МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Кваліфікаційна наукова праця
На правах рукопису

МУЗИКА ВІКТОРІЯ ВАСИЛІВНА

УДК 341.1/.8+341.6

ДИСЕРТАЦІЯ

АТРИБУЦІЯ КІБЕРАТАК ПРОТИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВИЗНАЧЕННЯ ОСНОВНИХ ПРОБЛЕМ ТА ШЛЯХІВ ЇХ ВИРІШЕННЯ

Спеціальність – 081 «Право»

Подається на здобуття наукового ступеня **доктора філософії**
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ В.В. Музика

Науковий керівник:
доктор юридичних наук, професор
Бігняк Олександр Валентинович

Одеса – 2021

АНОТАЦІЯ

Музика В. В. **Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення**. – *Кваліфікаційна наукова праця на правах рукопису*.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». Національний університет «Одеська юридична академія», Міністерство освіти і науки України. Одеса, 2021.

Дисертація є першим в українській юридичній науці спеціальним комплексним дослідженням атрибуції кібератак проти об'єктів критичної інфраструктури. У роботі представлено низку авторських ідей та висновків, які характеризуються науковою новизною.

У дисертації розкрито природу кіберпростору, що є середовищем реалізації кібератак та забезпечує необхідними засобами їх здійснення, а також визначено сутнісні характеристики кібератак. На підставі цього встановлено, що кібератаки можуть здійснюватися проти різних рівнів кіберпростору (фізичного, логічного та соціального) з метою порушення функціонування об'єктів критичної інфраструктури.

Встановлено, що передумовою для здійснення атрибуції кібератак є визначення міжнародно-протиправної поведінки, що вимагає атрибуції. Відсутність *lex specialis* значно ускладнює процес атрибуції, тому крім положень Талліннський керівництв, проаналізовано різноманітні форми *opinio juris*, які свідчать про певний рівень розходження в позиціях держав. Водночас *opinio juris* дозволило встановити, які діяння держави розглядають в якості кібератак, що є порушенням норм міжнародного права та вимагають атрибуції.

Доведено, що попри заперечення з боку низки держав, норми *jus in bello* та *jus ad bellum* в повній мірі застосовуються до кібератак і, відтак, впливають на процес здійснення атрибуції кібератак проти об'єктів критичної інфраструктури держави.

З урахуванням відсутності поняття «критична інфраструктура», ідентифіковано, які об’єкти та сектори держави найчастіше розглядаються в якості критично важливих. Обґрунтовано необхідність розробки поняття «критична інфраструктура» на міжнародному рівні, яке б дозволяло зберігати гнучкість і врахувати національні пріоритети окремих держав. В роботі також наголошується на тому, що розробка такого поняття повинна сприяти становленню оптимального підходу до категоризації об’єктів як таких, що є об’єктами критичної інфраструктури. Така потреба випливає із наявних підходів держав, які часто є невиправдано інклюзивними (фактично всі сектори/об’єкти інфраструктури національний законодавець відносить до критично важливих) або занадто вузьким (згадується два-чотири сектори).

Запропоновано виділити в окрему категорію транснаціональні (міждержавні) об’єкти критичної інфраструктури, які використовуються одночасно декількома державами. Така пропозиція робиться в силу їх підвищеної взаємозалежності та ризику настання більш серйозних та масштабних наслідків в результаті успішних кібератак.

В дисертаційному дослідженні визначено, що процес атрибуції кібератак проти об’єктів критичної атрибуції вимагає здійснення технічної, політичної та юридичної атрибуції. Таким чином, атрибуція кібератак не можлива без оцінки технічних та політичних індикаторів. Цей висновок знаходить підтримку в позиціях держав, які висловилися щодо застосування міжнародного права в кіберпросторі, висновках групи експертів Талліннського керівництва 2.0 та Групи урядових експертів щодо заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки.

Логічним завершенням будь-якого процесу атрибуції кібератак проти об’єктів критичної інфраструктури держави має стати юридична атрибуція кібератак, що є елементом міжнародно-протиправного діяння відповідно до статті 2 Статей про відповідальність держав за міжнародно-протиправні діяння 2001 року.

В роботі розкрито теоретичні та практичні аспекти застосування стандартів атрибуції до кібератак проти об'єктів критичної інфраструктури за участі органів держави; фізичних або юридичних осіб, які здійснюють елементи урядових повноважень; або недержавних суб'єктів, які діють під керівництвом або під контролем держави.

Обов'язок проявляти необхідну обачність не є стандартом для атрибуції поведінки державі, проте, враховуючи важливість атрибуції кібератак проти об'єктів критичної інфраструктури, ідея перенесення обов'язку *due diligence* з основних до похідних норм відповідальності держав аналізується та набуває подальшого розвитку в роботі.

В дисертаційному дослідженні вперше здійснено комплексний аналіз кібератак проти систем електроенергетики України у 2015 та 2016 роках в контексті збройного конфлікту на сході України. Обґрунтовано, що кібератаки в контексті збройного конфлікту *prima facie* не є випадковими. В конкретному випадку час, обраний для кібератак, та воєнні дії на сході України свідчать про пряму чи опосередковану участь країни-агресора. Відтак, на прикладі даних кібератак доводиться необхідність здійснення технічної та політичної атрибуції, яка б комплексно враховувала всі наявні індикатори.

В роботі визначено основні практичні кроки для ефективної атрибуції кібератак проти об'єктів критичної інфраструктури. Доведено необхідність здійснення атрибуції в межах державно-приватної співпраці. Оцінено переваги та недоліки можливих моделей взаємодії та визначено найбільш оптимальну, яка б передбачала залучення представників держави, приватного сектору та при потребі інших зацікавлених сторін.

Проаналізовано нову Кіберстратегію ЄС, яка містить інтеграційну модель взаємодії між державними та приватними суб'єктами та вводить інструменти кібердипломатії. Визначено, що інструмент кіберсанкцій, який застосовується на підставі рішення Ради ЄС, є кроком вперед в питанні атрибуції кібератак. Але загалом ефективність індивідуальних кіберсанкцій досить низька. Визначено перспективи використання інструменту кіберсанкцій на універсальному рівні, до

прикладу, в межах ООН. При цьому, для підвищення їх ефективності доречніше замінити індивідуальні санкції на секторальні.

В дисертаційному дослідженні також робиться спроба оцінити перспективи розгляду міждержавного спору щодо атрибуції кібератак проти об’єктів критичної інфраструктури держави в межах Міжнародного Суду ООН. Визначено, що розгляд такого міждержавного спору може вирішити низку теоретичних та практичних проблем, зокрема щодо особливостей застосування звичаєвих норм атрибуції до кібератак.

Ключові слова: критична інфраструктура; об’єкти критичної інфраструктури; атрибуція кібератак; кібернетичні атаки; кібератаки; відповідальність держав.

SUMMARY

Muzyka V. V. **Attribution of cyberattacks against critical infrastructure objects: identification of key problems and ways to solve them**. – *On the rights of the manuscript*.

The dissertation for obtaining the scientific degree of the Doctor of Philosophy in a specialty 081 “Law”. National University “Odesa Law Academy”, The Ministry of Education and Science of Ukraine. Odesa, 2021.

The dissertation is the first in the Ukrainian legal science special complex research on attribution of cyberattacks against objects of critical infrastructure. This work presents a number of author`s ideas and conclusions, which do have scientific novelty.

This dissertation characterizes the nature of cyberspace, which is the environment for the commission of cyberattacks. It also identifies the essential characteristics of cyberattacks. Based on the above mentioned, it has been established that cyberattacks can be carried out against different layers of cyberspace (physical, logical and social) in order to disrupt critical infrastructure.

It was found out that defining internationally wrongful behavior in cyberspace is the prerequisite for the attribution of cyberattacks. The lack of legally binding *lex specialis* significantly complicates this task, so in addition to the provisions of the Tallinn Manual 2.0, various forms of *opinio juris* were analyzed. In conjunction, they indicate a lack of consensus between states in respect to certain issues. At the same time, *opinio juris* has greatly helped to determine which acts of states are regarded cyberattacks that violate International Law and require attribution.

It has been shown that, despite objections from a number of states, the norms of *jus in bello* and *jus ad bellum* are fully applicable to cyberattacks and thus have an impact on the attribution of cyberattacks against critical infrastructure of states.

The dissertation identifies what objects and sectors of states fall within the scope of critical infrastructure concept. It insists on the need to develop such a concept of critical infrastructure at the international level that would maintain flexibility and take into account national priorities.

It is proposed to include transnational (inter-state) critical infrastructure objects in a separate category due to the use of such objects by several states. This proposal is made because of their increased interdependence and the high risk of more serious and far-reaching consequences in the context of international security.

In the dissertation, it is also found out that the process of cyberattacks attribution on critical infrastructure requires technical, political, and legal attribution. Thus, the attribution of cyberattacks is not possible without the assessment of technical and political indicators. This conclusion is supported by the position of states on the application of International Law in cyberspace, the conclusions of the Expert Group of the Tallinn Manual 2.0 and the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security.

Legal attribution of cyberattacks, which is an element of international wrongful acts of a state under Article 2 of the 2001 Articles on State Responsibility for Internationally Wrongful Acts, should be a final step in the process of attribution of cyberattacks against critical infrastructure of states.

The dissertation reveals the theoretical and practical aspects of the application of norms on attribution to cyberattacks against critical infrastructure in case they are carried out by organs of a state; persons or entities exercising elements of governmental authority; or a person or group of persons operating under the direction or control of the state.

The obligation to exercise *due diligence* is not a standard for attributing behavior to a state. However, in light of the importance of attribution of cyberattacks against objects of critical infrastructure, the idea of treating *due diligence* as a secondary rule, not as a primary one, has being analyzed and further developed.

The dissertation research for the first time in the Ukrainian legal science provides a comprehensive analysis of cyberattacks against Ukraine`s electric grids systems in 2015 and 2016 in the context of the armed conflict in eastern Ukraine. The example of Ukraine proves the need to assess both technical and political indicators during the process of attribution of cyberattacks, in particular in the context of armed conflict.

It is argued that cyberattacks in the context of armed conflict are not *prima facie* accidental. In this particular case, the time chosen for cyberattacks and hostilities in eastern Ukraine indicate the direct or indirect involvement of the Russian Federation. Therefore, the need for technical and political attribution, which would comprehensively take into account all available indicators, is substantiated on the example of these cyberattacks.

The work identifies the main practical steps for the effective attribution of cyberattacks against critical infrastructure. The necessity of attribution within the framework of public-private cooperation is proved. The advantages and disadvantages of possible models of interaction had been assessed and the most optimal one was identified, which foresees the involvement of state agents and private sector representatives.

The 2020 EU Cybersecurity Strategy, which contains a model of interaction between public and private entities on the basis of the European shield and introduces cyber diplomacy toolbox, has been analyzed. Based on that, it was determined that the cyber sanctions instrument imposed by the Council of the EU is a step toward legal attribution. However, the effectiveness of individual cyber sanctions is quite low. Prospects for the use of cyber sanctions at the universal level have been also identified, for example, within the United Nations. At the same time, to increase their effectiveness, it is more appropriate to use sectoral sanctions instead of individual ones.

The dissertation also attempts to assess the prospects of an interstate dispute concerning the attribution of cyberattacks on critical infrastructure within the framework of the UN International Court of Justice. It is concluded that the legal consideration of such an interstate dispute can solve a number of theoretical and practical problems regarding the application of customary norms on attribution to cyberattacks and its peculiarities.

Key words: critical infrastructure; objects of critical infrastructure; attribution of cyberattacks; cyberattacks; cybernetic attacks; responsibility of states.

Список публікацій здобувача:

Статті у фахових наукових виданнях категорії «Б»:

1. Музика В.В. Проблема атрибуції кібератак проти об'єктів критичної інфраструктури та шляхи її вирішення в міжнародному праві. *Юридичний вісник*. № 4. 2020. С. 164-171. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/1985/2080.
2. Muzyka V. Analysis of cyber-attacks on Ukrainian power grid systems in the context of armed conflict in Donbas. *Constitutional State*. № 39. 2020. С. 78-85. URL: http://pd.onu.edu.ua/article/view/212983/214967.
3. Muzyka V. New wine in old bottles: applicability of the rules on attribution to cyberattacks committed against objects of critical infrastructure. *Law Review of Kyiv University of Law*. № 3. 2020. С. 388-391. URL: https://chasprava.com.ua/index.php/journal/article/view/419/400.

Стаття в періодичному науковому виданні держави, що входить до Організації економічного співробітництва та розвитку та/або Європейського Союзу:

4. Музика В.В. Кібератаки та міжнародне право: природа та аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі : колект. моногр. «Проблеми публічного та приватного права» / за заг. ред. Н. В. Мішиної. 2021. С. 309-342.

Розділ колективної монографії:

5. Музика В.В. Політика ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки. *Evropský politický a právní diskurz*. 2021. Том 8 (1). С. 46-51. URL: https://eppd13.cz/wp-content/uploads/2021/2021-8-1/9.pdf.

Публікації, які засвідчують апробацію матеріалів дослідження:

6. Музика В.В. До питання про відсутність поняття «критична інфраструктура» в міжнародному праві. Матеріали міжнародної конференції : Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (21 травня 2021 року). Одеса, 2021. С. 359-362.
7. Музика В.В. Відповідальність держав за порушення обов'язку належної обачності (*due diligence*) в кіберпросторі. Право і суспільство: актуальні питання і перспективи розвитку : Матеріали V Міжнародної науково-практичної конференції Частина I (10 грудня 2020 року). Полтава, 2020. С. 107-110.
8. Muzyka V. Attribution of cyberattacks committed through cyber infrastructure of a third state and due diligence obligation. Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe : International Scientific Conference. Baltija Publishing. (20 November 2020). Riga, Latvia. 2020. P. 111-114.
9. Muzyka V. Human dimension of cyberoperations. Права людини – пріоритет сучасної держави : збір. матер. наук.-прак. конф. (м. Одеса, 10 грудня 2020 р.). Херсон : Видавничий дім «Гельветика», 2020. С. 179-182.
10. Muzyka Viktoriia V. Cyber-attacks attribution and EU collective cyber sanctions as a way to respond to cyber threats from outside the Union. Правова система України в умовах новітніх викликів міжнародного порядку : матеріали науково-практичної заочної конференції (м. Одеса, 20 травня 2020 р.) / за ред. М. Р. Аракеляна. Херсон : Видавничий дім «Гельветика», 2020. С. 63-65.
11. Muzyka Viktoriia V. Public Attribution of Cyber-Attacks: Toward a New Approach in International Law. Правове життя сучасної України : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Видавничий дім «Гельветика», 2020. Т. 3. С. 46-49.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АТО	Антитерористична операція
ГУ/ГРУ	Головного управління/Головне розвідувальне управління Генерального штабу Збройних Сил РФ
ГУЕ	Група урядових експертів ООН
ЄС	Європейський Союз
ЄСПЛ	Європейський суд з прав людини
ІКТ	інформаційно-комунікаційні технології
МАГАТЕ	Міжнародне агентство з атомної енергії
МАСПЛ	Міжамериканський суд з прав людини
МГП	міжнародне гуманітарне право
МІСД	Міжнародний інститут стратегічних досліджень
МКЧХ	Міжнародний Комітет Червоного Хреста
МСЕ	Міжнародний союз електрозв’язку
НАТО	Організація Північноатлантичного договору
НЦКБ	Національний центр кібербезпеки
ОАД	Організація американських держав
ОБСЄ	Організація безпеки та співробітництва в Європі
ООН	Організація об’єднаних націй
п.	пункт/параграф
прим.	примітка
РСЗВ	Реактивна система залпового вогню
с./С.	сторінка
СММ	спеціальна моніторингова місія
ФБР	Федеральне бюро розслідувань США
IP	Інтернет протокол
DDOS-атаки	розподілена атака на відмову в обслуговані
inter alia	серед іншого
SCADA	диспетчерське управління і збір даних

ВСТУП

Обґрунтування вибору теми дослідження. Об’єкти критичної інфраструктури та їх захист знаходяться в повістці багатьох держав світу з початку двадцять першого століття. Теракт 11 вересня 2001 року в Сполучених Штатах Америки та теракти 2004 і 2005 років на території країн-членів Європейського Союзу стали переломним моментом в усвідомленні важливості критичної інфраструктури, від нормального функціонування якої залежить безпека та добробут держави і людей. Але якщо на початку 2000-х років до атак проти об’єктів критичної інфраструктури вдавалися недержавні актори задля залякування населення, то поява і активне використання можливостей кіберпростору відкрили нові можливості для держав, зокрема, можливість переслідувати свої геополітичні інтереси в кіберпросторі.

Кібератаки на американську греблю у 2013 році, німецький металургійний комбінат у 2014 році, українські системи електропостачання у 2015 та 2016 роках, Національну службу охорони здоров’я у Великобританії у 2017 році, системи приладів безпеки Саудівської Аравії в 2017 році, систему електропостачання в Південній Африці, індійський атомний завод у 2019 році та найбільшу трубопровідну систему США у 2021 році – лише незначний перелік кібератак проти об’єктів критичної інфраструктури. І, як видається, це лише початок. Адже середовище толерування та нормалізація кібератак, що є наслідками відсутності юридичної атрибуції кібератак, сприяють зростанню їх кількості.

Більш того, з урахуванням постійного розвитку штучного інтелекту в недалекому майбутньому можна очікувати на масштабні та серйозні гуманітарні наслідки кібератак. Існує також висока вірогідність терористичних кібератак, серед пріоритетних об’єктів яких виділяють об’єкти атомної енергетики, авіа- та залізничної інфраструктури, системи водопостачання, небезпечні біологічні та хімічні об’єкти. У зв’язку з цим, держави не тільки повинні не вдаватися до кібератак, а також докладати всіх зусиль, щоб їх кіберінфраструктура не використовувалася такими акторами з метою завдання шкоди об’єктам

критичної інфраструктури третіх держав. Відтак, актуалізується необхідність здійснення атрибуції кібератак, оскільки встановлення джерела кібератак, сприятиме більш відповідальній поведінці держав в кіберпросторі.

Особливу актуальність даному дослідженню додає той факт, що наразі атрибуція кібератак в розумінні Статей про відповідальність держав за міжнародно-протиправні діяння 2001 року не здійснювалася. Зумовлено це тим, що атрибуція кібератак створює ряд викликів і виходить за межі традиційної концепції атрибуції в силу особливостей кіберпростору. Так, наприклад, в кіберконтексті атрибуція кібератак часто ускладняється використанням проксі, відсутністю у постраждалої держави людських та технічних ресурсів, необхідних для здійснення атрибуції, а також відсутністю розуміння того, як звичаєві норми щодо атрибуції застосовуються в кіберконтексті та чи існуюче міжнародно-правове регулювання є достатнім. Тому, в роботі здійснюється спроба визначити основні шляхи подолання проблем, пов'язаних з атрибуцією кібератак проти об'єктів критичної інфраструктури держави, зокрема, шляхом створення спеціального механізму з атрибуції кібератак. Втім, попри свою орієнтованість на здійснення юридичної атрибуції, дане дисертаційне дослідження комплексно підходить до атрибуції кібератак, що може мати як юридичний, так і технічний та політичний характер. В повній мірі враховується практика здійснення публічної атрибуції, що лише в незначній мірі стримує зростання кібератак.

Важливо, щоб вже зараз кібератаки проти об'єктів критичної інфраструктури, за якими стоїть держава, їй атрибутуватись, незалежно від того, здійснювалися вони державними агентами, під керівництвом або контролем держави чи недержавними акторами, які використовують кіберінфраструктуру держави, що не проявляє необхідної обачності. Водночас для вирішення проблеми атрибуції потрібно сформувати єдиний підхід до поняття «критична інфраструктура». Адже наразі в міжнародному праві відсутнє конвенційне визначення поняття «критична інфраструктура» та критерії ідентифікації об'єктів, що охоплюються цим поняттям. Відсутня також ясність щодо того, як

потрібно здійснювати атрибуцію кібератак проти об'єктів критичної інфраструктури і розуміння необхідності відходу від децентралізованого процесу атрибуції, що також зумовлено природою та особливостями кіберпростору.

