МУЗИКА ВІКТОРІЯ ВАСИЛІВНА

Національний університет «Одеська юридична академія»,
асистент кафедри міжнародного та європейського права

ДО ПИТАННЯ ПРО ВІДСУТНІСТЬ ПОНЯТТЯ «КРИТИЧНА ІНФРАСТРУКТУРА» В МІЖНАРОДНОМУ ПРАВІ

Швидкий розвиток та вдосконалення інформаційно-комунікаційних технологій змусив міжнародну спільноту задуматись над тим, чи застосовується міжнародне право в кіберпросторі. Як наслідок, все частіше держави в офіційних позиціях демонструють своє розуміння того, як уже існуючі норми міжнародного права можна інтерпретувати та застосувати до конкретних кібероперацій, зокрема кібератак, спрямованих проти об'єктів критичної інфраструктури. Та попри загальну увагу до кібератак проти критичної інфраструктури, держави несвідомо опускають питання щодо того, що вони розуміють під поняттям «критична інфраструктура». Лише Німеччина в своєму *opinio juris* щодо застосування міжнародного права в кіберпросторі від 5 березня 2021 року Німеччина акцентувала увагу на відсутності конвенційного поняття «критична інфраструктура», тому, усвідомлюючи різні підходи держав, поряд з ним використовує таке поняття як «компанії, що представляють особливий суспільний інтерес» [5, с. 4].

Враховуючи те, що конвенційне поняття «критична інфраструктура» чи «об'єкти критичної інфраструктури» в міжнародному праві відсутнє, логічно звернути увагу на підходи держав, в національному законодавстві яких визначається нормативний зміст такого поняття. Так, наприклад, в законодавстві Туреччини національна критична інфраструктура класифікована відповідно до 6 критично важливих секторів, а саме – електронні комунікації, управління водними ресурсами, енергетика, функціонування критично важливих державних служб, транспорт, банки та фінанси [3].

В Бельгії та Сальвадорі критично важливих секторів інфраструктури ще менше – законодавець визначає лише чотири. Національною критичною інфраструктурою в Бельгії вважається сектор енергетики, транспорту, фінансів та електронних комунікацій. В Сальвадорі їх також чотири, але перелік дещо відмінний, а саме – сектори енергетики, транспорту, водних ресурсів та комунікацій [2].

Переходячи до законодавства Індії та Індонезії, можна зауважити, що, серед іншого, критичними для функціонування держав є сектор щодо дослідження та використання космосу та електронний уряд; в той час як в списку об'єктів критичної інфраструктури Норвегії виділяється супутникова інфраструктура [2].

Сполучені Штати Америки виділяють 16 секторів критичної інфраструктури, серед яких, окрім уже традиційних, згадується урядовий сектор, сектор комерційних об'єктів (об'єкти, які приваблюють натовпи

людей для здійснення покупок, ведення бізнесу, розваг чи проживання), сектор гребель (проекти дамб, навігаційні замки, затоки, ураганні бар'єри та інші споруди для утримання води та/або її контролю), сектор промислової бази оборони тощо [6, с. 10–12]. Крім того, зазначається, що в це поняття входять як фізичні, так і віртуальні системи та ресурси, настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів ослабить безпеку, економіку, забезпечення громадського здоров'я тощо [6, с. 12]. З одного боку, такий підхід може здатись досить широким в порівнянні із законодавчими положеннями інших держав, особливо, коли мова йде про сектор розваг. З іншого – для деяких держав (або суб'єктів федерації) сектор розваг дійсно може відігравати критично важливу роль у забезпеченні її життєдіяльності.

Відтак, незважаючи на те, що поняття та перелік об'єктів критичної інфраструктури варіюється, в цілому можна прослідкувати консенсус між державами щодо важливості певних об'єктів інфраструктури. Чітко простежуються сектори критичної інфраструктури, які в національному законодавстві згадуються найчастіше: банки та фінанси; центральний уряд; комунікація / інформаційно-комунікаційні технології (ІКТ); енергетика; медичні послуги; транспорт / логістика / дистрибуція; вода (постачання); їжа; екологічний захист.

Аналіз національного законодавства цих країн також свідчить про різні підходи держав при вирішенні питання, що собою представляє критична інфраструктура та які об'єкти входить в це поняття. Одна група держав включає в це поняття максимальну кількість секторів, які, на їх думку, є критичними та забезпечують функціонування держави, інші – обмежуються згадками про декілька найбільш ключових. Ось і виходить, що в США 16 критичних секторів критичної інфраструктури, у Королівстві Нідерланди 12 секторів та 31 підсекторів, а в Бельгії, Сальвадорі та Аргентині – по чотири сектори.

Вузький підхід останніх також не є цілком виправданим. Так, іноді можливо об'єднати дві групи об'єктів критичної структури в одну, щоб уникнути їх «дроблення», але не завжди є така можливість. Так, наприклад, два відокремлені в національному законодавстві США сектори – систем водопостачання та дамб – можливо об'єднати, але з переліку об'єктів критичної інфраструктури Сальвадору та Бельгії ніяк не можна виокремити військові об'єкти (сектор зовнішньої та внутрішньої безпеки) чи демократичні інститути (урядовий сектор). Одразу виникає два запитання: у випадку атаки на урядові об'єкти цих країн, які забезпечують нормальне функціонування та управління держави, чи буде впливати визначення законодавця на кваліфікацію порушення? Крім того, якщо у випадку з урядовими та оборонними об'єктами можна подискутувати щодо їх «критичної важливості», то підхід бельгійського законодавця, який ігнорує важливість систем водопостачання, видається не досить логічний.

