANDBOOK-ENGLISH.pdf.
19. Jensen E.T. Cyber Sovereignty: The Way Ahead / E.T. Jensen // Texas International Law Journal. – 2014. – Vol. 50. – Issue 2. – P. 275–304.
20. Tallinn Manual on the International Law Applicable to Cyber Warfare [Електронний ресурс]. – Режим доступу : https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.
21. Goldsmith J. Who Controls The Internet? Illusions Of A Borderless World / J. Goldsmith, T. Wu. – Oxford : Oxford University Press, 2006. – 226 p.
22. The National Strategy to Secure Cyberspace (February 2003) [Електронний ресурс]. – Режим доступу : https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
23. Buchan R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? / R. Buchan // Journal of Conflict and Security Law. – 2012. – Vol. 17. – № 2. – P. 211–227.

Каминский И. И. Концепция государственного суверенитета в контексте применения киберсилы

Аннотация. В статье исследуется вопрос осуществления государствами своих суверенных прав в киберпространстве. Автор пытается установить правовую природу последнего, чтобы выяснить, есть ли возможность рассматривать принцип невмешательства, который тесно связан с концепцией государственного суверенитета, как международно-правовое основание запрета применение киберсилы.

Ключевые слова: государственный суверенитет, невооруженная сила, применение киберсилы, принцип невмешательства.

Kaminskyi I. The conception of state sovereignty in the context of use of cyberforce

Summary. The paper explores the issues concerning execution by states of their sovereign rights within cyberspace. Recent years has shown vulnerability of all states to the cyber attacks. This put on an agenda the need for establishment of an ability of international law to respond to cyber attacks; within the prism of the concept of non-armed force the Author proposes to qualify such attacks as the use of cyberforce. Firstly, at the present stage of development of international law, a normative prohibition on the use of non-armed cyberforce is not established in Article 2(4) of the UN Charter. Given the nature of realization of non-armed measures by the states, the Author suggests the hypothesis that the international legal prohibition of the latter follows from another basic principle of international law – the principle of the prohibition of intervention in matters which are within the domestic jurisdiction of any state (the principle of non-intervention). Since it is closely linked to the concept of state sovereignty, there is an urgent necessary to establish the existence of sovereign rights in cyberspace. To this effect, the Author investigates the legal nature of cyberspace in order to find out whether it is possible to consider the principle of non-intervention as an international legal ground for the prohibition of the use of cyberforce. As a result, the Author points out that states can not exercise sovereignty over cyberspace as a virtual environment, because it is a legal fiction as an object of legal regulation. At the same time the Author proves that states have sovereign rights over their cyber infrastructure, as well as the responsibility to control this infrastructure and to prevent it from deliberate use in order to harm other states. Such conclusion gives reasons to suggest that state sovereignty refers to cyberspace, so the principle of non-intervention can be explored as a norm prohibiting the use of cyberforce.

Key words: state sovereignty, non-armed force, use of cyberforce, principle of non-intervention.