Наявні у міжнародній та національній доктрині дослідження здебільшого стосуються питань атрибуції кібератак в загальному та практики їх публічної атрибуції. Проте відсутність комплексного дослідження, яке б аналізувало підходи держав до розуміння того, як існуючі норми міжнародного права застосовуються до кібератак проти об'єктів критичної інфраструктури, а також виробленої позиції щодо поняття критична інфраструктура та можливих шляхів вирішення проблемних аспектів, пов'язаних з атрибуцією, зумовлює потребу дослідження обраної тематики. Нарешті, кібератаки проти систем електропостачання України у 2015 та 2016 роках в контексті збройного конфлікту на сході України актуалізують необхідність дослідження атрибуції кібератак для захисту інтересів України і перенесення їх в юридичну площину. В сукупності все вище зазначене визначає актуальність даного дисертаційного дослідження.

Теоретичну основу дослідження становлять наукові положення, які містяться в роботах таких вчених, як К. Айхенсен, Д. Альперовіч, С.С. Андрейченко, Дж. Буттігідж, Д. Вагнер, Дж. К. Вольтаг, Н. В. Галлагхер, А. Гавріловіч, Л. Гісел, М. В. Грушко, К. В. Дам, Д. Джонсон, Е. Корзак, С. Лін, С. Калтагіроне, Н. Карнієвіч, Д. Кларк, О. Климчук, С. І. Кондратов, Дж. Кроуфорд, А. Кляйнер, Е. Луїджф, К. Мачак, П. Мейер, Г. Навін, Ф. Німанн, В. А. Овенс, Д. Пост, М. Сасолі, Р. Сетола, Б. Сміт, Дж. Ставрідіс, О. О. Сурілова, А. Расселл, Ш. Розен, Т. Роденхойсер, М. Росіні, М. Теохаруду, Н. Томпсон, Р. Хенг, Т. Хітченс, Н. Цагоріас, С. Чарней, Б. Швайцер, М. Шмідт, Р. Шондорф та інших.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано в рамках наукових досліджень Національного університету «Одеська юридична академія» «Стратегія

інтеграційного розвитку України: правовий і культурний вимір» на 2016-2020 роки (державний реєстраційний номер 0116U001842), а також плану науково-дослідницької роботи кафедри міжнародного та європейського права Національного університету «Одеська юридична академія» в межах теми «Міжнародне право в період трансформації міжнародного правопорядку та захист національних інтересів України» на 2016-2020 рр.

Мета і завдання дослідження. Мета дисертації полягає в дослідженні проблематики атрибуції кібератак проти об'єктів критичної інфраструктури з ціллю встановлення основних проблем і можливих шляхів їх вирішення. Для досягнення цієї мети, на виконання було поставлено такі завдання:

– визначити природу та сутнісні ознаки кібернетичних атак, а також їх співвідношення з суміжними поняттями;

– встановити які норми міжнародного права та як можуть бути порушені в кіберпросторі і, відповідно, вимагають атрибуції в межах інституту відповідальності держав;

– прослідкувати та проаналізувати практику та *opinio juris* держав щодо ключових питань застосування міжнародного права до кібератак та їх атрибуції;

– визначити які об'єкти, відповідно до офіційної позиції держав, входять в поняття «критична інфраструктура»;

– охарактеризувати особливості застосування звичаєвих правил атрибуції міжнародно-протиправних діянь до кібератак;

– дослідити питання атрибуції кібернетичних атак у випадку порушення обов'язку необхідної обачності (*due diligence*);

– встановити відмінності між політичною, технічною та юридичною атрибуціями кібератак, а також визначити необхідність їх інтегрального здійснення;

– проаналізувати кібератаки проти об’єктів критичної інфраструктури України в контексті збройного конфлікту на сході України та практичні аспекти їх атрибуції;

– визначити специфіку публічної атрибуції кібератак в Європейському Союзі, що здійснюється через інструмент кіберсанкцій, а також можливість застосування практики ЄС на універсальному рівні;

– оцінити перспективи розгляду міждержавної скарги щодо кібератак проти об’єктів критичної інфраструктури з ціллю заповнення прогалин у досліджуваній проблематиці.

Об’єкт дослідження – міжнародні правовідносини, пов’язані зі встановленням відповідальності держав за кібернетичні атаки проти об’єктів критичної інфраструктури держави, що становлять міжнародно-протиправне діяння.

Предмет дослідження: атрибуція кібератак проти об’єктів критичної інфраструктури, ідентифікація основних проблем при здійсненні такої атрибуції і шляхів їх вирішення.

Методи дослідження. Герменевтичний метод є ключовим при здійсненні дисертаційного дослідження. Цей метод допоміг здійснити інтерпретацію юридичних та технічних текстів для встановлення розуміння та осягнення понять, категорій та процесів, що є центральними при дослідженні питання атрибуції кібератак проти об’єктів критичної інфраструктури (підрозділи 1.1., 1.2., 2.1, 2.2., 2.3.). Порівняльно-правовий метод використано для здійснення компаративних досліджень підходів держав до застосування міжнародного права в кіберпросторі, встановлення розуміння та змісту поняття критична інфраструктура та визначення об’єктів, які, на думку держав, входять в дане поняття (підрозділ 2.1.). Задля досягнення поставлених завдань були також використані прийоми аналізу, синтезу, індукції, дедукції тощо.

В першому розділі чітко простежується використання аксіологічного, цивілізаційного та антропологічного підходів. Аксіологічний підхід допоміг розкрити цінність атрибуції як одного із елементів міжнародно-протиправного

діяння, необхідного для встановлення відповідальності держави, а також цінність існуючих норм міжнародного права, порушення яких в кіберпросторі сприймається членами міжнародної спільноти як таке, що потребує подальшої атрибуції для цілей відповідальності держав та встановлення справедливості (підрозділ 1.2, 1.3). Використання цивілізаційного та антропологічного підходів дозволило розглядати процес атрибуції як міжцивілізаційну та загальнолюдську цінність (підрозділ 1.2., 2.2., 2.3., 3.1., 3.2.).

В другому розділі історико-правовий підхід допоміг простежити виникнення та еволюцію такого поняття як критична інфраструктура та визначення його нормативного змісту (підрозділ 2.1). Цивілізаційний підхід на основі лінійно-стадіальної моделі допоміг підкресли перехід від менш прогресивної до більш прогресивної атрибуції – від атрибуції міжнародно-протиправних діянь, що вчиняються в межах традиційних просторів (кінетичного світу) до атрибуції міжнародно-протиправних діянь, що пов’язанні з віртуальним простором, а саме – кіберпростором (підрозділ 2.2, 2.3.,2.4).

Основним підходом, що є наріжним каменем третього розділу є прогностичний метод, який сприяв встановленню перспектив щодо можливого вирішення практичних проблем атрибуції кібератак (підрозділи 3.1., 3.2., 3.3.).

Наукова новизна одержаних результатів. Дисертація є першим дослідженням комплексного характеру, що розкриває теоретичні та практичні аспекти процесу атрибуції кібернетичних атак проти об’єктів критичної інфраструктури, окреслює основні проблеми та шляхи їх вирішення. У дисертації виконано наступне:

вперше:

– комплексно досліджено атрибуцію кібератак, яка загалом вимагає здійснення технічної, політичної та юридичної атрибуції як нероздільної тріади при встановленні відповідальності держави за міжнародно-протиправні діяння держав в кіберпросторі;

– здійснено аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі, визначено спільне та відмінне у існуючих

підходах та баченні перспектив міжнародно-правового регулювання кібернетичних атак та їх атрибуції;

– встановлено зміст поняття «критична інфраструктура» і визначено сектори (сукупність об’єктів критичної інфраструктури), які, на думку, більшості держав входять в дане поняття;

– запропоновано виділити об’єкти критичної інфраструктури, які використовуються спільно декількома державами в окрему категорію – транснаціональні (міждержавні) об’єкти критичної інфраструктури в силу спільного інтересу держав в забезпеченні їх кіберстійкості та залежності від їх функціонування;

– здійснено атрибуцію кібератак проти систем електропостачання України в контексті збройного конфлікту на Донбасі з урахуванням наявних технічних та політичних індикаторів, що підтверджує необхідність врахування загального контексту, мотивації, використаних ресурсів та інших релевантних факторів;

– встановлено перспективи подолання практичних проблем атрибуції кібератак на прикладі інтегральної моделі взаємодії в Європейському Союзі: державно-приватної співпраці та застосування інструментарію кібердипломатії на універсальному рівні;

– проаналізовано перспективи розгляду міждержавного спору щодо відповідальності за кібератаки проти об’єктів критичної інфраструктури держави як варіант подолання проблем атрибуції на практиці.

удосконалено:

– розуміння застосування звичаєвих норм атрибуції до кібератак, що здійснюються проти об’єктів критичної інфраструктури держави;

– ідеї розвитку здійснення централізованої та децентралізованої атрибуції кібернетичних кібератак проти об’єктів критичної інфраструктури з урахуванням наявних політичних та технічних індикаторів;

– наукові ідеї щодо створення спеціального механізму, який би здійснював технічну та політичну атрибуцію кібератак з метою уникнення

помилкової атрибуції та вирішення проблеми обмежених людських та технічних ресурсів постраждалих держав;

– розуміння процесу політичної атрибуції кібератак, яке ґрунтується на оцінці мотивації, стратегічних інтересів, технічних показників, рівня близькості між державними та недержавними акторами, географічної локації та інших важливих індикаторів.

***набули подальшого розвитку*:**

– положення щодо атрибуції кібератак, об'єктом яких є критична інфраструктура держави;

– наукові ідеї щодо застосування міжнародного права до кібератак, зокрема звичаєвих норм атрибуції поведінки державі, що містяться в Статтях про відповідальність держав за міжнародно-протиправні діяння 2001 року;

– ідеї перенесення обов'язку проявляти необхідну турботу (*due diligence),* який не є стандартом для атрибуції поведінки державі, з основних до похідних норм відповідальності держав, враховуючи важливість атрибуції кібератак проти об'єктів критичної інфраструктури

– обґрунтування необхідності врахування технічних та політичних індикаторів при здійсненні атрибуції кібератак, що часто є взамокомпенсуючими та у своїй сукупності дозволяють звести до мінімуму помилку у встановленні джерела кібератаки;

– необхідність співпраці між державою та приватним сектором для обміну інформацією щодо існуючих вразливостей та кращих практик технічної атрибуції кібератак;

– теоретично обґрунтовано потребу розробки та прийняття юридично обов'язкового міжнародного інструменту, який безпосередньо би стосувався атрибуції кібератак проти об'єктів критичної інфраструктури, включав відповідні поняття та встановлював права та зобов'язання у випадку того, коли кібернетичні атаки кваліфікуються як «застосування сили» чи «збройна атака».

Практичне значення одержаних результатів полягає у тому, що сформовані в дисертації висновки, пропозиції та рекомендації можуть бути використані у:

науково-дослідній сфері – з метою подальшого розвитку доктринальних досліджень щодо відповідальності держав за міжнародно-протиправні діяння, пов'язані із кіберпростором, а також щодо атрибуції кібератак проти об'єктів критичної інфраструктури держав;

нормотворчій діяльності – в процесі підготовки та удосконалення законодавчих та підзаконних актів, що стосуються захисту та забезпечення стійкості критичної інфраструктури від кібернетичних атак та взаємодії з приватним сектором (обмін інформацією щодо вразливостей та процесу атрибуції кібератак);

правозастосовній діяльності – для забезпечення єдиного підходу до застосування звичаєвих норм щодо атрибуції міжнародно-правових діянь до кібератак проти об'єктів критичної інфраструктури;

науково-методичній роботі – при підготовці навчальних посібників та підручників з міжнародного права, при читанні курсів міжнародного права, розробці спецкурсів, що пов'язані з питаннями відповідальності держав та забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки;

навчальному процесі – при вивченні дисциплін «Міжнародне право», «Відповідальність в міжнародному праві», «Міжнародне гуманітарне право», «Міжнародне право безпеки»;

правовиховній – для підвищення рівня правової культури населення, формування правосвідомості здобувачів закладів вищої освіти.

Особистий внесок здобувача в одержання наукових результатів. Дисертаційне дослідження виконано дисертантом самостійно. Щодо використаних автором джерел, у роботі містяться відповідні посилання.

Апробація результатів дослідження. Дисертацію обговорено та виконано на кафедрі міжнародного та європейського права Національного університету «Одеська юридична академія».

Результати дисертаційного дослідження доповідалися на очних та заочних науково-практичних конференціях і семінарах, а саме: «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру» (м. Одеса, 21 травня 2021 року); «Право і суспільство: актуальні питання і перспективи розвитку» (м. Полтава, 10 грудня 2020 року); «Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe» (м. Рига, Латвія, 20 листопада 2020 року); «Права людини – пріоритет сучасної держави» (м. Одеса, 10 грудня 2020 р.); «Правова система України в умовах новітніх викликів міжнародного порядку» (м. Одеса, 20 травня 2020 р.); «Правове життя сучасної України» (м. Одеса, 15 травня 2020 р.).

У процесі здійснення дослідження здобувачка брала участь у фахових обговореннях, круглих столах, семінарах присвячених сучасним проблемам міжнародного права. Зокрема, 4-9 вересня 2019 року дисертантка взяла участь у 42-му Круглому столі з актуальних проблем МГП, присвяченому 70-літтю прийняття Женевських Конвенцій «Whither the human in armed conflict? IHL implications of new technology in warfare» (Сан Ремо, Італія). 26 червня 2020 року долучилась до міжкафедрального семінару, в якому брали участь здобувачі та науковців кафедри міжнародного та європейського права. 23 червня 2021 року результати дослідження представленні в ході семінару, присвяченого актуальним питанням міжнародного права, в рамках модулю Жана Моне, що проходив на базі Національного університету «Одеська юридична академія».

Публікації. Основні наукові результати дисертації висвітлено в одній статті періодичного наукового виданнях Чеської Республіки, що входить до Організації економічного співробітництва та розвитку і Європейського Союзу, трьох наукових публікаціях в наукових виданнях, включених до переліку наукових фахових видань України категорії «Б» та одному розділі колективної

монографії. В сукупності дані публікації розкривають основний зміст дисертації.

Структура та обсяг дисертації. Дисертація складається із анотації, вступу, 3 розділів, які містять 11 підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 219 сторінок, у тому числі основного тексту – 167 сторінок. Список використаних джерел налічує 251 найменування і розташований на 28 сторінках.

РОЗДІЛ 1.
КІБЕРАТАКИ ЯК МІЖНАРОДНО-ПРОТИПРАВНІ ДІЯННЯ В КІБЕРПРОСТОРІ: ВИЗНАЧЕННЯ ПОВЕДІНКИ, ЩО ВИМАГАЄ АТРИБУЦІЇ

1.1. Природа та сутнісні характеристики кібератак

Стрімкий розвиток інформаційно-комунікаційних технологій створив ряд можливостей для міжнародної спільноти в цілому та для окремих держав загалом. Такий розвиток ІКТ сприяв тому, що паралельно звичним для людства просторам – суша, повітряний, морський та космічний простори, виникає ще один – кіберпростір, який фактично є віртуальним інформаційно-комунікаційним простором.

Станом на жовтень 2021 року близько 4,88 мільярдів осіб постійно користуються можливостями Інтернету, що становить більш ніж 62% населення Землі [102]. Водночас потрібно усвідомлювати те, що кіберпростір – це щось значно більше, ніж просто Інтернет. Він є досить комплексним, динамічним, всеохоплюючим та повсюдним робочим середовищем, яке включає, серед іншого, системи управління авіапольотами, медичні системи життєзабезпечення, фізичні контролери пристроїв та національні системи розподілу електроенергії [228].

Зважаючи на те, що використання кіберпростору значною частиною людей здійснюється з ціллю встановлення та реалізації політичних, економічних та соціальних зв’язків (участь в прийнятті політичних рішень, доступ до публічних послуг, комунікація тощо), можна з впевненістю стверджувати, що кіберпростір став невід’ємною та важливою частиною життя у XXI столітті. Тому, на думку низки вчених, кіберпростір охоплюється концепцією «спільна спадщина людства», а доступ до тих можливостей та переваг, які він надає, захищається на міжнародному та національному рівнях [59, с. 89-90].

Саме кіберпростору ми завдячуємо виникненню нетрадиційних для людства атак – кібератак, адже він є середовищем для їх реалізації та

«забезпечує» необхідними засобами здійснення – технічними можливостями кіберпростору [42, с. 341]. На відміну від «фізичного» світу з його «кінетичними» атаками, кіберпростір та здійснювані в межах нього кібератаки характеризуються рядом особливостей. Згідно з Талліннським керівництвом 2.0, що представляє собою найбільш авторитетне доктринальне дослідження щодо застосування міжнародного права до кібероперацій, кіберпростір – це «середовище, утворене фізичними та нефізичними компонентами для зберігання, модифікації та обміну даними за допомогою комп'ютерних мереж» [209, с. 564].

Схоже розуміння цього поняття міститься в статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, де зазначається, що під кіберпростором варто розуміти «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [29].

Аналіз вищезгаданих понять підводить до того, що кіберпростір – це не лише віртуальне середовище. Він складається з трьох різних рівнів (пластів) – фізичного, логічного та соціального [209, с. 12], – в межах яких або проти яких можна здійснювати кібератаки. Важливо, що у будь-який момент «функціонально релевантні компоненти кожного пласту знаходяться десь на земній кулі, як правило, на суверенній території або підконтрольній принаймні одній державі» [72, p. 9], що є принципово важливим для здійснення атрибуції.

Як влучно зазначив Уряд Німеччини в своїй заяві щодо застосування міжнародного права в кіберпросторів, «кіберпростір не є детеріторізованим простором… не існує незалежних «кіберкордонів», які не узгоджуються з фізичними кордонами держави, обмежуючи або нехтуючи територіальною сферою охоплення суверенітету» [230, с. 3]. Відтак, усвідомлення цих рівнів забезпечує розумінням того, що кібератаки здійснюються проти різних

компонентів фізичного, логічного та соціального рівнів кіберпростору, які майже завжди знаходяться в межах території держав.

Фізичний рівень кіберпростору складається з фізичних компонентів мережі, а також географічної складової. Фізичні компоненти мережі включають всі елементи – від оптоволоконних кабелів до стільникових вишок, комп'ютерів та серверів, що необхідні для зберігання, обробки та передачі інформації в кіберпросторі. Знаходження цих елементів у фізичному просторі є відправною точкою для встановлення географічного розташування, а отже, – становить географічну складову фізичного пласту кіберпростору [209, с. 9; 72, с. 9].

Логічний рівень кіберпростору можна розглядати в якості центральної нервової системи кіберпростору. Цей рівень відповідає за маршрутизацію пакетів даних до їх кінцевих пунктів призначення [202, с. 40-41]. Він є абстрактним та стосується систем доменних імен, Інтернет-протоколів, браузерів, програмного забезпечення, через які передаються дані, та покладається на згадані вище компоненти фізичного рівня.

Нарешті, соціальний рівень охоплює всіх акторів, що беруть участь у кібератівності. Іноді його ще називають компонентом «кіберперсона», оскільки він охоплює процес ідентифікації особи або персони в мережі (електронна адреса, IP-адреса комп'ютера, номер мобільного телефону та інші) [126, с. 121]. При цьому, індивід може мати декілька кіберперсон (наприклад, за рахунок наявності декількох облікових записів на різних комп'ютерах), а одна кіберперсона може використовуватися декількома користувачами (особами).

У Талліннському керівництві 2.0 підкреслюється, що «фізичний, логічний та соціальний рівні кіберпростору підпадають під сферу охоплення принципу суверенітету» [209, с. 12]. Водночас кіберпростір *per se* – це глобальний вимір, позбавлений фізичних кордонів, який фактично має транснаціональний характер. Він доступний для всіх і кожного, що робить його системи тісно взаємопов'язаними і часто призводить до кваліфікації таких систем в якості систем подвійного використання. Відтак, для того, щоб, наприклад, нападнику обірвати військовий зв'язок в ході збройного конфлікту, швидше за все,

прийдеться зруйнувати всю мережу, яка використовується не лише комбатантами, а й цивільними. Такий тісний взаємозв'язок вже зараз змушує задуматись над тим, як гарантувати відповідальне використання кіберпростору в мирний та воєнний час, враховуючи високу залежність від об'єктів критичної інфраструктури.