Загалом будь-який закритий список об'єктів критичної інфраструктури – це швидше мінус, ніж плюс, незважаючи на доповнення, які

вносять держави. Причиною цьому є відсутність в міжнародному праві загально прийнятого визначення «критичної інфраструктури» та необхідність звернення до національного законодавства у випадку серйозних порушень норм міжнародного гуманітарного права чи міжнародного права прав людини, а найголовніше – коли потрібно атрибутувати кібератаку та вдатися до реакції на таку атаку.

Цікавим у цьому плані є підхід у Франції, який може бути використаний як спосіб вирішення проблем з цим поняттям. Французький законодавець ставлення до критичної інфраструктури визначає через цілі діяльності певних об'єктів. Так, наприклад, діяльність цих об'єктів має бути пов'язана з виробництвом та розподілом товарів або послуг, необхідних для задоволення основних потреб населення; для виконання державних повноважень або забезпечення функціонування економіки; підтримання обороноздатності або безпеки нації, «оскільки цю діяльність важко замінити; або це може серйозно вплинути на здоров'я чи життя населення». Загалом виділяється 12 секторів, забезпечення нормального функціонування яких належить до відповідальності відповідних міністерств [4, с. 8].

Схожим у цьому плані є і підхід українського законодавця, який зазначає, що такі об'єкти «мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення». Згідно зі статтею 6 Закону України «Про основні засади забезпечення кібербезпеки України», до об'єктів критичної інфраструктури України належать підприємства, установи та організації незалежно від форми власності, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, ІКТ, електронних комунікацій, у банківському та фінансовому секторах; життєзабезпечення населення (централізоване водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, охорони здоров'я; є аварійними та рятувальними службами; мають стратегічне значення для економіки і безпеки держави; є об'єктами потенційно небезпечних технологій і виробництв [1, ст. 6].

Як видається, підхід до поняття «критична інфраструктура» через функції є найбільш доцільним і має право на утвердження в міжнародному праві. Він надасть членам міжнародної спільноти та міжнародним судовим органам гнучкості у випадку кібератаки з кінетичними наслідками, а значить – надасть можливість притягнути нападників, які фінансуються іншими державами, до відповідальності. Крім того, такий підхід допоможе врахувати особливості розвитку та функціонування окремих держав. Наприклад, для малих острівних держав іноді саме сферу туризму дозволяє забезпечувати нормальне функціонування держави та суспільства. Що ж до переліку секторів або об'єктів критичної інфраструктури, то він має залишатись відкритим у світлі постійного розвитку технологій та суспільства. У випадку, якщо новий інструмент з цим поняттям не буде розроблений та прийнятий, практика держав та їх *opinio juris* допоможуть сформулювати підхід до розуміння того, які об'єкти охоплюються поняттям «критична інфраструктура».

Список використаної літератури:

1. Про основні засади забезпечення кібербезпеки України від 24.10.2020, 2163-VIII. *Відомості Верховної Ради*, 2017, № 45. Ст. 403.
2. Critical Infrastructure Sector. *CIPedia*. URL: https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector#cite_note-54
3. Decree No. 2 on the Regulation Amending the Regulation on Military Forbidden Zones and Security Zones, 20-6-2013; 2016–2019 Ulusal Siber Güvenlik Stratejisi. URL: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf
4. Instruction Generale Interministerielle Relative a la securite des activites d'Imprortance vitale N°6600/SGDSN/PSE/PSN du 7 janvier 2014. Direction Protection et Sécurité de l'Etat N° NOR: PRMD1400503J. URL: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf
5. On the Application of International Law in Cyberspace Position Paper. March 2021. *The Federal Government*: https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf
6. The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) (Feb. 12, 2013). URL: https://fas.org/irp/offdocs/ppd/ppd-21.pdf

Ключові слова: критична інфраструктура; *opinio juris*; кібератаки.
Ключевые слова: критическая инфраструктура; *opinio juris*; кибератаки.
Key words: critical infrastructure; *opinio juris*; cyberattacks.

ГРОМЛЮК АЛІНА ВІТАЛІЇВНА

Національний університет «Одеська юридична академія»,
аспірант кафедри міжнародного та європейського права

ПИТАННЯ ЗАХИСТУ ПРАВА ВЛАСНОСТІ В СУЧАСНОМУ МІЖНАРОДНОМУ ПРАВІ

Право власності є одним з фундаментальних прав людини та невід'ємною складовою інституту такої галузі міжнародного публічного права як міжнародне право прав людини.

Варто відзначити, що єдиної думки серед юристів-міжнародників стосовно існування у міжнародному праві свого автономного поняття права власності немає. Одні автори зазначають, що міжнародному праву невідоме визначення даного терміну, інші вважають, що категорія права власності у міжнародному праві має абсолютно автономне значення, яке зазвичай не співпадає з тим, що прийняте у національних правових системах.

Досить довгий час право власності підтримувалось лише на національному рівні та захищалось тільки правовою системою держав,