Зважаючи на природу кібероперацій і можливість їх легко «замаскувати», кіберпростір надає можливість зберегти анонімність і передбачає складний процес атрибуції для встановлення кола осіб, причетних до кібероперацій. А вторинні чи навіть третинні наслідки кібератак часто є більш значимими, ніж їх первинні наслідки, що значно вирізняє кібератаки на фоні звичайних атак [204, с. 534]. Всі ці особливості створюють серйозний виклик для міжнародного права, якому потрібно швидко адаптуватись до розвитку технологій, що, як правило, випереджають право на один крок, а кодифікацію його норм – принаймні на два.

В доктрині є багато визначень того, що входить в поняття кібератака. Більшість вчених сходяться на тому, що кібератака – це діяльність, яка спрямована на використання, спотворення, підміну або знищення інформації в комп'ютерній мережі або пов'язаній системі [15, с. 29]. З позиції міжнародно-правової доктрини, на особливу увагу заслуговує визначення, надане експертами Талліннського керівництва. Згідно з ним, кібератака – «це кібероперація, наступальна або оборонна, що цілком очікувано може призвести до завдання трав чи смерті осіб або шкоди чи знищення об'єктів» [209, ст. 92]. До прикладу, кібератаки включають маніпуляції чи знищення даних або коду в комп'ютерній системі для управління або відключення електромережі, з метою обривання (чи іншого порушення функціонування) військового зв'язку або для послаблення надійності банківських даних.

Необхідно також розмежовувати поняття «кібератака» та поняття «кіберексплуатація», що за своєю природою також є кібероперацією. Фундаментальна відмінність полягає в тому, що вони призводять до різних юридичних та політичних наслідків. Випадки кіберексплуатації, хоч і мають вплив на міжнародні відносини між державами, але, як правило, підпадають під

виключну сферу регулювання національного права, в той час як до більшості кібератак застосовується міжнародне право. Крім того, кіберексплуатація є актом спостереження (моніторингу) та пов'язаного з ним шпигунства за комп'ютерними системами, а також копіювання (і відтак, це фактично крадіжка) даних у цих системах. Приклади кіберексплуатації включають викрадення військових таємниць, об'єктів інтелектуальної власності, номерів кредитних карток тощо [182, с. 9-12, 32].

На відміну від кібератак, кіберексплуатація не спрямована на порушення звичного функціонування комп'ютера або мережі і не становить порушення міжнародного права, оскільки останнє не містить заборони щодо шпигунства в мирний час. Така заборона фактично міститься лише в статі 46 Додаткового Протоколу І до Женевських Конвенція 1949 року та діє лише у воєнний час [7, ст. 49].

В центрі цього дослідження знаходяться кібератаки, що передбачають втручання та мають потенціал до завдання кінетичних наслідків, тому їм приділятиметься майже вся увага. Проте важливо розуміти, що на практиці кіберексплуатація досить часто передує здійсненню кібератаки, оскільки успішна кібератака залежить від ефективного спостереження за комп'ютерними системами та виявлення існуючих вразливостей таких систем. Як уже зазначалося, середовищем реалізації кібератак є кіберпростір, а засобами здійснення – технічні можливості кібернетичного простору, зокрема розробка або пошук вразливостей систем управління (активів) [42, с. 341]. Тому, на противагу кіберексплуатації, в ході кібератак використовують активні можливості вірусів-шифрувальників та/чи ботнетів задля розгортання розподілених атак проти операційних систем (DDoS-атак), активації багатофункціонального шкідливого програмного забезпечення, хмарних ланцюгів тощо [132, с. 823; 37, с. 2]. Разом з тим, дослідження враховує кращу практику атрибуції випадків кіберексплуатації, оскільки така практика демонструє здатність багатьох державних та недержавних акторів здійснювати атрибуцію кібероперацій з високим рівнем достовірності. Така практика свідчить

про наступне: якщо атрибуція можлива у випадку відсутності порушення функціонування комп'ютера чи мереж (кіберексплуатація), то, як видається, вірогідність її здійснення зростає у випадку, коли має місце порушення такого функціонування.

З першого погляду може здатися, що існує загальне розуміння того, що собою представляють кібератаки для розробки колективних заходів реагування (зокрема, в цілях атрибуції) на наслідки та їх попередження у майбутньому. Проте, в теорії, і ще більше на практиці, виникає ряд питань до атак в кіберпросторі, зокрема: що є об'єктом кібератаки; в який момент конкретна кібероперація може кваліфікуватися як кібератака; коли виникає необхідність у здійсненні атрибуції; чи застосовується міжнародне право до кібератак і, якщо так, то в якому об'ємі. Всі ці питання є логічним наслідком відсутності *lex specialis* для регулювання кібероперацій, яке б містимо юридично обов'язкове поняття та норми, що застосовуються до кібератак. Це зумовлює необхідність дослідження позиції держав та міжнародних установ щодо застосування міжнародного права в кіберпросторі.

1.2. Застосування наявного міжнародно-правового регулювання до кібератак

Генеральний секретар ООН Антоніо Гутеррес в ході свого інтерв'ю від 15 січня 2020 року заявив, що наступний великий конфлікт у світі розпочнеться у кіберпросторі: «Я переконаний, що якщо одного разу [у нас] відбудеться серйозне протистояння, то воно розпочнеться з масштабної кібератаки не лише на військові об'єкти, а й на певні об'єкти цивільної інфраструктури. І ми не маємо ясності щодо правових рамок такого сценарію» [234]. Думка, виражена Генеральним секретарем, досить точно характеризує наявний стан речей, проте відсутність *lex specialis* не означає відсутність міжнародних зобов'язань в кібердомені.

Експерти Талліннського керівництва зробили значний внесок в розуміння того, як міжнародне право застосовується до кіберпростору, але, як зазначив,

професор Женевського університету М. Сассолі, «воно [Талліннське керівництво] не зуміло представити нові правила там, де це було потрібно, і часто критикується за те, що було розроблено в основному експертами НАТО». Він також зазначив, що сучасна міжнародна атмосфера не сприяє і не буде сприяти розробці нових правил, допоки міжнародна спільнота не засвідчить кібератаку з катастрофічними наслідками [204, с. 541-542]. Прикро це визнавати, але історія людства підтверджує висновок професора М. Сасолі: чомусь саме збройні конфлікти, техногенні катастрофи та інші кризові ситуації є каталізатором розробки та прийняття важливих норм міжнародного права. Разом з тим, потрібно усвідомлювати наступне: навіть якщо спеціальні норми будуть розроблені, існує високий ризик того, що в силу швидкого розвитку технологій вони застаріють до свого вступу в силу [251, п. 24].

Водночас не можна повністю погодитись з думкою професора М. Сасолі, оскільки позиція держав, виражена в їх односторонніх заявах та деклараціях, свідчить про те, що вона є реакцією на норми Талліннських керівництв, які загалом знаходять підтримку серед держав. Відтак, ці Керівництва мають більший вплив, ніж може здатись на перший погляд, адже норми звичаєвого міжнародного права формуються саме на їх основі.

Як видається, Талліннські керівництва можна прирівняти до Статей про відповідальність держав від 2001 року: ця доктринальна кодифікація навряд чи переросте в міжнародно-правовий інструмент в сфері регулювання кібероперації, але більшість положень мають всі шанси на те, щоб отримати статус звичаєвих норм міжнародного права. Зумовлено це унікальністю Талліннських керівництв, які є найбільш авторитетною кодифікацію норм щодо застосування міжнародного права до кібероперацій.

Держави постійно стикаються з кібератаками, але не завжди можуть самостійно сформувати розуміння про атрибуцію та кібератаки, наприклад, щодо того, коли такі кібероперації призводять до порушення міжнародного права, і, найголовніше – щодо визначення того, застосовується загальне міжнародне право чи спеціальний міжнародно-правовий режим. Водночас ці

аспекти є принципово важливими для того, щоб визначити – з якою ціллю здійснюється атрибуція кібератаки – до прикладу, для реагування на кібератаку шляхом застосування сили чи для подальшого притягнення до відповідальності за наслідки такої атаки. Фактично лише Талліннські керівництва роблять спробу дати відповідь на ці питання, і саме до них держави звертаються в першу чергу, тому не варто недооцінювати їх роль, попри відсутність юридично обов'язкового характеру.

Що стосується застосування міжнародного права до інформаційно-комунікаційних технологій та до кібератак, яке тривалий час було дискусійним [145, с. 1367], наразі це вже не оспорюється. Як наголошується в Доповіді групи урядових експертів щодо досягнень в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки від 24 червня 2013 року, «Міжнародне право, і зокрема Статут Організації Об'єднаних Націй, застосовується і має важливе значення для підтримки миру і стабільності, створення відкритого, безпечного, мирного і доступного інформаційного середовища… [М]іжнародні норми і принципи, що випливають з принципу державного суверенітету, поширюються на поведінку держав у межах діяльності, пов'язаної з використанням ІКТ, а також на юрисдикцію держав над ІКТ-інфраструктурою на їх території» [9, п. 19-20; 10, п. 24-26].

У Доповіді Групи урядових експертів від 2015 року, яка підтверджує висновок про застосування Статуту та міжнародного права до ІКТ, вказується, що найважливіше значення мають такі зобов'язання як: «суверенна рівність держав; вирішення міжнародних суперечок мирними засобами таким чином, щоб не ставити під загрозу міжнародний мир, безпеку і справедливість; відмова в 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 Організації Об'єднаних Націй; повага до прав людини і основних свобод; невтручання у внутрішні справи інших держав» [10, п. 26]. Попри це, держави не завжди розуміють, коли ці принципи порушуються і по-різному підходять до їх інтерпретації, що, в свою

чергу, зумовлює питання про те, чи мало місце порушення, яке має атрибутуватись державі. І від відповіді на це питання буде залежати здійснення атрибуції, зокрема, у ситуаціях незначного порушення функціонування систем чи активів, що спричинило короткострокові незручності.

Таким чином, кібератаки не є однорідними за своєю природою та наслідками. Неоднорідним є і саме міжнародне право, яке представляє систему, що об'єднує норми в галузі, інститути та спеціальні міжнародно-правові режими.

Аналіз наявної доктрини та позицій держав дозволяє виділити три групи кібератак, які «запускають» різні правові режими та зобов'язання в системі міжнародного права, відтак, вимагають різних видів атрибуції:

1) кібератаки, які не досягли порогу збройної атаки, але призвели до порушень міжнародних зобов'язань (зокрема, основних принципів міжнародного права, порушень прав людини тощо) [206, с. 698];

2) кібератаки, які досягають рівня збройного нападу (атаки) та наділяють державу правом на самооборону відповідно до *jus ad bellum* [207, с. 571-572];

3) кібератаки, які можна кваліфікувати як збройну атаку, коли вони здійснені в ході збройного конфлікту або такі, що активують *jus in bello* [211, с. 368-375].

Без розуміння цієї природи не можливо говорити про те, чи здійснюється атрибуція і головне – для яких цілей. Адже в кожному із зазначених випадків атрибуція буде здійснюватися для різних цілей і встановлюватиме вимоги, зокрема, щодо часу та оцінки наявних індикаторів. Так, наприклад, у випадку звернення до односторонніх заходів самодопомоги в рамках *jus ad bellum* державам потрібно здійснити атрибуцію *ex ante* в короткі строки, яка буде відрізнятися від атрибуції *post factum* судового чи іншого органу [209]. Отже, розуміння характеру кібератаки визначає право, яке буде застосовуватися до кібернетичної атаки, мету атрибуції і найголовніше – заходи реагування на таку кібератаку. В кіберконтексті це також означає встановлення того, чи достатнім буде здійснення виключно технічної та/чи політичної атрибуції кібератак проти об'єктів критичної інфраструктури (детальніше в підрозділі 2.4).

Як було зазначено вище, факт застосування міжнародного права до кібератак вже не викликає сумнівів, але низка держав все ще оспорює застосування *jus in bello* та *jus ad bellum* до кібератак. У Консультативному висновку 1996 року про законність погрози ядерною зброєю або її застосування Міжнародний Суд ООН підкреслив, що міжнародне гуманітарне право «застосовується до всіх форм воєнних дій та всіх видів зброї минулого, сьогодення і майбутнього» [16, п. 86]. Відтак, очікуваним та логічним є застосування міжнародного гуманітарного права в кіберпросторі.

В межах роботи Групи урядових експертів, експерти від Російської Федерації та Китаю заперечували можливість застосування МГП до кібератак, оскільки, на їх думку, це може призвести до виправдання ворожого застосування кіберпростору проти військових об'єктів [151]. Позиція Куби, яка є у відкритому доступі, також зводиться проти визначення того, як *jus ad bellum* та *jus in bello* застосовуються до використання ІКТ в силу побоювань щодо потенційної мілітаризації кіберпростору, яка може «легітимізувати ... односторонні каральні силові дії, включаючи застосування санкцій і навіть збройної сили державами, які заявляють, що є жертвами незаконного використання ІКТ» [98]. В дійсності такі побоювання не позбавленні раціонального зерна, але, не дивлячись на таку риторику, застосування міжнародного гуманітарного права до кібероперацій, незалежно від того, розглядаються вони в якості засобу чи методу ведення збройних дій, є беззаперечним [204, с. 534].

Декларація Куби робить акцент на неможливості розглядати зловмисне використанням ІКТ в якості «збройної атаки», що згадується в статті 51 Статуту ООН та наділяє постраждалу державу правом на самооборону відповідно до *jus ad bellum.* Такий підхід представник Куби обґрунтував тим, що оновлена інтерпретація положень Статуту призведе до нав'язування «законів джунглів», де інтереси найсильніших держав матимуть перевагу над інтересами найбільш вразливих. В Декларації містився заклик до необхідності «прийняти міжнародний юридично обов'язковий інструмент, щоб на основі співпраці ефективно реагувати на значні існуючі правові прогалини в контексті

кібербезпеки та зростаючі виклики та загрози, з якими ми стикаємось у цій галузі» в межах діяльності Організації Об'єднаних Націй [98].

Беручи до уваги той факт, що у роботі Групи урядових експертів приймали представники лише 25 держав світу, можна допустити, що низка країн світу, зокрема латиноамериканських, схиляється до позиції вираженої представником Куби. Пояснити це можна реальними побоювання щодо потенційних маніпуляцій і помилкової атрибуції, що є наслідком спуфінгу (маскування з метою фальсифікації даних щодо особи чи програми).

В українському контексті також не варто виключати зловживання з боку Російської Федерації в силу активності Головного управління Генерального штабу Збройних Сил РФ (ГУ/ГРУ). Адже в ході низки збройних конфліктів за участю Росії неодноразово виникали розбіжності щодо певних фактів. Згадати хоча б так званий «хлібний кошик Молотова», який містив в собі десятки запалювальних бомб та використовувався проти Фінляндії в ході Другої світової війни [40]. Відповідно до офіційної позиції, вираженої тодішнім міністром закордонних справ В. Молотовим – Радянський Союз скидав фінам хліб та їжу, а не бомби. Аналогічним чином вже Російська Федерація заперечувала характер «гуманітарної допомоги» ДНР/ЛНР, що загалом була не гуманітарною, а військовою допомогою цим формуванням [80]. Ці два приклади є показовими в тому плані, що навіть в фізичному світі є проблеми зі встановленням фактів причетності держав до неправомірних дій, а в кіберпросторі – все ще складніше. Серйознішими є і наслідки толерування неправомірної поведінки в силу особливостей кіберпростору.

Що ж до маніпуляцій в кіберпросторі, то вони ще раз підкреслюють важливість атрибуції кібератак. Дану проблему частково можна вирішити шляхом розробки юридично обов'язкового інструменту, який передбачав би створення спеціального механізму для здійснення міжнародно-правової кваліфікації кібератак та їх атрибуції на міжнародному рівні. Інакше, дійсно складно собі уявити як Рада Безпеки ООН може надавати рекомендації «зацікавленим сторонам» чи щодо них, чи приймати рішення щодо застосування

заходів, які не передбачають чи передбачають використання збройних сил відповідно до статей 40 та 41 Статуту [245], коли відсутнє розуміння того, – хто ці сторони (як правило, складнощі існують саме щодо ідентифікації держави-правопорушниці). Те саме стосується держав, які постраждали від збройної атаки та, відповідно, мають всі права на реалізацію свого права на самооборону відповідно до Статуту ООН.

З позиції встановлення норм відповідальної поведінки держав в кіберпросторі, досить негативним є той факт, що багато держав-учасниць Відкритої робочої групи, яка була створена за ініціативи Російської Федерації, досі заперечують застосування міжнародного гуманітарного права у кіберпросторі. Так, наприклад, перший проект звіту групи, в розробці якого брали участь такі держави як Австралія, Єгипет, Індонезія, Росія та Великобританія, в досить стриманому стилі згадує про міжнародне гуманітарне право: «… міжнародне право є основою стабільності та передбачуваності відносин між державами. Зокрема, міжнародне гуманітарне право зменшує ризики та потенційну шкоду як для цивільних осіб, так і для цивільних об’єктів, а також для комбатантів у контексті збройного конфлікту. У той же час держави наголошують, що міжнародне гуманітарне право ані заохочує мілітаризацію, ані легітимізує вдавання до конфліктів у будь-якій сфері» [146].

На превеликий жаль, даний параграф не увійшов в фінальний звіт 2021 року [117], навіть попри намагання Міжнародного Комітету Червоного Хреста мінімізувати заперечення деяких держав шляхом внесення поправок. До прикладу, МКЧХ запропонував доповнити завершення параграфу фразою «і не повинно тлумачитись [інтерпретуватись] як таке», а також фразою «підкреслюючи, що збройному конфлікту у кіберпросторі необхідно запобігати» в середині 84 параграфу [70, п. 84]. Очевидно, цього було не достатньо, щоб підтвердити те, що визнання застосування МГП до кіберпростору не рівнозначне його мілітаризації.

Разом з тим, як підкреслює професор М. Шмітт, кібератаки, як і акти спричинення голоду, удушення, побиття, стрільби та бомбардування,

підпадають під дію гуманітарного права в силу конкретних наслідків, до яких призводить [211, с. 375]. Відтак, заперечувати застосування норм *jus in bello* в кіберпросторі вважаємо за неприпустиме.

Міжнародне гуманітарне право або *jus in bello* буде застосовуватися до кібероперацій, якщо кібератака здійснюється в ході збройного конфлікту або пов'язана з ним і входить в зміст поняття «атака», що згадується в джерелах МГП. Оскільки юридично встановлене визначення того, що таке кібератака, відсутнє, звернемося до традиційного поняття «атака» (або «напад», що відповідно до офіційного перекладу з англійської є синонімом поняття «attack»), яке міститься в статті 49 (1) Додаткового Протоколу І до Женевських Конвенцій 1949 року. Згідно з ним, поняття «атака» охоплює «акти насильства щодо противника, незалежно від того, здійснюються вони під час наступу чи під час оборони» [7, ст. 49 (1)], а також представляє собою військові дії «на суші, в повітрі або на морі» [7, ст. 49 (3)]. При цьому, «акти насилля» не обмежені кінетичними засобами [103, с. 5].

Вважається, що у випадку з кібератаками це визначення є проблематичним та надмірно інклюзивним [204, с. 535]. По-перше, тому що кібератаки фактично здійснюються в кіберпросторі, а не «на суші, в повітрі або на морі», як встановлює Додатковий протокол І. По-друге, це поняття фактично охоплює весь спектр кібератак. Отже, можна погодитись з підходом експертів Талліннського керівництва, які встановили, що вирішальним фактором для кваліфікації є очікувані наслідки від такої атаки, незалежно від того, є вони вторинними чи третинними за своєю природою [209, с. 415].

Саме кібероперації, які здійснюються проти осіб чи об'єктів, розглядаються в якості атаки, якщо ціллю останніх було завдання шкоди або знищення. Аналогічний підхід, зокрема, застосовується до використання ядерної, хімічної та біологічної зброї, що не вимагає застосування фізичної сили [139, п. 120, 124]. Загалом такі кібератаки повинні атрибутуватися державам, навіть у ситуації, коли їх деструктивний потенціал з певних причин не був реалізований державою, що за ними стояла.

Також потрібно розуміти, що завдання шкоди системам, які використовуються для здійснення кібератаки, не є необхідною умовою. Так, наприклад, за допомогою маніпуляцій системи управління SCADA водних дамб, можна спричинити викид вод, а отже – втрати серед цивільного населення і знищення цивільних об'єктів. При цьому, в подальшому сама система може продовжити своє нормальне функціонування і не зазнати пошкодження чи знищення [209, с. 416].

Суперечливим є момент щодо того, чи можуть дані бути об'єктом атаки. Від відповіді на дане питання залежить те, чи будуть такі кібератаки атрибутуватись державі. Це питання загалом залишається відкритим, але в Талліннському керівництві зазначається, що «операція проти даних, на яку покладається функціональність фізичних об'єктів, іноді може становити атаку» [209, с. 416]. Водночас відкритим залишається питання – в яких саме випадках кібератака спрямована проти даних об'єкта критичної інфраструктури буде становити атаку.

Припустимо, що мова йде про нейтралізацію даних як об'єкта кібератаки, коли сторона отримує військову перевагу шляхом видалення даних, а не знищення систем. Стаття 52 (2) Додаткового протоколу I до Женевських Конвенцій встановлює, що військовими є об'єкти «… повне або часткове руйнування, захоплення або нейтралізація яких при існуючих в даний момент обставинах надає очевидну військову перевагу» [7].

Як випливає з поняття «нейтралізація», знищення об'єкту не є обов'язковою умовою [106, с. 4]. Тому, повертаючись до Талліннського керівництва, можна зробити висновок, що дані можуть стати об'єктом кібератаки, попри те, що об'єкт має бути «видимим та відчутним», як підкреслюється в коментарі Міжнародного Комітету Червоного Хреста [69, п. 2006-2007].

І хоча можна сперечатись щодо того, в яких ситуаціях військові операції проти даних становитимуть атаку і передбачатимуть застосування норм МГП, такі випадки, наприклад, як знищення даних, що забезпечують функціонування

фінансового ринку країни, дозволяють маніпулювати системами управління повітряним рухом противника, системами потоків нафтопроводів або атомними станціями тощо, очевидно, розглядатимуться в якості атаки. Адже складно, якщо взагалі можливо, розглядати такі дії в якості короткотривалих незручностей.

Нарешті, кібератаки, які не досягли мінімального рівня застосування сили, але призвели до порушень міжнародних зобов'язань. Найчастіше вони розглядаються в якості порушення основних принципів міжнародного права – принципу суверенної рівності держав, заборони інтервенції чи втручання у внутрішні справи держав тощо, або порушення договірних чи звичаєвих норм окремих галузей міжнародного права (міжнародного права прав людини, міжнародного повітряного права, міжнародного економічного права та інших) залежно від конкретної ситуації. Реагування на них може бути різним, тут все залежить від зобов'язання, яке було порушено.

Підсумовуючи, варто зазначити, що міжнародне право в повному об'ємі застосовується до кібернетичних атак, хоча його застосування вимагає певної конкретизації з урахуванням природи та особливостей кіберпростору. Кібератаки та середовище їх застосування часто вимагають від міжнародної спільноти переосмислення та нового підходу до застосування існуючих норм міжнародного права, але, незважаючи на відсутність юридично обов'язкового інструменту та небажання низки держав визнавати застосування деяких галузей міжнародного права до кібератак, вони все ж застосовуються. Відповідно, здійснення атрибуції в межах, до прикладу, *jus in bello* чи *jus ad bellum* переслідуватиме різні цілі та матиме різні наслідки. І наразі важливо, щоб держави прийшли до консенсусу про застосування всього спектру норм міжнародного права в кіберпросторі та визначення особливостей їх застосування.

1.3. Аналіз *opinio juris* та практики держав щодо поведінки в кіберпросторі, яка повинна атрибутуватись державам

Пандемія COVID-19 перше, що спадає на думку, коли мова йде про 2020 рік. Але 2020 рік також увійшов в історію як рік «кіберпандемії». В силу того, що значна частина соціальних, економічних та політичних взаємозв'язків відбувалась в кіберпросторі без перебоїв чи серйозних наслідків для близько 80 відсотків економіки, кібердіяльність значно зросла. З одного боку, кіберпростір вирішив виклики, спричинені COVID-19, які не могли подолати, наприклад, під час пандемії 1918 року, з іншого – в декілька разів збільшив кількість кібероперації [163]. На фоні всіх суб'єктів, що стоять за кібератаками як різновидом кібероперацій, на особливу увагу заслуговують саме ті, чиї дії можуть атрибутуватися державі для цілей притягнення держав до відповідальності за міжнародним правом.

Загалом притягнення держави до відповідальності представляє собою правовий режим, основні правила якого зав'язані на наявності двох елементів. Згідно зі статтею 2 Статей про відповідальність держав за міжнародно-протиправні діяння, міжнародна відповідальність держави наступає у випадку наявності протиправної поведінки, яка «(а) атрибутується державі відповідно до міжнародного права; (б) представляє собою порушення державою свого міжнародного зобов'язання» [107, ст. 2]. Тобто, відповідальність держав настає при наявності юридичних та фактичних підстав для такої відповідальності.

Під юридичними підставами відповідальності держав слід розуміти міжнародно-правові зобов'язання держави, незалежно від їх походження, які містять вимогу щодо поведінки держави, порушення якої дозволяє кваліфікувати діяння як міжнародне правопорушення [41, с. 153]. Як неодноразово вказував Міжнародний суд ООН, «зобов'язання можуть покладатись на державу в силу договору і в силу дії звичаєвої норми, або в силу договору і в силу одностороннього акту» [176, п. 63].

У випадку з кіберпростором, щодо застосування якого відсутнє *lex specialis*, виникає необхідність у встановленні того, як існуючі міжнародні зобов'язання повинні тлумачитись та застосовуватись до конкретних кібероперації. Вважається, що *opinio juris* може компенсувати недостатньо розвинену або непослідовну практику держав щодо формування міжнародних звичаїв [158, с. 111-112]. Водночас потрібно розуміти, що на стадії формування звичаєвих норм, заяви, декларації, кіберстратегії та воєнні доктрини, які можна розглядати в якості форм вираження *opinio juris,* не мають визначального характеру. Їх характер швидше орієнтуючий, що дозволяє на підставі аналізу *opinio juris* встановити «межі» відповідальної поведінки в кіберпросторі та розуміння того, якими держави бачать існуючі зобов'язання та що вкладають в їх зміст.

Для даного дослідження визначення таких зобов'язань – це підґрунтя та передумова атрибуції, оскільки без розуміння того, що конкретна поведінка є порушенням міжнародних зобов'язань, складно (якщо взагалі можливо), здійснювати атрибуцію; і що не менш важливо – це відповідь на питання, яким держави бачать процес здійснення атрибуції кібератак. Крім того, такі позиції демонструють переважаюче непогодження щодо таких аргументів як необхідність нового правового інструменту задля заповнення «правового вакууму» (з позиції Куби, вираженої в ході роботи ГУЕ) або «прогалину некерованих територій» (позиція Індонезії, яка виступала від імені Руху неприєднання) [120].

Вироблення і узгодження позицій держав в майбутньому сприятиме загальній практиці, а значить – формуванню звичаєвих норм міжнародного права. Цілком справедливо можна зауважити, що саме в сфері регулювання діяльності держав в кіберпросторі, як вбачається, норми звичаєвого права відіграватимуть ключову роль, оскільки розробка міжнародного інструменту швидше стане ще одним «проектом статей» в силу швидкого розвитку інформаційних технологій, які завжди випереджають позитивне міжнародне право.

Загалом аналіз *opinio juris* в даній роботі здійснюється для:

1) визначення того, які норми міжнародного права застосовуються в кіберпросторі;

2) ідентифікації кібератак, які держави розглядають в якості міжнародно-протиправної поведінки, що має атрибутуватись державі;

3) встановлення того, яким держави бачать процес атрибуції кібератак, а також з метою визначення їх позиції щодо необхідності здійснення технічної та політичної атрибуції кібератак;

4) встановлення суб'єктів, поведінка яких, на думку держав, буде атрибутуватись в кожному конкретному випадку.

З позицій держав, які опублікували офіційні заяви щодо того, як міжнародне право застосовується до кіберпростору, загальну підтримку має ідея того, що міжнародне право застосовується. Коли ж мова йде про конкретні зобов'язання, держави не завжди спроможні виробити чітку позицію. Так, наприклад, опублікована у 2021 році промова заступника генерального прокурора Ізраїлю, яка містить погляди Ізраїлю щодо ключових правових та практичних питань застосування міжнародного права до кібероперацій, містить більше питань, ніж відповідей [212]. Включення її до бази НАТО [224] підтверджує юридичний характер такої заяви, а не виключно доктринальний підхід.

В свою чергу, позиція Ліхтенштейну від 10 лютого 2020 року зводиться до визнання того, що Статут ООН в цілому та інші джерела міжнародного права, зокрема в галузі міжнародного гуманітарного права, права людини та міжнародного кримінального права застосовуються в кіберпросторі. Наразі Ліхтенштейн єдина держава, яка безпосередньо згадала міжнародне кримінальне право в своїй заяві. Що ж стосується інших держав, то їх позиція зводиться до відповідальності держав – згадка про можливу відповідальності індивідів відсутня (за винятком згадок про відповідальність за національним правом). Але Ліхтенштейн закликав розглянути питання щодо встановлення того, як Римський

Статут Міжнародного кримінального суду застосовується до кібервоєн [217, с. 3].

Аналіз позицій різних держав демонструє зацікавленість у встановленні та конкретизації того, як певні норми застосовуються в кіберпросторі. В першу чергу, на увагу заслуговує інтерпретація принципу суверенної рівності держав. Одні держави ігнорують його або наголошують на його абстрактному характері, інші – розкривають його зміст в кіберконтексті. В контексті даної дисертаційної роботи визнання того, що принцип суверенної рівності держав є юридичним зобов'язанням, яке може бути порушене в результаті застосування кібератаки, означатиме можливість та/чи необхідність здійснення атрибуції кібератак; в противному випадку – така можливість та/чи необхідність відсутня. Адже не можна державі атрибутувати поведінку, яка не порушує зобов'язань за міжнародним правом.

Класичне визначення того, що представляє «суверенітет» було надано в арбітражному рішенні щодо острову Пальмас (США проти Нідерландів). Арбітр М. Губер вказав, що «Суверенітет у відносинах між державами означає незалежність. Незалежність щодо частини земної кулі являє собою право здійснювати там, за винятком будь-якої іншої держави, функції держави. Розвиток національної організації держав протягом декількох останніх століть і, як наслідок, розвиток міжнародного права встановив цей принцип виключної компетенції держави щодо її власної території […]» [143, с. 8].

В класичному варіанті нормативний зміст принципу суверенної рівності держав розкрито в Декларації про принципи міжнародного права 1970 року, а також в Заключному акті НБСЄ від 1975 року. Відповідно до положень Декларації 1970 року поняття «суверенна рівність» включає шість елементів:

1) держави є юридично рівними;

2) кожна держава користується правами, властивими повному суверенітету;

3) кожна держава зобов'язана поважати правосуб'єктність інших держав;

4) територіальна цілісність і політична незалежність держави є недоторканними;

5) кожна держава має право вільно обирати й розвивати свої політичні, соціальні, економічні та культурні системи;

6) кожна держава зобов'язана виконувати добросовісно та в повному обсязі свої міжнародні зобов'язання, жити в мирі з іншими державами [5].

Найбільш послідовно та зважено, як видається, до інтерпретації принципу суверенітету підійшла Німеччина у свої позиції щодо застосування міжнародного права в кіберпросторів від 5 березня 2021 року. Пояснюється те, як Німеччина бачить порушення політичної незалежності (втручання в хід виборів), а також територіальної цілісності. Щодо останнього, зазначається, що «кіберпростір не є детеріторізованим простором» [230, с. 3]. Звичайно в кіберпросторі відсутні традиційні кордони між державами, але, як зазначив Уряд Німеччини, «не існує незалежних «кіберкордонів», які не узгоджуються з фізичними кордонами держави, обмежуючи або нехтуючи територіальною сферою охоплення суверенітету». Тобто, держави в межах своїх фізичних кордонів, з одного боку, мають право в повній мірі здійснювати свої повноваження щодо захисту кібердіяльності осіб, які в ній беруть участь, а також кіберінфраструктури від втручання (включаючи кібервтручання) з боку іноземних держав, з іншого – зобов'язанні не дозволяти використовувати їх територію для дій, що суперечать правам інших держав [230, с. 3].

Німеччина також виразила підтримку Правилу 4, запропонованому в Талліннському керівництві 2.0, яке говорить про те, що кібероперації, які атрибутуються державі та призвели до фізичних наслідків і шкоди на території іншої держави, є порушенням територіального суверенітету цієї держави. В контексті цього наукового дослідження важливим є і той факт, що, на думку Німеччини, кібероперації в ході яких постраждали об'єкти критичної інфраструктури можуть розглядатися в якості порушення територіальної цілісності.

Поряд з критичною інфраструктурою згадуються і «компанії, що представляють особливий суспільний інтерес». Логічно допустити, що таке формулювання викликане відсутністю загально прийнятого поняття «критична інфраструктура». Це випливає з того, що позиція щодо цього принципу завершується твердженням про те, що кібероперації спрямовані проти інших об'єктів чи компаній, що не кваліфікуються в якості «критичної інфраструктури» або «компаній, що представляють особливий суспільний інтерес» також можуть призвести до порушення принципу територіальної цілісності, як одного із конститутивних елементів принципу суверенної рівності [230, с. 4].

Досить схожою є позиція Франції, виражена в 2019 році. Згідно з нею, Франція наголошує, що здійснює свій суверенітет над інформаційними системами, розташованими на її території, а також вимагає слідувати принципу *due diligence*, який випливає з суверенітету. Як зазнає французька сторона, держави повинні: (1) використовувати кіберпростір відповідно до міжнародного права, зокрема – не використовувати третіх осіб (проксі) для вчинення дій, які за допомогою ІКТ порушують права інших держав, та (2) гарантувати, щоб їх територія не використовується для таких цілей, в тому числі недержавними суб'єктами [123, с. 6].

Що ж стосується принципу суверенітету, то зазначається, що він може бути порушений виключно державою, яка діє через офіційні органи, *de facto* органи, які виконують елементи урядових повноважень, або через приватних осіб, що діють за вказівками або під керівництвом чи контролем держави. Відтак, виключається можливість розглядати спорадичні кібератаки незалежних хакерів в якості порушень суверенітету держави. Призвести до порушення суверенітету можуть будь-які кібератаки, спрямовані проти цифрових систем Франції, або наслідки, що є результатом використання цифрових систем в межах території Франції [123, с. 7]. З цього робимо висновок, що підхід держави полягає в тому, що будь-яке несанкціоноване проникнення в інформаційно-комунікаційні системи Франції, є порушенням даного принципу.

В офіційній позиції Чеської Республіки прослідковується досить чітка конкретизація того, що, на думку держави, становить порушення принципу суверенної рівності держав за умови, що здійсненні проти Чехії кібероперації атрибутуються іноземній державі. Справедливим буде зазначити, що Чехія відходить від підходу щодо необхідності «проникнення». Уже в першому пункті («А») виділяються кібероперації, що призводять до смерті або поранення людей або завдають значної фізичної шкоди. Наразі Чехія єдина відома нам держава, що пов'язує такі ситуації з принципом суверенної рівності держав. Як видається, таким чином держава хоче посилити свою позицію щодо того, що принцип суверенітету є «самостійним правом», повага до якого становить «самостійне зобов'язання» [96, с. 3].

Як правило, кібероперації, що спричиняють смерть (чи поранення) людей або значний фізичний збиток кваліфікуються як застосування сили, якщо на це вказуватиме тест на «масштаб та наслідки» («*scale and effects*»), що є досить популярним серед держав та використовується задля співставлення кібератак із атаками у «фізичному» світі. Прикрим упущенням цієї заяви є те, що в позиції Чехії відсутні висновки щодо того, коли кібератаки кваліфікуються як застосування сили. Проте, відсутність таких положень може розглядатись в якості свідчення загальної підтримки положень та висновків, до яких прийшли держави та експерти Талліннського керівництва.

В другому пункті («В») згадуються кібероперації, що спричиняють пошкодження або порушують функціонування кіберінфраструктури чи іншої інфраструктури, що суттєво впливає на національну безпеку, економіку, охорону здоров'я чи навколишнє середовище. Кібероперації, що передбачають втручання в дані або надання послуг, необхідні для здійснення невід'ємних функцій уряду («С»), також розглядаються як порушення принципу суверенної рівності держав. В заяві наводиться приклад останніх кібероперацій: розповсюдження програм-шантажистів, що шифрують комп'ютери, які використовуються урядом, коли воно призводить до затримки виплати пенсій [96, с. 3].

В розріз з позицією більшості держав та експертів Талліннського керівництва йде останній пункт («D»), який, на жаль, не супроводжується поясненням з боку Уряду Чехії. Так, кібероперації проти держави, державних органів чи агентів, що знаходяться в межах її території, включаючи міжнародні організації, є порушенням принципу суверенітету, якщо здійснюються органами іншої держави, що фізично присутні на території Чехії. Не зрозуміло, чому акцент робиться на фізичній присутності агентів іноземної держави, а не на наслідках кібероперації. Виходить, що кібероперації, які здійснюються з території держави-порушниці, незалежно від наслідків, не розглядаються в якості порушення суверенітету Чехії. В той час, як аналогічні операції здійснювані з території останньої – є порушенням суверенітету. Як видається, наслідки в обох випадках можуть бути ідентичними, але їх юридична кваліфікація – різна. Відтак, виникає чимало питань до такого підходу, на які наразі відсутня можливість отримати відповіді.

Цей пункт також змушує задуматись над кібероперaціями, здійсненими недержавними акторами. В пункті «D» чітко зазначається «органами іншої держави» («*organ of another State*»), і під це формулювання однозначно не можуть підпадати проксі, які діють відповідно до вказівок або під контролем чи керівництвом держави. Враховуючи те, що цей пункт використовує формулювання з Талліннського керівництва щодо реалізації елементів внутрішнього суверенітету в кіберконтексті, можна зробити висновок, що виключення частини «та інших, чия поведінка атрибутується державі» [209, с. 19] з заяви Чехії було свідомим вибором. Адже навряд чи мало місце випадкове скорочення.

В липні 2020 року свою офіційну позицію щодо застосування міжнародного права у кіберпросторі опублікував Генеральний штаб Збройних сил Ісламської Республіки Іран [99]. Декларація складається лише з преамбули і чотирьох статей, які в досить стислому вигляді висвітлюють позицію Ірану з ключових питань: принципу суверенітету, заборони інтервенції та заборони використання сили.

Відповідно до статті II (4) неправомірне проникнення в публічну чи приватну кіберінфраструктуру може розглядатися в якості порушення суверенітету держави, що стала жертвою такого проникнення [99, ст. II (4)]. Цікаво, що у параграфі 5 цієї статті зазначається, що принцип суверенітету підпорядковується принципу рівності, і «суверенітет будь-якої держави не вище суверенітету інших держав. Отже, будь-які обмежувальні та заморожувальні заходи, включаючи санкції, є порушенням суверенітету незалежних держав через недотримання суверенітету держав-жертв атаки» [99, ст. II (5)]. Звичайно держави повинні поважати суверенітет одна одної, але санкції не є порушенням суверенітету. Такий висновок суперечить положенням міжнародного права, тому що санкції – це форма дозволеного примусу, що є реакцією на міжнародно-протиправне діяння. Можна справедливо припустити, що така позиція держави є наслідком того, що Іран тривалий час знаходився під односторонніми та багатосторонніми санкціями. Разом з тим, така позиція є своєрідним повідомленням для міжнародної спільноти щодо того, яку поведінку, пов’язану з кіберпростором, Ісламська Республіка Іран готова атрибутувати.

Позицію Сполучених Штатів Америки щодо принципу суверенної рівності держав конкретизував Головний Радник Департаменту оборони П. Ней: «Щодо кібероперацій, які не є забороненою інтервенцією чи застосуванням сили, Департамент вважає, що відсутня загальна і послідовна практика держав, яка б випливала із усвідомлення юридичного обов’язку, що міжнародне звичаєве право загалом забороняє такі несанкціоновані кібероперації на території іншої держави». На думку Департаменту оборони США, мовчання багатьох держав щодо низки публічно відомих кіберпроникнень в іноземні мережі виключає висновок про те, що держави об’єдналися навколо спільної думки про те, що існує міжнародна заборона на всі подібні операції (хоча й зазначається, що такі операції, як правило, забороняються національним правом та передбачають відповідне покарання) [105].

Також було зазначено, що, не дивлячись на те, що США не розглядає «всі порушення суверенітету в кіберпросторі» в якості порушень міжнародного

права, Департамент продовжить вивчення цього питання. Отже, США відкидає підхід щодо того, що будь-яке несанкціоноване втручання (проникнення) є порушенням суверенітету, але залишає за собою можливість визначити «поріг» втручання для констатації порушення суверенітету.

В цілому не можна погодитись з позицією США. Те, що багато держав мовчать щодо того, що стали жертвами несанкціонованого проникнення, не означає, що вони таким чином виражають позицію щодо відсутності юридичних зобов'язань, які випливають з принципу суверенної рівності держав.

Як зазначала Комісія з міжнародного права, мовчання має значення в процесі формування звичаєвого права, коли воно має місце з боку постраждалої держави і *за умови, що така держава могла відреагувати* [108, с. 142-143]. Реальність кіберпростору полягає в складнощах здійснити достовірну атрибуцію кібератак, тому більшість держав, не маючи необхідних технічних та людських ресурсів, просто не знаходять себе «в позиції для реагування».

Що ж до тих держав, що мають необхідні спроможності, то їх практика демонструє зворотне. Так, наприклад, у вербальній ноті до Генерального Секретаря ООН Постійне представництво Венесуели при ООН від імені держав МЕРКОСУР засудило акти шпигунства з боку США, підкресливши, що такі дії «є неприйнятною поведінкою, яка порушує наш суверенітет і шкодить нормальним відносинам між народами» [125]. Подібним чином Грузія, яка зазнала широкомасштабної кібератаки з боку Головного управління розвідки Російської Федерації (ГРУ) у жовтні 2019 року, засудила дану атаку як таку, що «йде в розріз з міжнародними нормами і принципам, ще раз порушила суверенітет Грузії» [222]. Вірогідність того, що кібератаки були здійснені Головним управлінням ЗС РФ (ГРУ), відповідно до позиції Національного Центру Кібербезпеки Великобританії, який допомагав в питаннях атрибуції, становила більш ніж 95 відсотків [241].

Отже, коли постраждалі держави знаходяться «в позиції для реагування», тобто мають відповідні знання щодо того, хто стоїть за конкретною кібероперацією, вони впевнено вдаються до публічної атрибуції поведінки

іноземній державі та наголошують на порушені норм та принципів міжнародного права.

Доволі однозначною і не узгодженою з практикою самої держави є позиція Великобританії, озвучена 23 травня 2018 року. Генеральний прокурор Дж. Райт зазначив, що, попри фундаментальне значення суверенітету для міжнародно-правової системи, на даний момент неможливо екстраполювати із цього загального принципу конкретне правило або додаткову заборону для кібердіяльності, окрім заборони втручання. Таким чином, «[…] позиція уряду Великобританії полягає в тому, що не існує такої норми в межах сучасного міжнародного права» [91].

Наразі лише Великобританія зайняла таку позицію публічно, в той час як інші держави, що висловились з цього приводу, характеризують суверенітет як принцип і норму міжнародного права (наприклад, Німеччина, Франція, Чехія, Фінляндія, Іран, Нідерланди, Болівія, Китай, Гватемала, Гайана, Нова Зеландія, Республіка Корея та Швейцарія, а також НАТО, звісно, за винятком Великобританії). Інтерес привертає Кіберстратегія Великобританії на 2016-2021, де наголошується, що кіберпростір є сферою, в якій *«…* ми повинні захищати свої інтереси та суверенітет» [169]. Таке твердження піднімає досить важливе і частково неспівзвучне з офіційною позицією питання: чи дійсно треба захищати те, що, згідно з офіційною позицією уряду, не може бути порушено?

Існує ще одна група держав, позиція яких не містить визначеності. Так, наприклад, в позиції Ізраїлю відсутнє роз’яснення того, чи принцип суверенної рівності держав розглядається як норма міжнародного права, що застосовується в кіберпросторі та передбачає відповідальність у випадку його порушення. З одного боку, Ізраїль визнає те, що принцип суверенітету є «наріжним каменем міжнародного права та міжнародних відносин».

З іншого боку, проводиться розмежування між «суверенітетом як загальним поняття» (незалежність) та «територіальним суверенітетом, який є міжнародно-правовою нормою». Виходить, що позиція Ізраїлю зводиться до того, що посилаючись на захист своєї політичної волі та автономії, держави не

обов’язково посилаються на норму права. Свою позицію щодо принципу суверенітету представник Ізраїлю завершує твердження про злиття двох розумінь суверенітету та застереження про те, що «слід бути дуже обережними, роблячи юридичні висновки» [212, с. 402]. Відтак, не зрозуміло, чи з ремарки щодо злиття можна зробити висновок про те, що Ізраїль не розглядатиме втручання чи узурпацію невід’ємних урядових функцій в якості порушення суверенітету постраждалої держави, як це роблять експерти Талліннського керівництва відповідно до Правила 4.

Після цього, хочеться звернутися до позиції Фінляндії, яка досить вдало наголосила на наступному: «Погодитись з тим, що ворожа кібероперація, яка не досягає порогу забороненої інтервенції, не становить міжнародно-протиправне діяння, означає залишити такі операції поза рамками правового регулювання та позбавити постраждалу державу важливої можливості захищати свої права» [119, с. 3]. Відповідно, Уряд Фінляндії розгадає принцип суверенної рівності як норму міжнародного права, порушення якої є міжнародно-протиправним діянням та сигналом для притягнення держави до відповідальності держави. Отже, вони переконані в тому, що ця норма повністю застосовується в кіберпросторі.

B opinio juris Фінляндії також підкреслюється, що вирішення питання щодо того, чи несанкціоноване кіберпроникнення призведе до порушення суверенітету держави, яка була ціллю кібератаки, залежить від характеру такої атаки та її наслідків і підлягає оцінці в кожному конкретному випадку [119, с. 3]. Складно не погодитись з таким висновком, оскільки незначні кібератаки, без руйнівного потенціалу, що призвели до незначних короткострокових незручностей в роботі об’єктів критичної інфраструктури, навряд чи будуть розцінюватися як порушення одного із основних принципів міжнародного права. Сумнівною буде і необхідність їх атрибуції на міжнародному рівні, хоча навіть в таких випадках існує потреба у встановленні джерела кібероперації. І таке завдання, швидше за все, лежатиме виключно на компетентних органах держави.

Поряд із принципом суверенної рівності держав згадується заборона інтервенції. Згідного з Правилом 66 Талліннського керівництва, «[д]ержава не може здійснювати інтервенцію (прим. – *анг*. «intervene»), в тому числі за допомогою кіберзасобів, у внутрішні або зовнішні справи іншої держави» [209, с. 312]. Враховуючи непослідовність у використанні таких термінів як «інтервенція» та «втручання», підкреслимо, що мова йде саме про інтервенцію у розумінні інструментів, прийнятих в рамках ООН (зокрема, Декларації про заборону інтервенції та втручання у внутрішні справи держав), та Міжнародного Суду ООН. Держави досить часто використовують поняття «втручання» замість поняття «інтервенція», але вони мають різне юридичне наповнення.

Під «втручанням» слід розуміти дії держав, які вдираються у справи, що належать до суверенної прерогативи іншої держави, але позбавлені примусової сили, щоб досягти рівня інтервенції. Натомість поняття «інтервенція» обмежується таким втручанням у справи іноземної держави, що має примусовий ефект [209, с. 313]. Як зазначає Міжнародний Суд ООН: «Інтервенція є неправомірною, коли вона передбачає використання методів примусу щодо такого вибору, який повинен залишатися вільним» [62, п. 205]. Тобто, обов’язковою характеристикою інтервенції є наявність примусу.

Що стосується принципу заборони інтервенції, то всі держави, які висловили свою офіційну позицію щодо застосування міжнародного права у кіберпросторі, зійшлись на тому, що цей звичаєвий принцип безсумнівно застосовується. Серед основних прикладів інтервенції, більшість держав згадувала інтервенцію у виборчий процес, яка є втручанням у внутрішні справи держави та характеризується наявністю примусу (маніпулювання результатами голосування), втручання у фундаментальну діяльність парламенту або стабільність фінансових систем держав (Франція, США, Німеччина, Ізраїль, Австралія).

Як і у випадку з принципом суверенної рівності, принцип заборони інтервенції застосовується виключно у відносинах між державами. Відтак, порушення даного принципу матиме місце, якщо за міжнародно-протиправними

діями стояли агенти держави або приватні особи, дії яких атрибутуються державі відповідно до норм міжнародного права [209, с. 313-314].

В Декларації Ісламської Республіки Іран від липня 2020 року підтверджується звичаєвий характер принципу заборони інтервенції [99]. Під порушенням цього принципу в кіберпросторі держава розглядатиме ситуації політичного силового втручання (маніпулювання результатами виборів або формування громадської думки перед виборами як приклади грубої інтервенції), призупинення роботи веб-сайтів з ціллю спровокувати внутрішню напруженість і конфлікти або масове надсилання повідомлень виборцям з ціллю впливу на результати виборів [99, ст. III (1)]. В статті III окрема увага приділяється військовій інтервенції, яка не містить відхилень від загально прийнятого підходу.

Під інтервенцією збройні сили також розглядатимуть всі ситуації, що передбачають застосування явних та «вишуканих» форм і складних прийомів примусу, повалення чи вираження обурення (образ) задля «інтриг в політичному, соціальному чи економічному порядку» чи «дестабілізації урядів, що прагнуть лібералізації власних економічних, політичних та культурних систем» (форм контролю, що існують в таких системах).

Втручання іноземців є незаконним відповідно до цієї статті щодо заборони інтервенції [99, ст. III (3)]. Така згадка про втручання іноземців без посилання на атрибуцію викликає ряд питань, зокрема, чи це випадковість, а якщо ні, то яким чином поведінка приватних осіб може призвести до порушення одного із основних принципів міжнародного права, що застосовується виключно у відносинах між державами. В будь-якому випадку, відсутні будь-які доступні для аналізу офіційні пояснення з приводу вираженої позиції щодо втручання іноземців.

Достатньо деталізованою є позиція Німеччини щодо принципу заборони інтервенції. Німеччина залишає за собою право розглядати розповсюдження дезінформації через Інтернет в якості порушення, якщо воно здійснюється з ціллю підбурення до насильницьких політичних переворотів, заворушень та/або громадянських міжусобиць у чужій країні, тим самим суттєво перешкоджаючи

нормальному проведенню виборів та підрахунку бюлетенів. На думку Уряду Німеччини, за своїми масштабами та наслідками така діяльність близька до підтримки повстанців, тому містить елемент примусу. У виборчому контексті інтервенцією у внутрішні справи держави також є виведення із ладу виборчої інфраструктури та технологій (зокрема електронних бюлетенів), «якщо це компрометує або навіть перешкоджає проведенню виборів, або якщо результати виборів тим самим суттєво модифіковані [230, с.5].

Як вже зазначалося, офіційне висловлення позиції щодо застосування міжнародного права в кіберпросторі відіграє важливу роль в процесі атрибуції міжнародно-протиправного діяння. З одного боку, *opinio juris* у всіх своїх формах сприяє формуванню звичаєвих норм, оскільки є одним із двох елементів такої норми. З іншої боку, в подальшому має визначальний вплив на практику держав.

Для прикладу, 3 жовтня 2018 року Національний центр кібербезпеки Великобританії на своєму офіційному сайті розмістив заяву про «невибіркові та безвідповідальні» кібератаки Головного розвідувального управління РФ (ГУ/ГРУ). В заяві цитується позиція міністра закордонних справ, в якій наголошується, що дії ГРУ «є безвідповідальними та невибірковими: вони намагаються зірвати та втрутитися у вибори в інших країнах; вони навіть готові завдати шкоди російським компаніям та громадянам Росії. Така модель поведінки демонструє їх бажання діяти, ігноруючи міжнародне право чи встановлені норми, діяти з почуттям безкарності та без наслідків». Також наголошується на тому, що Великобританія разом із своїми союзника готова реагувати на таку поведінку [168].

В заяві Національного центру кібербезпеки міститься перелік кібератак із відповідною оцінкою. Щодо чотирьох нових кібератак, які атрибутуються в цій заяві, зазначається наступне: «НЦКБ з високим ступенем впевненості (*high confidence*) встановив, що ГРУ майже напевно (*almost certainly*) відповідальне» [168]. Така атрибуція, очевидно, є значною перемогою в боротьбі за відповідальну поведінку в кіберпростору. Проте, відсутність конкретизації того,

які норми міжнародного права були «грубо» порушені з боку ГРУ, дещо нівелюють отримані результати, тому спробуємо розібратися з наявною практикою атрибуції кібератак та її відповідністю *opinio juris*.

Що стосується першої категорії атрибутованих кібератак, то саме з нею пов'язана найбільша складність встановлення того, які норми міжнародного права були порушені. Національний центр кібербезпеки випустив із уваги наявність збройного конфлікту в Україні, оскільки він ніде не згадується і відсутнє розмежування з іншими країнами, які не знаходяться в стані збройного конфлікту (поруч із постраждалими українськими секторами згадується «європейські та російські бізнес-структури»). Відтак, робимо висновок про те, що мова очевидно не про порушення норм міжнародного гуманітарного права.

Шифрування жорстких дисків, що призвело до неоперабельності систем київського метро, одеського аеропорту, Російського центрального банку та ряду російських ЗМІ, які перераховуються в першій категорії, представляє постійну втрату функціональності [168]. Відповідно до позиції деяких експертів Талліннського керівництва, серйозні наслідки (які не призвели до людських втрат чи знищення) можуть кваліфікуватися в якості порушення заборони незастосування сили [209, с. 342]. Проте, беручи до уваги позицію Великобританії, де було зазначено, що кваліфікуватися як порушення цього принципу будуть кібератаки проти ядерних реакторів та систем управляння повітряним рухом, що мали летальний ефект [91], можна з впевненістю відкинути імовірність того, що, на думку Великобританії, мало місце порушення цього принципу.

Що стосується принципу заборони інтервенції, досить складно (якщо взагалі можливо) встановити намір Російської Федерації змінити прийняте Україною рішення, що входить в коло суверенних прерогатив щодо «свободи вибору власної політичної, соціальної, економічної та культурної системи». Тому найбільш очікуваним є твердження про порушення принципу суверенної рівності держав. На противагу принципу незастосування сили чи заборони

інтервенції, він не містить важко досяжних вимог (щодо наслідків та примусу відповідно), а також є очевидно порушеним.

Виникає логічне запитання – чи може держава, яка не визнає, що з принципу суверенної рівності витікають юридичні зобов'язання, наполягати на його порушені та атрибутувати таке порушення іншій державі. Спільно з низкою держав, менше ніж через два тижні після публікації заяви на сайті Національного центру кібербезпеки, міністр закордонних справ з питань кібербезпеки наголосив на відповідальності ГРУ за кібератаку «NotPetya», підкреслюючи, що така кібератака «свідчить про тривалу зневагу суверенітету України», що проявляється у кібератаках проти уряду, енергетичного та фінансового секторів [219].

Зі свого боку, Україна наразі не представила свою офіційну позицію щодо застосування міжнародного права в кіберпросторі. Проте, із Стратегії кібербезпеки на 2021-2025 роки, затвердженої 14 травня 2021 року, випливає, що Україна підтримує тезу про повне застосування міжнародного права в кібердомені. Зокрема, в Стратегії зазначається, що «Україна продовжить активну участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також добровільних необов'язкових норм, правил та принципів відповідальної поведінки держави», а також те, що «Україна буде сприяти подальшому дотриманню міжнародного права та стандартів у галузі прав людини, […]» [37].

Крім того, в Законі України «Про основні засади забезпечення кібербезпеки України» згадується реалізація «невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі» [29]. Таким чином, виводячи приватне із загального, можна з високою вірогідністю допустити, що позиція України проявляється у повному застосуванні норм міжнародного права до кібератак. Це могло б означати те, що Україна вправі притягнути Російську Федерацію до відповідальності за порушення суверенітету, але, враховуючи наявний збройний конфлікт, виникає

питання, яке виходить за межі даного дослідження – чи може заборона застосування сили та інтервенції, а також вимога поважати суверенітет порушуватися воюючими сторонами.

У другій категорії кібератак, присвоєних Головному розвідувальному управлінню РФ, міститься кібератака проти Всесвітнього антидопінгового агентства (ВАДА), в результаті якої були оприлюднені конфіденційні медичні справи ряду міжнародних спортсменів. ВАДА публічно заявила, що поширені дані було отримано шляхом зламу її антидопінгової системи адміністрування та управління.

За прикладом своїх партнерів у Сполученому Королівстві, міністерство закордонних справ Канади опублікувало заяву щодо відповідальності ГРУ [221]. Але, на відміну від заяви Великобританії, заява Канади, на території якої знаходиться штаб-квартира ВАДА, звучить досить узгоджено із внутрішньою позицією держави щодо застосування міжнародного права в кіберпросторі, оскільки Уряд Канади не висловлює заперечень щодо того, що принцип суверенної рівності держав є нормою, що покладає на державу конкретні зобов’язання.

Аналогічним чином міністр оборони Нідерландів публічно атрибутував кібероперацію ГУ/ГРУ, спрямовану проти Організації із заборони хімічної зброї, яка базується в Нідерландах, зауваживши, що ця кібероперація ГУ/ГРУ підриває міжнародне верховенство права. На своєму офіційному веб-сайті міністерство оборони досить детально описало те, як їм вдалося зірвати кібероперацію, яка могла б скомпрометувати висновки щодо Солсберівської атаки (отруєння Сергія Скрипаля речовинами нервово-паралітичної дії сімейства «Новичок»). Служба розвідки та безпеки Нідерландів не тільки зірвала операцію ГУ/ГРУ, але й випроводили їх з країни. Наявна інформація щодо їх переміщення напередодні та спорядження, яке активно використовувалося проти Бразилії, Швейцарії та Малайзії, дозволили з впевненістю встановити, що агенти ГУ/ГРУ перебували в Нідерландах з ціллю виконання вказівки Уряду РФ [172], а не з метою просто провести в Нідерландах вікенд.

Зауважимо, що в офіційному листі міністерства безпеки, міністерства іноземних справ та міністерства юстиції до Палати представників Нідерландів відсутнє посилання на те, що Російська Федерація порушила суверенітет Нідерландів [104]. Разом з тим, відповідно до Талліннського керівництва, здійснення кібероперацій органами держави або особами, поведінка яких може атрибутуватися державі, що перебувають на території іншої держави, проти держави або утворених там осіб є порушення суверенітету цієї держави. В керівництві надається приклад, коли агент однієї держави використовує флеш-накопичувач USB для введення шкідливого програмного забезпечення в кіберінфраструктуру, розташовану в іншій державі. На думку експертів, такі дії порушують суверенітет держави [209, с. 19].

Оскільки агенти ГРУ намагалися зламати мережу Wi-Fi задля проникнення в мережу Організації із заборони хімічної зброї, така поведінка цілком справедливо може розглядатися в якості проникнення в кіберінфраструктуру Нідерландів, а отже, – становити порушення суверенітету. Такий висновок випливає із спільної статті професора Університету Редінга М. Шмітта, що є основним розробником та автором Талліннського керівництва, та підполковника Дж. Біллера Центру вивчення міжнародного права Військово-морського коледжу США [244].

Попри це, офіційна позиція Нідерландів полягає в тому, що поведінка ГУ/ГРУ розцінюється як «підрив цілісності міжнародної організації». Також зазначається, що «як приймаюча країна, Нідерланди несуть особливу відповідальність за те, щоб міжнародні організації могли виконувати свої обов’язки як вільно, так і безпечно» [104]. З цього випливає, що мова йде про порушення норм дипломатичного права міжнародних організацій, а не суверенітету Нідерландів. Хоча, зважаючи на те, що ВАДА не має власної кібернетичної інфраструктури, а використовує інфраструктуру держави, на території якої перебуває, вважаємо, що Нідерланди мали право кваліфікувати такі дії як порушення власного суверенітету.

Чимало можуть сказати кібератаки проти приватних осіб. Зокрема, існуючі підходи свідчить про те, що такі атаки не розглядаються в якості порушення норм міжнародного права. Так, наприклад, Великобританія та США не згадували про порушення норм міжнародного права щодо кампанії цільового фішингу, спрямованої проти приватних університетів, приватних компанії та неурядових організацій, яку ці держави пов'язали з Іраном в березні 2018 року [220]. Фактично уряди двох держав розглядали кіберпроникнення як злочинну діяльність відповідно до свого внутрішнього законодавства, тому США висунули звинувачення проти дев'яти іранців, які діяли в ім'я Корпусу вартових ісламської революції [175]. Такі заяви проводять кордон між діяльністю, яка впливає на здатність держави забезпечувати нормальне функціонування своїх «систем» (наприклад, функціонування парламенту; фінансового сектору; енергетики; транспорту) та діяльністю, спрямованою на забезпечення інтересів приватних осіб або приватних компаній.

Принципу розмежування такої діяльності також слідує Європейський Союз, що випливає із прийнятого рішення про застосування обмежувальних заходів у випадку кібератак, що загрожують ЄС або його країнам-членам. В статті 4, де міститься перелік кібератак, які розглядаються в якості загроз та підпадають під сферу дії рішення Ради ЄС згадуються кібератаки спрямовані проти: 1) критичної інфраструктури; 2) сфер, що забезпечують соціальну та / або економічну діяльність; 3) критичних функцій держави; 4) зберігання або обробки секретної інформації; 5) урядових груп реагування на надзвичайні ситуації [76]. Відтак, кібератаки, що спрямовані проти приватних індивідів та компаній, виключаються, – акцент робиться на цілих секторах.

В своїх заявах держави також згадують різні варіанти реагування на поведінку іншої держави в кіберпросторі, які міжнародне право їм надає. Варіанти, доступні в конкретному випадку, залежать від конкретних обставин. Різні форми *opinio juris* свідчать про те, що держави, в разі необхідності, можуть вдаватися до реторсій, контрзаходів, самооборони та застосування принципу необхідності (як для підстави, що виправдовує загалом неправомірні дії).

Стаття 51 Статуту ООН гарантує невід'ємне право держав на самооборону. В своїх документах, що містять правову позицію, держави беззаперечно підтримують застосовність даного права в кіберконтексті. Щоправда, думки розходяться щодо того, коли його можна застосувати, та чи існує в кібердомені право на превентивну самооборону чи самооборону на випередження. Так, наприклад, аналізуючи позицію Великобританії, стає очевидним, що держава не виключає використання права на самооборону на випередження, зазначаючи, що «кібероперації, що призводять до або представляють безпосередню загрозу смерті та знищення в масштабі, еквівалентному збройному нападу, породжуватимуть невід'ємне право вживати заходів для самооборони, як це визнано у статті 51 Статуту ООН» [91]. Тобто, така позиція є посиланням на тест, розроблений у справі про судно «Caroline» (Великобританія проти США), де серед критеріїв права на самозахист вказувалась необхідність, пропорційність і невідкладність [133, с. 921-925]. Зазначимо, що підхід Міжнародного Суду ООН до вирішення даної справи і сьогодні знаходить критику серед противників концепції превентивної самооборони, які стверджують, що стаття 51 Статуту ООН не передбачає превентивну самооборону чи самооборону на випередження.

Що ж до інших держав, то їх позиція також не виключає можливість застосування концепції превентивної самооборони або самооборони на випередження. Так, наприклад, Франція висловлює свою рішучу позицію щодо застосування концепцій самооборони на випередження (*pre-emptive*) та/або колективного реагування (відповіді), що передбачається інструментами кібердипломатії ЄС, але не визнає превентивну самооборону [123, с. 9].

На увагу заслуговує позиція Нідерландів, яка містить, чи не найжорсткіші умови, що мають бути виконані до того, як держава вдасться до реалізації свого права на самооборону після атрибуції кібератаки. Так, Нідерланди встановили досить високий поріг для характеристики кібератаки в якості збройної атаки. Лише серйозна, організована кібератака проти основних функцій держави може кваліфікуватися як «збройна атака» у значенні статті 51 Статуту ООН, якщо така операція могла привести або призвела до серйозних порушень функціонування

держави або серйозних і довготривалих наслідків для стабільності держави. Для прикладу, кібератака спрямована проти всієї фінансової системи або така, що перешкоджає уряду виконувати важливі завдання (охорона навколишнього середовища, оподаткування) буде розцінюватися в якості збройного нападу, а отже, наділятиме державу правом на самозахист [173, с. 23].

З ціллю припинення міжнародно-протиправного діяння держави можуть вдаватися до реторсій. В цілому аналіз *opinio juris* свідчить про відсутність модифікації основних правил щодо їх застосування. Держави мають право на свій розсуд обирати вид реторсії, який хоч і є недружнім, не становить порушення міжнародного права. Окрім визнання дипломата персоною *non grata*, застосування економічних чи інших заходів впливу, держави також можуть обмежити чи закрити доступ до своєї цифрової інфраструктури (за умови відсутності договірних зобов'язань щодо надання спільного доступу на території двох країн).

На відміну від реторсій, певні процедурні правила щодо застосування контрзаходів, швидше за все, потребуватимуть коригування, як влучно підкреслив Уряд Фінляндії. Так, наприклад, атрибуція зловмисної кібероперації можлива лише після того, як вона завершена (на практиці потрібен час для розслідування кіберінциденту та ідентифікації відповідальних осіб), тоді як контрзаходи, як правило, слід вживати, поки триває міжнародно-протиправне діяння [119, с. 5]. Виділяється і позиція Німеччини щодо контрзаходів, яка наразі єдина виразила публічну підтримку Правилу 20 Талліннського керівництва в своїй офіційній позиції від березня 2021 року, зазначивши, що у випадку порушень, які пов'язанні чи не пов'язані з кіберпростором, держави можуть вдаватися як до звичайних контрзаходів, так і до кіберконтрзаходів [230, с. 13].

Таким чином, аналіз наявних форм *opinio juris* (заяв, декларацій, воєнних стратегій, доктрин тощо), з одного боку, свідчить про загальний консенсус щодо застосування міжнародного права в кіберпросторі, а з іншого – про різне розуміння того, які норми міжнародного права застосовуються до кібератак, як та за яких умов.

Зважаючи на постійне збільшення кібератак, зокрема проти об’єктів критичної інфраструктури, що забезпечують нормальне функціонування держави та суспільства, виникає гостра необхідність в узгодженні позицій з практикою. Лише нормативна чіткість офіційних позицій здатна посилити стійкість та мінімізувати ескалацію кібернетичних атак шляхом формування звичаєвих норм міжнародного права.

Наразі наявні позиції держав свідчать про формування певних політичних блоків держав, які намагаються пріоритезувати власні інтереси в питаннях, пов’язаних з кіберпростором. Тому на практиці виходить, що позиція держави щодо застосування конкретних принципів та норм міжнародного права в кіберпросторі визначається політичними інтересами держави (наприклад, позиція Росії та Китаю щодо неможливості застосування норм міжнародного гуманітарного права в кіберпросторі).

Встановлено також, що практика в деяких випадках не узгодження з офіційною позицією держави (позиція Великобританії щодо абстрактного характеру принципу суверенної рівності держав та заяви про серйозні порушення міжнародного права в силу порушення суверенітету держав).

Попри те, що існують норми, застосування яких в кіберпросторі викликає низку дискусій серед держав (принцип суверенної рівності, заборони інтервенції та погрози чи застосування сили), уже зараз можна говорити про формування певного консенсусу (зокрема, щодо заходів реагування на кібератаку).

Нарешті, держави в своїх позиціях не оминули увагою питання застосування норм звичаєвого права щодо атрибуції до кібератак. Швейцарія у своїй заяві підкреслила, що процес атрибуції кібератак є цілісним, міждисциплінарним процесом, та з ціллю ідентифікації держави-правопорушниці має включати оцінку технічних та юридичних аспектів. Для реалізації поставленого завдання швейцарський уряд передбачає використання всього спектру інформації отриманої в результаті розвідувальної діяльності та врахування геополітичного контексту.

Важливо, що, хоча держава не згадує оцінку політичних індикаторів, а лише технічних та юридичних аспектів, згадка геополітичного контексту все ж таки свідчить про наміри брати до уваги релевантні політичні індикатори. В заяві також використовується поняття «кіберінцидент», яке не обов'язково є кібератакою, а може мати ненавмисний характер у зв'язку з, наприклад, людським фактором. Швейцарія також залишає на розсуд держави питання щодо того як реагувати на «кіберінціденти». Зокрема, держава може прийняти рішення про застосування політичних заходів, здійснити або не здійснити публічну атрибуцію. Що стосується підстав для атрибуції міжнародно-протиправного діяння, то вони не містять новел та дублюють ті, що виокремлені в Статтях про відповідальність держав [226, с. 5].

Аналогічним чином Австралія виразила свою готовність атрибутувати незаконні кібератаки відповідно до звичаєвих норм міжнародного права відповідальності держав. Тобто, для атрибуції потрібно, щоб діяльність здійснювалась органом держави; фізичними або юридичними особами, які здійснюють елементи урядових повноважень, або недержавними суб'єктами, які діють під керівництвом або під контролем держави [47].

В позиції Естонії атрибуція розглядається як політичне рішення, яке може бути прийнято як індивідуально, так і колективно. Важливо також те, що Естонія визнає, що, залежно від конкретної ситуації, окрім технічної інформації, процес атрибуції може включати оцінку політичного та економічного контексту, «усталені моделі поведінки», іншу відповідну інформацію та показники [225].

Загально прийнятим в позиції держав є те, що рішення про атрибуцію поведінки державі належить постраждалій державі, і відповідно до міжнародного права на цю державу не покладається обов'язок розкривати інформацію, на основі якої було прийнято рішення про атрибуцію кібератаки [226, с. 6]. До такого ж висновку прийшли експерти Талліннського керівництва після оцінки існуючої практики та *opinio juris* держав.

Загалом такий висновок був досить очікуваним, адже держави максимально намагаються тримати у таємниці свої кіберспроможності, зокрема

ті, що пов’язані із роботою розвідки. Відтак, наразі неможливо вивести звичаєву норму, яка б зобов’язувала державу оприлюднити докази, на які ця держава покладалась в процесі здійснення атрибуції кібератаки конкретній державі. Разом із тим, неможливо не погодитися з позицією експертів Талліннського керівництва щодо того, що представлення таких доказів є розумним рішенням задля уникнення політичної та іншої напруженості [209, с. 83].

Проте твердження про здійснення протиправної кібероперації державою має бути обґрунтованими та розумним. Держави повинні усвідомлювати, що можуть стати жертвами спуфінгу – маскування однієї особи або програми під іншу шляхом фальсифікації даних. У випадку помилкової атрибуції та невиправданих дій (наприклад, застосування сили) держави нестимуть відповідальність за останні, незважаючи на те, що стали жертвами спуфінгу.

Застосування техніки спуфінг є досить поширеним і особливо знайомим Україні. Так, у 2013 році внаслідок шкідливих кібероперацій здійснено спробу видати себе за Центр передового досвіду співробітництва з кіберзахисту НАТО і створити враження того, що Центр відповідальний за зіпсовані урядові сайти України. Звичайно за кібероперацією не стояв Центр НАТО і достатньо було використати цей принцип розумності в атрибуції кібероперацій. Цікаво те, що майже одразу відповідальні за кібероперацію особи спрямовували свої зусилля проти веб-сайтів вище згадуваного Центру НАТО, Збройних сил Естонії та військових сил інших держав НАТО, сфальсифікувавши вихідні IP-адреси так, щоб здавалося, ніби український уряд стояв за ними [209, с. 83].[1]

Таким чином, аналіз *opinio juris* свідчить про певний рівень консенсусу щодо застосування міжнародного права в кіберпросторі та наявність розбіжностей в інтерпретації та застосуванні конкретних норм і принципів міжнародного права. Такі розбіжності, зокрема щодо принципу суверенної рівності держав, потребують уваги та розгляду на міжнародному рівні. Що

[1] Наукові результати, представлені в Розділі 1, опубліковані в одному із розділів колективної монографії : Кібератаки та міжнародне право: природа та аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі : колект. моногр. «Проблеми публічного та приватного права» / за заг. ред. Н. В. Мішиної. 2021. С. 309-342.

стосується атрибуції, то різні форми *opinio juris* демонструють досить послідовний підхід, який, з одного боку, враховує положення про атрибуцію поведінки державі, що містяться в Статтях про відповідальність держав за міжнародно-протиправні діяння 2001 року, з іншого – особливість кібератак та кіберпростору, де технічні та політичні індикатори в значній мірі взаємокомпенсуючі.

Висновки до першого розділу

1. Стрімкий розвиток інформаційно-комунікаційних технологій сприяв виникненню кіберпростору, який є віртуальним інформаційно-комунікаційним простором. Саме кіберпростір є середовищем реалізації кібератак та забезпечує їх необхідними засобами здійснення – технічними можливостями кіберпростору. Поняття кіберпростору охоплює середовище, утворене фізичними та нефізичними компонентами для зберігання, модифікації та обміну даними за допомогою комп'ютерних мереж.

Він складається з трьох різних рівнів (пластів): фізичного, логічного та соціального – в межах яких або проти яких можуть здійснюватися кібератаки. Фізичний рівень кіберпростору складається з фізичних компонентів мережі, а також географічної складової. Логічний рівень відповідає за маршрутизацію пакетів даних до їх кінцевих пунктів призначення, а відтак, включає системи доменних імен, Інтернет-протоколів, браузерів, програмного забезпечення, через які передаються данні. Соціальний рівень охоплює всіх акторів, що беруть участь у кіберактивності. При цьому, компоненти кожного рівня, як правило, знаходяться на території конкретних держав.

2. Кібератака представляє собою кібероперацію, яка може мати наступальний чи оборонний характер та цілком очікувано може призвести до завдання трав чи смерті осіб або шкоди чи знищення об'єктів (маніпуляції чи знищення даних або коду в комп'ютерній системі для управління або відключення електромережі тощо). Зважаючи на природу кіберпростору, який є середовищем реалізації кібератак, останні можна легко замаскувати, що надає можливість зберегти анонімність і ускладнює процес атрибуції. Крім того, особливість кібератак проявляється в тому, що вторинні чи навіть третинні наслідки кібератак є більш значимими та серйозними, ніж їх первинні наслідки, що значно виділяє кібератаки на фоні звичайних атак.

3. Наразі відсутнє *lex specialis*, яке містило б спеціальне регулювання кібератак. Експерти Талліннського керівництва зробили значний внесок в

розуміння того, як міжнародне право застосовується до кіберпростору, але керівництву бракує юридично обов'язкової сили, а також воно критикується в силу того, що участь в його розробці брали виключно експерти НАТО. Водночас, Група урядових експертів ООН відзначила, що міжнародне право, та зокрема Статут Організації Об'єднаних Націй, застосовується у межах діяльності, пов'язаної з використанням ІКТ, а також підтвердила юрисдикцію держав над ІКТ-інфраструктурою на їх території.

Окрім загального міжнародного права до кібератак можуть застосовуватись спеціальні режими. Так, наприклад, право застосування сили (*jus ad bellum)* застосовуватиметься до кібератак, які досягають рівня збройного нападу (атаки) та наділяють державу правом на самооборону; міжнародне гуманітарне право застосовуватиметься до кібератак, які можна кваліфікувати як збройну атаку, що здійснені в ході збройного конфлікту або пов'язані з ним, та активують *jus in bello*, не дивлячись на заперечення з боку низки держав.

4. Для здійснення атрибуції кібератак потрібно чітко розмежовувати дії, які порушують міжнародно-правові зобов'язання від тих, які їх не порушують. Щодо кіберпростору відсутнє *lex specialis*, тому виникає необхідність у встановленні того, як існуючі міжнародні зобов'язання повинні тлумачитись та застосовуватись до конкретних кібероперації. *Opinio juris,* як правило, може компенсувати недостатньо розвинену або непослідовну практику держав щодо формування міжнародних звичаїв. Заяви, декларації та воєнні доктрини мають орієнтуючий, а не визначальний характер, але на стадії формування норм, що діють в кіберпросторі, аналіз *opinio juris* дозволяє встановити «межі» відповідальної поведінки в кіберпросторі, розуміння того, якими держави бачать існуючі зобов'язання та чи узгоджується їх позиція з наявною практикою.

5. Позиції держав, які опублікували офіційні заяви щодо того, як міжнародне право застосовується до кіберпростору, свідчать про загальну підтримку ідеї того, що воно застосовується. Коли ж мова йде про конкретні зобов'язання, держави не завжди спроможні виробити чітку позицію. В першу чергу привертає позиція щодо принципу суверенітету. Більшість держав

характеризують суверенітет як принцип і норму міжнародного права (наприклад, Німеччина, Франція, Чехія, Фінляндія, Іран, Нідерланди, Болівія, Китай, Гватемала, Гайана, Нова Зеландія, Республіка Корея та Швейцарія, а також держави-члени НАТО, за винятком Великобританії), який порушується у випадку проникнення однієї держави в кіберінфраструктуру іншої. Але попри фундаментальне значення цього принципу, позиція уряду Великобританії полягає в тому, що не існує такої норми в межах сучасного міжнародного права. Ізраїль та Сполучені Штати досі остаточно не визначились. Разом з тим, позиція Великобританії йде врозріз з практикою, оскільки Великобританія намагається захищати те, що не визнає в якості юридично обов'язкового зобов'язання.

6. Всі держави, які висловили свою офіційну позицію щодо застосування міжнародного права у кіберпросторі, зійшлись на тому, що принцип заборони інтервенції безсумнівно застосовується. Серед основних прикладів інтервенції, більшість держав згадує інтервенцію у виборчий процес, яка є втручанням у внутрішні справи держави та характеризується наявністю примусу (маніпулювання результатами голосування), втручання у фундаментальну діяльність парламенту або стабільність фінансових систем держави (Франція, США, Німеччина, Ізраїль, Австралія). Німеччина та Іран зберігають за собою право розглядати дезінформацію та політичні інтриги відповідно в якості порушення даного принципу.

7. В своїх заявах держави також підтверджують різні варіанти реагування на поведінку іноземної держави в кіберпросторі. Варіанти, доступні після атрибуції кібератак, залежать від конкретних обставин. Загалом різні форми *opinio juris* свідчать про те, що держави, в разі необхідності, можуть вдаватися до реторсій, контрзаходів, самооборони та застосування принципу необхідності (як для підстави, що виправдовує загалом неправомірні дії). Відтак, наслідки кібератаки впливатимуть на процес атрибуції та вибір форм та видів відповідальності.

8. Існуючі підходи держав також свідчать про те, що кібератаки проти приватних осіб не розглядаються в якості порушення норм міжнародного права

та не вимагають юридичної атрибуції. Уряди розглядають такі дії як злочинну діяльність відповідно до свого внутрішнього законодавства. Проте заяви проводять певну лінію розмежування між діяльністю, яка впливає на здатність держави забезпечувати нормальне функціонування своїх «систем» (наприклад, функціонування парламенту; фінансового сектору; енергетики; транспорту) та діяльністю, спрямованою на забезпечення інтересів приватних осіб або приватних компаній. Якщо кібератака спрямована проти, між іншим, критичної інфраструктури, вона буде розглядатись в якості міжнародно-протиправного діяння, незалежно від форми власності.

9. Держави в своїх позиціях не оминули увагою питання застосування норм звичаєвого права щодо атрибуції до кібератак. Аналіз свідчить про застосування традиційних підстав атрибуції поведінки державі. Держави з незначними змінами фактично дублюють стандарти атрибуції, що виокремлені в Статтях про відповідальність держав за міжнародно-протиправні діяння 2001 року.

Тобто, відповідно до офіційної позиції держав, для атрибуції потрібно, щоб діяльність здійснювалась органом держави; фізичними або юридичними особами, які здійснюють елементи урядових повноважень, або недержавними суб’єктами, які діють під керівництвом або під контролем держави. Разом з тим, більшість держав, що виразила офіційну позицію щодо застосування норм міжнародного права в кіберпросторі, зійшлась на необхідності здійснення технічної та політичної атрибуції, яка у випадку з кібератаками передує здійсненню юридичній атрибуції.

РОЗДІЛ 2. ОСОБЛИВОСТІ АТРИБУЦІЇ КІБЕРАТАК ПРОТИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

2.1. Встановлення змісту поняття «критична інфраструктура»

Переходячи до практики атрибуції кібератак проти об'єктів критичної інфраструктури, спершу потрібно розібратись з нормативним наповненням поняття «критична інфраструктура». Оскільки конвенційне поняття в міжнародному праві відсутнє, логічно звернутись до національного законодавства держав, що містить дефініцію чи перелік об'єктів та/або секторів критичної інфраструктури.

В процесі встановлення змісту поняття «критична інфраструктура», яке знаходиться в центрі даного підрозділу, будуть також використовуватися такі суміжні поняття як «сектор (підсектор) критичної інфраструктури» та «об'єкти критичної інфраструктури». Одразу відзначимо, що залежно від країни, законодавство якої аналізується, згадка про «об'єкти критичної інфраструктури» або «сектори (підсектори) критичної інфраструктури» не завжди присутня. Іноді використовується виключно поняття «критична інфраструктура», яке включає сектори та об'єкти. Що ж стосується поняття «сектори (підсектори) критичної інфраструктури», то в цілому воно є збірним та представляє «сукупність об'єктів критичної інфраструктури, які належать до одного сектору (підсектору) економіки та/або мають спільну функціональну спрямованість» [6, п. 2].

Загалом поняття «критична інфраструктура» є відносно новим, і наразі його можна знайти далеко не в кожному національному законодавстві країн світу. Якщо ж воно згадується, то, як правило, є досить неточним та потребує вдосконалення. Водночас загрози, що існують для систем та активів, які забезпечують національну безпеку, економічний та соціальний добробут, існували задовго до появи цього поняття в офіційних документах. Так, наприклад, ще в Стародавній Греції спартанський полководець Лісандр захопив протоку Геллеспонт (Дарданелли), через яку здійснювався імпорт зерна до Афін. Таким чином Лісанд хотів примусити місто здатися, спровокувавши серйозний

голод. В результаті цього ослаблені афіняни зазнали поразки при Егоспотамах, попри всі намагання дати відсіч [3, с. 329; 189, с. 10-29]. З більш пізніх прикладів можна виділити прийняту у 1943 році Директиву Касабланки, що адресувалась командирам повітряних сил Великобританії та США щодо управління діяльністю британського та американського командування бомбардувальників з території Великобританії.

У пункті 1 Директиви зазначалося: «Вашим Першочерговим завданням буде поступове знищення та дислокація німецької військової, промислової та економічної системи, а також підрив морального духу німецького народу до такої міри, що здатність до збройного опору фатально ослабне» [122]. Крім того, згадувалися конкретні об'єкти для здійснення потенційних атак, а саме – німецькі підводні будівельні арсенали; німецька авіаційна промисловість; транспортування; нафтові заводи; інші об'єкти ворожої воєнної промисловості [122, п. 2]. Ці приклади демонструють, що атаки проти критичної інфраструктури не є новим феноменом, хоча й з виникненням кіберпростору вони стали більш прогресивними та витонченими.

Існує ряд причин, чому критична інфраструктура, яка фактично забезпечує життєдіяльність держави та є її кровоносною системою, все частіше стає ціллю кібератак. По-перше, це пов'язано з порівняно незначними ресурсами, необхідними для нанесення атаки. Ще в VI ст. до н.е. китайський стратег та мислитель Сунь-цзи писав, що найвищим мистецтвом війни є перемога над ворогом без боротьби. І дійсно, кібератаки відкривають нові можливості перед державами, адже тепер навіть малі держави, які не володіють значними ресурсами та воєнний потенціал яких є порівняно незначним, мають всі шанси на те, щоб стати світовим центром сили при високому розвитку технологій та наявності необхідних людських ресурсів.

Використання кібератак відкриває для держав нові горизонти, адже навіть такі центри сили в міжнародних відносинах як США, Росія, Китай стають уразливими та слабкими внаслідок своєї залежності від технологій, тому змушені постійно нарощувати свої кіберспроможності. Отже, кібератаки

надають всім державам, незалежно від їх розміру, національних багатств та ресурсів, місце за столом наддержав [249].

Відповідно до дослідження Міжнародного інституту стратегічних досліджень від 21 червня 2021 року є три рівні розвитку кіберспроможностей держав. Це дослідження в повній мірі підкреслює взаємозв'язок між нарощенням кіберспроможностей та захистом критичної інфраструктури. Так, наприклад, Сполучені Штати Америки, наступальні кіберспроможності яких розвинені краще, ніж у будь-якої іншої країни, готові при необхідності вдатися до використання таких спроможностей проти національної критичної інфраструктури інших держав [92, с. 22]. Окрім США, значний акцент на захисті критичної інфраструктури та реагуванні на кібератаки проти критично важливих об'єктів інфраструктури робиться такими країнами-лідерами як Канада, Австралія, Японія, Індія та В'єтнам [92, с. 42, 50, 80, 137, 162].

Нарощування кіберпроможностей не є випадковим: саме об'єкти критичної інфраструктури забезпечують нормальне функціонування сучасних держав. Якщо в діяльності цих життєвоважливих об'єктів виникне збій або основні елементи інфраструктури перестануть функціонувати, вплив поширитися і на інші сектори в силу тісної взаємозалежності. Саме тому на практиці об'єкти критичної інфраструктури частіше всього стають ціллю кібератак.

Крім того, цілком вірогідним є завдання транскордонної шкоди іншим державам у випадку кібератак проти критично важливих об'єктів інфраструктури. Ризик такої шкоди підвищується, коли мова йде про вплив на віртуальні системи секторів критичної інфраструктури. Все це свідчить про те, що кібератаки проти об'єктів критичної структури мають високий потенціал для того, щоб забезпечити «перемогу без боротьби». І тому це ключова причина, яка підвищує привабливість кібератак, направлених проти об'єктів критичної інфраструктури держави.

По-друге, кібератаки тривалий час гарантували анонімність та відсутність відповідальності в кіберпросторі. З одного боку, досить непросто прослідкувати

хто і як здійснив певну кібератаку, хоча це завдання не є недосяжним. З іншого боку, відповідно до рішення у справі Нікарагуа лише ефективний контроль держави над операцією передбачає міжнародно-правову відповідальність держав за дії проксі [62, п. 105-115], а ось підтримка та фінансування приватних осіб чи груп, які були виконавцями, не що інше як здійснення загального контролю [191, п. 131]. Виходить, що постраждалі держави та міжнародна спільнота в цілому не можуть притягнути державу до відповідальності за кібератаки проти об'єктів критичної інфраструктури. Більш того, ситуація часто ускладняється відсутністю конвенційного поняття «критична інфраструктура».

На перший погляд може здатися, що з позиції середньостатичної особи («reasonable person») можна без проблем визначити відноситься об'єкт до критичної інфраструктури чи ні. Водночас, все не так просто з позиції міжнародного права, яке у випадку з атрибуцією кібератак проти об'єктів критичної інфраструктури, в першу чергу, зіштовхнеться з категоризацією таких об'єктів як критичних відповідно до національного права. Забігаючи наперед зазначимо, що відповідно до позиції Групи урядових експертів, представленої в Доповіді від 14 липня 2021 року віднесення об'єктів до критичної інфраструктури залишається на розсуд держав і має ґрунтуватися на національних пріоритетах [194, с. 15]. Саме цей висновок змушує звернути увагу на національне законодавство і оцінити, наскільки адекватно та зважено національні законодавці підходять до визначення змісту поняття «критична інфраструктура» та категоризації об'єктів і/чи секторів критичної інфраструктури.

Вважається, що вперше концепцію критичної інфраструктури було представлено у Виконавчому указі № 13010 Президента США Білла Клінтона [114], прийняттю якого частково послужив теракт 1995 року в Оклахома-Сіті. До подій 11 вересня 2001 року він був наймасштабнішим в історії США. Вибух заповненої вибухівкою вантажівки біля восьмиповерхової урядової будівлі призвів до гибелі 168 осіб, близько 650 осіб зазнали трав внаслідок руйнації, а також постраждало близько 300 будівель, що знаходились у безпосередній

близькості [179]. Уряд США також засвідчив всеосяжні наслідки цього теракту – від втрат відділу оплати праці, спустошення крила ФБР до шкоди завданої іншим державним та приватним установам далеко за межами відповідного штату [58, с. vii].

У Виконавчому указі зазначалося, що критична інфраструктури – це системи, які є «настільки життєвонеобхідними, що їх непрацездатність або руйнування матимуть послаблюючий вплив на оборону або економічну безпеку Сполучених Штатів». Також було ідентифіковано вісім секторів, які, на думку Уряду, підпадають під відповідну характеристику, а саме: телекомунікація; електроенергія; газ і нафта; банківська справа та фінанси; транспорт; постачання води; діяльність екстрених служб; і продовжуваність діяльності уряду [114].

Після 11 вересня 2001 року визначення критичної інфраструктури у законодавстві США зазнає модифікації в силу розширення критеріїв критичності. В прийнятому 26 жовтня 2001 року «Патріотичному Акті» згадується не лише важливість інфраструктури для національної оборони та економічної безпеки, а й для охорони здоров'я і безпеки громадськості [247, с. 130].

Важливо, що до жовтня 2001 року ніхто не включав ядерну чи хімічну індустрію в перелік критичної інфраструктури США. Ці сектори не були стратегічно важливими для національної безпеки чи економіки, але вірогідність терористичних атак проти об'єктів хімічної та ядерної індустрій, як видається, змусила задуматись над потенційно високим числом жертв, що можна порівняти, наприклад, із ситуацією застосування зброї масового знищення. Отже, трагедія 11 вересня послужила передумовою для включення критерію «життєвонеобхідні для охорони здоров'я і безпеки громадськості».

Аналіз Директиви 2003 року щодо захисту критичної інфраструктури також свідчить про виділення такого критерію як «громадська мораль і впевненість в національних економічних та політичних інститутах». Відповідно, було додано ще два сектори критичної інфраструктури – національні монументи та символи і заходи спеціальної національної оборони (заходи національного або

міжнародного значення, які можуть бути ціллю потенційної терористичної діяльності або іншої кримінальної діяльності) [135]. Наразі сектор національних монументів та символів разом із підсектором освітніх закладів є підсекторами урядового сектору [128, с. 4, 10].

Загалом аналіз розробки поняття «критична інфраструктура» в історичному розрізі свідчить про те, що класифікація активів та систем в якості таких, що в ходять в поняття критичної інфраструктури США є досить динамічним процесом. Востаннє Сполучені Штати Америки розширили перелік секторів критичної інфраструктури у 2015 році до 16. Зокрема, наразі серед секторів критичної інфраструктури 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 бази промислової оборони тощо. 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 [233, с. 10-12].[2]

На нашу думку, такий підхід видається не виправдано інклюзивним в контексті США. Так, наприклад, в межах сектору комерційних об'єктів виділено 8 підсекторів, а саме: 1) заклади розваг та ЗМІ (наприклад, кіностудії, радіомовлення); 2) гральні заклади (наприклад, казино); 3) заклади тимчасового перебування (готелі, мотелі, конференц-центри); 4) заходи на свіжому повітрі (наприклад, тематичні та розважальні парки, ярмарки, кемпінги, паради); 5) місця масових зібрань (арени, стадіони, акваріуми, зоопарки, музеї, конференц-центри); 6) нерухомість (офісні та багатоквартирні будинки, ОСББ, об'єкти змішаного призначення, об'єкти індивідуального зберігання);

[2] Наукові результати, представлені в підрозділі 3.2, попередньо оприлюднено в наступній публікації: До питання про відсутність поняття «критична інфраструктура» в міжнародному праві. Матеріали міжнародної конференції : Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (21 травня 2021 року). Одеса, 2021. С. 359-362.

7) роздрібна торгівля (торгові центри та райони); 8) спортивні ліги (професійні спортивні ліги та федерації).

Як видається, комерційний сектор не є настільки критично важливим для США, щоб класифікувати його в якості критичної інфраструктури. Звичайно, ніщо не може обмежити право США класифікувати відповідні сектори як критичні, користуючись дискрецією, яка випливає із суверенітету держави. Разом з тим, жодна інша держава світу не розглядає згаданий сектор в якості критичного, що може свідчити про необхідність вироблення більш стриманого підходу до критичної інфраструктури, який би не включав всю наявну в державі інфраструктуру. Разом з тим, ми не виключаємо можливість категоризації комерційних об'єктів як критично важливих, проте така оцінка має робитися з урахуванням особливостей та рівня розвитку держав. Так, наприклад, якщо економіка малої острівної держави в значній мірі опирається на діяльність сектору туризму, а знищення певних комерційних об'єктів призведе до значних економічних втрат для держави та громадян, то такі об'єкти, в принципі, на наш погляд, можуть бути класифіковані як об'єкти критичної інфраструктури держави.

В законодавстві України поняття критична інфраструктура тривалий час не визначалося, що зумовлювало правову невизначеність в ситуаціях, коли це поняття згадувалося. До прикладу, рішення Ради національної безпеки та оборони від 1 березня 2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» покладало на Міністерство внутрішніх справ України обов'язок забезпечити «посилену охорону об'єктів енергетики та критичної інфраструктури» [28]. Пізніше у рішенні Ради « Про Стратегію національної безпеки України» від 6 травня 2015 року серед актуальних загроз вперше згадувалися загрози безпеці критичної інфраструктури, а також «вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак» [31].

Саме ці рішення послужили поштовхом до встановлення нормативного змісту поняття «критична інфраструктура» в національному законодавстві

України, адже вони вимагали від національних органів здійснення відповідних заходів щодо захисту критичної інфраструктури, ефективність та реалізація яких напряму залежала від розуміння того, що розглядається в якості критичних систем та активів (об'єктів критичної інфраструктури).

Згідно зі Постановою Кабінету Міністрів України № 563 від 23 серпня 2016 р. «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», до об'єктів критичної інфраструктури законодавець відніс «підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення» [26, п. 2]. Такий підхід законодавця демонструє розуміння критичності певних секторів, але, вважаємо, що використання формулювання «підприємств та установ» замість традиційного «систем та активів» є не до кінця продуманим, тому що іноді кібератаки здійснюються саме проти систем чи активів, а не проти підприємств чи установ в цілому.

29 червня 2021 року Верховною Радою України в першому читанні прийнято проект Закону України «Про критичну інфраструктуру». Можна справедливо зазначити, що він є своєрідним проривом в питаннях забезпечення захисту та стійкості об'єктів критичної інфраструктури України. По-перше, визначення поняття «критична інфраструктура» не обмежується згадкою «об'єктів критичної інфраструктури», перелік яких міститься в статті 6 Постанови КМУ «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави». Тобто, критична інфраструктура – це не лише підприємства та установи, а й «системи, їх частини та їх сукупність». По-друге, визначаються категорії критичності, оскільки одні об'єкти є більш критично важливі, ніж інші. По-третє, визначається 18 життєвоважливих функцій та/або послуг, порушення

яких призводить до негативних наслідків для національної безпеки України [27], що слугуватимуть основою для виділення окремих секторів Кабінетом Міністрів України. Останнє є стратегічно вірним напрацювання, оскільки процедура прийняття актів Кабінетом Міністрів України простіша, ніж процедура прийняття (внесення змін) законів Верховною Радою. Тобто, перелік секторів (підсекторів) критичної інфраструктури можна буде швидше та легше сформулювати та за потреби скорегувати.

Що стосується нормативного визначення «критична інфраструктура» в законодавстві інших держав, то загалом прослідковується певна узгодженість у розумінні даного поняття та іноді досить обмежені підходи до виокремлення секторів критичної інфраструктури. Так, зокрема, з 2013 по 2020 роки в законодавстві Туреччини національна критична інфраструктура класифікувалася відповідно до 6 критично важливих секторів, а саме: сектор електронних комунікацій, сектор управління водними ресурсами, сектор енергетики, сектор критично важливих державних служб, сектор транспорту, сектор банків та фінансів [45]. Національна стратегія та план дій з кібербезпеки на 2020-2023 роки в цілому згадує ті самі сектори, проте сектор банків та фінансів тепер називається просто – сектор фінансів [243].

В Бельгії та Сальвадорі критично важливих секторів інфраструктури законодавець визначає лише чотири. Зокрема, в Бельгії до національної критичної інфраструктури зараховується сектор енергетики, транспорту, фінансів та електронних комунікацій [214]. В Сальвадорі їх також чотири, але перелік дещо відмінний, а саме – сектори енергетики, транспорту, водних ресурсів та управління ризиками (стихійні лиха) [186]. В законодавстві Індії [141] та Індонезії [192], серед іншого, критичними для функціонування держав є сектор щодо дослідження та використання космосу та електронний уряд; в той час як в списку секторів критичної інфраструктури Норвегії виділяється супутникова інфраструктура [177].

До критично важливої інфраструктури в Німеччини зараховуються організаційні та фізичні структури та об’єкти у сферах енергопостачання,

інформаційних технологій та телекомунікацій, транспорту, охорони здоров'я, водопостачання, харчування, фінансового та страхового секторів, держави та управління, а також засобів масової інформації та культури [170]. Закон ФРН про IT-безпеку 2.0, що вступив в силу 28 травня 2021 року, свою сферу охоплення поширює не тільки на вказані вище сектори, а й на сектор утилізації комунальних відходів. Таким чином, в недалекому майбутньому перелік секторів критичної інфраструктури імовірно може зазнати змін, поповнившись сектором утилізації комунальних відходів.

Крім того, в цьому Законі представлена нова категорія – компанії, що представляють особливий суспільний інтерес. Дана категорія заслуговує на увагу в силу того, що кібератаки проти таких компаній згадуються поруч із кібератаками проти критичної інфраструктури в позиції Німеччини щодо застосування міжнародного права в кіберпросторі. До таких компаній належать: 1) компанії-виробники озброєння та військової техніки, а також розробники IT-продуктів для обробки секретної державної інформації; 2) найбільші компанії Німеччини (що мають значне економічне значення для держави); 3) хімічні компанії та інші компанії, що підпадають під визначення статті 1 (2) Декрету про небезпечні інциденти [150].

Як видається, таке розмежування двох понять є досить раціональним. В той час як законодавець в США керується максимально інклюзивним підходом до критичної інфраструктури, нівелюючи тим самим закладеною в саме поняття «критичністю», то у Німеччині пішли дещо іншим підходом. Так, компанії, що представляють суспільний інтерес, не стали розглядатися в якості об'єктів критичної інфраструктури, проте для забезпечення їх стійкості та безпеки законодавець розробив окрему категорію.

В березні 2014 року спільний наратив «Формування спільного розуміння критичної інфраструктури» опублікувала група держав «Critical Five», створена у 2012 році. До складу «Critical Five» входять члени державних установ, що відповідають за безпеку та стійкість критичної інфраструктури у Австралії, Канаді, Новій Зеландії, Сполученому Королівстві та США. Для посилення

ефективної взаємодії ці держави спробували виробити спільний підхід. В результаті обговорення їм вдалось виділити 5 секторів, які є критичними в кожній із згаданих держав: комунікації, енергетика; охорона здоров'я та громадське здоров'я; транспорт та водопостачання (включаючи системи стічних та зливових вод). Позиція щодо ще 6 секторів варіювалася залежно від національних інтересів держав. Так, зокрема, в якості сектору критичної інфраструктури також розглядаються:

- сектор банківських та фінансових послуг (крім Нової Зеландії);
- сектор критичного виробництва (в Канаді та США);
- сектор екстрених служб (в Канаді, Великобританії та США);
- сектор продовольства та сільського господарства (крім Нової Зеландії, але у Великобританії згадується тільки продовольство);
- сектор урядування (крім Австралії);
- сектор інформаційних технологій (Канада, Нова Зеландія, США; у Великобританії сектор комунікацій включає радіо- та телерадіомовлення, поштовий зв'язок та телекомунікації) [88, с. 6].

Відтак, незважаючи на те, що поняття та перелік об'єктів критичної інфраструктури варіюється, в цілому можна прослідкувати консенсус між державами щодо важливості певних секторів інфраструктури. Чітко простежуються сектори критичної інфраструктури, які в національному законодавстві згадуються найчастіше, а саме: сектор комунікації, сектор енергетики, урядовий сектор, сектор водопостачання, сектор охорони здоров'я, транспортний сектор та сектор оборони.

Попри консенсус у розумінні поняття «критична інфраструктура», аналіз національного законодавства 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. Тому виходить, що в США 16 секторів критичної інфраструктури, у

Королівстві Нідерланди 12 секторів та 31 підсекторів, в той час як в Бельгії, Сальвадорі та Аргентині – по чотири. На формування переліку об'єктів критичної інфраструктури значно впливають і національні інтереси: наприклад, *inter alia*, для Малі таким пріоритетом є боротьба зі змінами клімату, а для України – оборона України від зовнішнього агресора.

Зазначимо, що вузький підхід держав також не є повністю виправданим. Так, іноді видається за можливе об'єднати дві групи об'єктів критичної структури в одну, щоб уникнути їх «дроблення», але така можливість є не завжди. Наприклад, два відокремлені в національному законодавстві США сектори – систем водопостачання та дамб – можна об'єднати, але з переліку об'єктів критичної інфраструктури України ніяк не можна виокремити демократичні інститути (урядовий сектор). Підхід бельгійського законодавця теж не досить логічний, оскільки він, серед іншого, ігнорує важливість систем водопостачання.

Можна цілком справедливо зробити висновок, що 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 «критична інфраструктура» та необхідність звернення до національного законодавства у випадку серйозних порушень норм міжнародного гуманітарного права чи міжнародного права прав людини.

Цікавим у цьому плані є підхід Франції, що також відображений в проекті Закону України «Про критичну інфраструктуру». Французький законодавець ставлення до критичної інфраструктури визначає через функції певних об'єктів. Так, наприклад, функціонування цих об'єктів має бути пов'язане 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». В цілому визначено 12 секторів, забезпечення

нормального функціонування яких належить до повноважень відповідних міністерств [142, с. 8].

Загалом вважаємо, що критерії, які слугували б визначенню того, яку інфраструктуру слід вважати критичною, повинні бути сформульовані не тільки на рівні країни, а й на рівні регіону. Важливим кроком в цьому напрямку стало прийняття Європейською Радою Директиви 2008/114/ЕС щодо ідентифікації та визначення в якості європейської критичної інфраструктури та оцінки необхідності вдосконалення її захисту від 8 грудня 2008 року. Звісно, Директива поширюється виключно на територію інтеграційного утворення, але все ж сприяє утвердженню підходу до забезпечення стійкості спільної критичної інфраструктури в Європі.

Згідно зі статтею 2(a), під критичною інфраструктурою слід розглядати «активи, систему або їх частину, розташовані в державах-членах, які є необхідними для підтримки життєвоважливих функцій суспільства, здоров'я, безпеки, економічного або соціального благополуччя людей, порушення або знищення яких матиме значний вплив у державі-члені внаслідок нездатності підтримувати ці функцій» [77].

Сфера дії Директиви охоплює не просто критичну інфраструктуру конкретних держав-членів ЄС, а безпосередньо «європейську критичну інфраструктуру». Це означає, що вдосконалення захисту передбачено для тієї інфраструктури, яка розташована в державах-членах та порушення чи знищення якої матиме значний вплив як мінімум на дві держави-члени ЄС [77, ст. 2 (b)].

В ЄС також розроблено наскрізні критерії, що, зокрема, оцінюють наявність та рівень міжсекторальної залежності від інших типів інфраструктури: критерій оцінки кількості потенційних жертв, економічних втрат та соціальних наслідків. Що ж до сфери охоплення, то Директива обмежується двома секторами – енергетики та транспорту, за що піддається серйозній критиці. Крім того, як видається, необхідним є і зміна орієнтирів, які передбачали б не лише захист, а й забезпечення стійкості такої інфраструктури.

Наявні підходи до інфраструктури свідчать про можливість виокремлення не тільки національної, а й транснаціональної (міждержавної) критичної інфраструктури. Практика Європейського Союзу є тому яскравим свідченням. Окрім ЄС, варто також згадати партнерство між США та Канадою, деякі елементи критичної інфраструктури яких є спільними (наприклад, електрична мережа) [61]. Група урядових експертів теж згадує спільну для декількох держав інфраструктуру, зокрема технічну, і наголошує на тому, що така інфраструктура може «мати вирішальне значення для міжнародної торгівлі, фінансових ринків, глобального транспорту, зв'язку, охорони здоров'я або гуманітарної діяльності» [194, с. 15].

Вважаємо, що ідентифікація транснаціональної інфраструктури повинна здійснюватися паралельно ідентифікації національної критичної інфраструктури, і ці об'єкти не потрібно змішувати в одну категорію, оскільки роль об'єктів критичної інфраструктури, що використовується спільно буде значно більшою, ніж тих, що використовуються однією державою. Відтак, атрибуція кібератак проти міждержавних об'єктів критичної інфраструктури матиме колективний характер, як і подальше реагування на кібератаки проти них.

Разом з тим, підхід до категоризації певних об'єктів в якості критичних має бути універсальним. На нашу думку, до змісту поняття «критична інфраструктура» варто підходити через функції. Такий підхід наддасть членам міжнародної спільноти та міжнародним судовим органам гнучкість у випадку кібератаки з руйнівними кінетичними наслідками, а значить – можливість притягнення держави до відповідальності.

Ще одним моментом, який потрібно враховувати при розробці конвенційного поняття «критична інфраструктура» є необхідність розробки критеріїв оцінки критичної важливості (критичності) окремо взятого об'єкта, які б використовувались на міжнародному рівні. До таких критеріїв загалом відносять масштаб потенційних наслідків у випадку порушення нормального функціонування об'єкта критичної інфраструктури, його систем чи активів,

вразливість та взаємозалежність з іншими об’єктами критичної інфраструктури, тривалість та серйозність наслідків, що викликані пошкодженням, знищенням, поломкою або функціональним збоєм .

Доповідь групи урядових експертів від 28 травня 2021 року, що міститься в Резолюції ГА ООН від 14 липня 2021 року, свідчить про неготовність міжнародної спільноти до прийняття єдиного поняття «критична інфраструктура». Так, відповідно до норми 13 (f), «держави не повинні свідомо здійснювати та підтримувати діяльність у сфері ІКТ, якщо така діяльність суперечить їх зобов’язанням з міжнародного права, завдає навмисних збитків критично важливій інфраструктурі або іншим чином перешкоджає використанню та функціонуванню критично важливої інфраструктури для обслуговування населення» [194, с. 15]. В параграфі 44, що містить коментар до даної норми зазначається, питання про віднесення об’єктів чи навіть цілих секторів, що знаходяться в межах юрисдикції держави, до критично важливих, залишається на розсуд кожної держави. Крім того, їх категоризація як критично важливих повинна базуватися на національних пріоритетах і методах віднесення об’єктів до критично важливої інфраструктури.

Такий підхід, хоч і має свої переваги, все ж може створити можливості для зловживань, оскільки занадто інклюзивний підхід держав не буде, серед іншого, відповідати характеристиці критично важливої інфраструктури, що міститься в попередньому параграфі. Зокрема, в параграфі 43 зазначається, що «Їхнє [об’єктів критичної інфраструктури] значне послаблення чи пошкодження може призвести до серйозних людських втрат, а також призвести до помітного впливу на економіку, розвиток, політичне та соціальне функціонування та національну безпеку держави» [194, п. 43].

Мало імовірно, що шкода завдана мотелям, казино, конференц-залам, які категоризовані як об’єкти, що входять в систему критично важливого сектору США, призведе до таких наслідків. Доповідь групи урядових експертів також містить приклади критично важливої інфраструктури. Зокрема, згадується санітарно-медична інфраструктура та об’єкти охорони здоров’я, енергетика,

виробництво електроенергії, водопостачання, санітарія, освіта, комерційні та фінансові послуги, транспорт, телекомунікації та процес проведення виборів.

Підсумовуючи, аналіз національного законодавства держав та інших релевантних документів свідчить про загальний консенсус щодо того, які об'єкти входять в поняття «критична інфраструктура».

Разом з тим, досить інклюзивні чи, навпаки, обмежені підходи до визначення секторів/об'єктів критичної інфраструктури створюють розбіжності, які можна усунути шляхом прийняття конвенційного чи доктринального (розроблено спеціалізованим органом/механізмом) поняття критичної інфраструктури. Таке поняття має опиратися на певні функції (альтернативні та/чи кумулятивні критерії) з ціллю врахування рівня та особливостей розвитку держав і національних пріоритетів держав, а також задля обмеження можливостей для зловживання чи виникнення несприятливого становища для держави.

2.2. Застосування звичаєвих правил атрибуції міжнародно-протиправних діянь до кібератак

Підвищення поваги та підтримання авторитету норм міжнародного права не можливе без встановлення відповідальності держав, які стоять за міжнародно-протиправними діяннями. Це випливає із правосуб'єктності держав та з факту того, що держави є головними носіями міжнародних зобов'язань, які вправі створювати правила поведінки та впливати на міжнародний правопорядок. Відтак, як справедливо зазначив Д. Кроуфорд, професор та суддя Міжнародного Суду ООН (2015-2021), «відповідальність держав – найважливіший інститут міжнародного права» [86].

Тема відповідальності держав закріпилась у повістці міжнародної спільноти лише на початку першої половини двадцятого століття. Тоді Ліга Націй всіляко сприяла кодифікації норм щодо відповідальності держав, але її зусилля не

увінчались успіхом, навіть попри те, що питання відповідальності держав було обрано в якості основного на конференції 1930 року у Гаазі.

В 1948 році вже Організація Об'єднаних Націй робить впевнений крок в напрямку кодифікації норм відповідальності держав, створивши Комісію ООН з міжнародного права. Питання відповідальності одразу потрапляє в перелік 14 тем, які Комісія повинна була розглянути першочергово.

Перший доповідач Комісії з міжнародного права Ф.В. Гарсіа-Амадор зазначав, що «важко було б знайти тему, яка б спричинила більшу плутаницю та невизначеність» [124, с. 175]. Один із факторів, що стояв за такою плутаницею та невизначеністю – скептицизм країн загального права, що був підґрунтям для суперечок.

Джейсм Кроуфорд, який був спеціальним доповідачем з цього питання у 1997-2001 роках, пояснював це тим, що ідея загального права щодо відповідальності не викликала особливого резонансу у свідомості представників країн загального права: «Ми звикли до такого історичного розвитку правових систем, в яких категорії є конструкціями *post factum*... Але представники правових систем цивільного права, як нам кажуть, принаймні з часів Юстиніана, думають про загальне зобов'язальне право як про категорію, і ПСВД (*прим*. – Проект Статей про відповідальність держав) натхнений способом мислення системи цивільного права, а не загального права» [85, с. 304].

Намагання першого доповідача кодифікувати положення щодо відповідальності держав зазнали краху, незважаючи на значну увагу у післявоєнний час. Комісія не змогла детально розглянути представлену доповідь, що готувалась з 1956 по 1961 роки в силу своєї завантаженості і внутрішніх суперечок навколо питання відповідальності держав [84]. Крім того, проблема виникла в силу того, що Гарсіа-Амадор звузив фокус до питання відповідальність за шкоду нанесену іноземцям, тобто – до дипломатичного захисту [56, с. 777].

Після приходу Роберта Аго, який замінив Ф.В. Гарсіа-Амадора, відбулося переорієнтування на «визначення загальних норм, регулюючих міжнародну

відповідальність держави». Важливим внеском Роберта Аго у розвиток питання відповідальності держав стало те, що він переосмислив поділ на основні та похідні норми відповідальності, розробив структуру проекту Статей, відповідно до якої перша частина стосувалась загальних питань відповідальності (поняття міжнародно-протиправного діяння, правил атрибуції поведінки державі та перелік обставин, що виключають протиправність діяння), а друга – форм та наслідків відповідальності [56, с. 778]. Більшість статей, розроблених ним, були в подальшому відображені в фінальній версії Проекту Статей про відповідальність держав 2001 року.

Завершити розробку Статей про відповідальність держав за міжнародно-протиправні діяння вдалось лише Джеймсу Кроуфорду, коли проект отримав схвалення від Генеральної Асамблеї ООН та був включений у текст Резолюції 56/83 від 12 грудня 2001 року [198]. Варто відзначити, що, намагаючись уніфікувати визначення відповідальності держави та відповідні правила, Комісія з міжнародного права здійснила значний вплив на світогляд держав та їх розуміння відповідальності. Таке твердження знаходить підтвердження у вищезгаданій Резолюції, в якій Генеральна Асамблея рекомендує Статі державам-членам Організації Об’єднаних Націй, незалежно від їхніх намірів щодо офіційної ратифікації та імплементації у внутрішні правові системи.

Статі про відповідальність держав за міжнародно-протиправні діяння представляють найбільш авторитетну кодифікацію звичаєвих норм щодо відповідальності держав. Очікувалось, що проект Статей стане основою для розробки міжнародного договору, який би ще більше кристалізував зміст звичаєвих норм. Проте такі очікування не були реалізовані. Текст Резолюції 71/133 щодо відповідальності держав за міжнародно-протиправні діяння від 13 грудня 2016 року також засвідчує зацікавленість Генеральної Асамблеї у прийнятті відповідної конвенції, а також робить акцент на важливості Статей 2001 року та необхідності для урядів звернути увагу на їх зміст і надання відповідних коментарів [22].

Важливість цих Статей, серед іншого, полягає у тому, що у Розділі II (*статті 4-11*) містяться основні стандарти атрибуції поведінки державі. Зазначимо, що тривалий час в українській доктрині використовувалося поняття «присвоєння поведінки держави», яке є прямим перекладом з російської («присвоение поведения государству»). Втім, в англійському та французькому варіантах використовує термін «*attribution*» («атрибуція») і, як зазначає професор С.С. Андрейченко, використання терміну «атрибуція поведінки державі» замість «присвоєння поведінки державі» є більш доречним, оскільки перше більш точно виражає сутність та природу даного процесу, що полягає в установленні авторства міжнародно-протиправного діяння [1, с. 25]. Складно не погодитись з таким висновком з урахування того, що «принцип об'єктивної відповідальності міцно закріпився в сучасному міжнародному праві, що підтверджується відповідними напрацюваннями вчених та рішеннями міжнародних судових інституцій» [1, с. 107].

В контексті кібератак проти об'єктів критичної інфраструктури найбільша увага приділяється питанням атрибуції поведінки індивідів чи юридичних осіб, що уповноважені на здійснення елементів урядових функцій (*стаття 5*), і осіб чи групи осіб, що діють під керівництвом чи контролем держави (*стаття 8*), оскільки діяльність таких осіб та органів створює ряд викликів для міжнародного права. Це зумовлено тим, що держави фінансово підтримують, використовують або контролюють таких осіб, докладаючи максимум зусиль для того, щоб приховати факти свого втручання та протиправні дії, здійсненні приватними акторами. В меншій мірі увага приділятиметься поведінці органів держави в межах статті 4 Статей про відповідальність держав, тому почнемо з аналізу її положень.

Стаття 4 Статей про відповідальність держав містить найбільш очевидну підставу атрибуції поведінки державі. Відповідно до цієї статті, «[п]оведінка будь-якого органу держави розглядається як діяння цієї держави», незалежно від його функцій та місця в системі держави. Застосування цієї статті до атрибуції кібероперацій підтверджує Правило 15 Талліннського керівництва. Відтак, дії

кіберармій чи інших державних суб'єктів атрибутуються державам відповідно до норм міжнародного права відповідальності держав [209, с. 87]. Експерти НАТО також визнали висновки Комісії міжнародного права, виражені у параграфі 11 коментаря до статті 4, щодо неможливості уникнути відповідальності, відмовляючи національному органу у такому статусі відповідно до свого законодавства [209, с. 88].

У справі про Боснійський геноцид Міжнародний суд ООН розробив тест «повної залежності», відповідно до якого певне об'єднання може бути визнано в якості органу держави. При цьому, відсутня необхідність визнання їх статусу в національному праві. Достатньо, щоб особа, група осіб чи юридична особа слугували інструментом держави та знаходились в повній залежності від неї [48, п. 391-392]. Щодо форми власності, то в теорії та на практиці вона не є вирішальною: ця стаття охоплює як *de jure*, так і *de facto* органи держави, фактично нівелюючи форму власності.

Талліннське керівництво в параграфі 6 коментаря до статті 15 також підтверджує застосовність статті 7 Статей, яка стосується перевищення повноважень або порушень вказівок з боку органів держави. Діяння *ultra vires* в кіберпросторі, відтак, атрибутуватимуться державі, як це встановлює інститут відповідальності держав. Так, наприклад, держава нестиме відповідальність за дії члена військового кіберпідрозділу, який здійснив незаконну кібероперацію всупереч наказам керівництва. Але якщо він використав кіберінфраструктуру держави з ціллю отримання приватної вигоди в результаті кримінальної діяльності, відповідальність держави виключається в силу приватного характеру такої поведінки [209, с. 89].

Стаття 5 Статей про відповідальність також атрибутує державі поведінку осіб чи юридичних осіб, що виконують елементи урядових повноважень. Цікаво, що відповідне положення інтегроване експертами Талліннського керівництва у вище розглянуте Правило 15, яке стосується кібероперацій вчинених державними органами.

На думку Комісії з міжнародного права, юридична особа є такою, що здійснює елементи урядових повноважень, коли вона «уповноважена... виконувати певні функції, подібні до тих, які зазвичай виконують органи держави» [196, с. 281]. Найважливішим питанням є те, які функції «зазвичай» виконують органи держави.

У своєму коментарі Комісія пропонує підхід, який базується на аналізі конкретного контексту, а отже, залежить від конкретного суспільства, його історії та традицій [107, с. 43]. В кіберконтексті серед звичних для держави XXI століття функцій експерти Талліннського керівництва виділяють кіберрозвідку та наступальні кібероперації проти іншої держави [209, с. 89]. Таким чином, держава може укласти контракт з приватною компанією та фактично передати їй виконання певних урядових функцій. Вірогідність такого сценарію особливо зростає, коли у держави відсутні технічні можливості для реалізації деяких функцій в кіберпросторі.

Що стосується атрибуції, то лише поведінка, яка пов’язана із виконанням елементів урядових функцій, буде атрибутуватись державі. При цьому, складно повністю погодитися з думкою експертів щодо того, що наступальні кібероперації є реалізацією урядових повноважень. Складається враження, що у держави є право на застосування сили проти інших держав, хоча з урахуванням наявної в Статуті ООН заборони застосування сили чи погрози силою, такий висновок не є вірним. Відтак, не зрозуміло, чому експерти згадали саме наступальні, а не оборонні кібероперації. Вважаємо, що саме останні можуть здійснюватися державою або делегуватися приватним особам, а отже – атрибутуватимуться відповідно до положень статті 5 Статей про відповідальність держав. Наступальні кібероперації проти об’єктів критичної інфраструктури, навпаки, потрібно атрибутувати на підставі статті 8, про яку піде мова трохи пізніше.

Діяльність, яка не пов’язана з урядовими функціями та здійснюється приватною компанію на вимогу приватних корпорацій, неурядових організацій або є проявом кіберзлочинної діяльності, атрибутуватись державі не буде [209,

с. 89]. Відзначимо, що в даному випадку такий підхід експертів є досить логічним та послідовним, оскільки навряд чи можна прийти до висновку про те, що злочинна кібердіяльність є відображенням реалізації урядових функцій держави.

Стаття 8 Статей про відповідальність держав передбачає, що поведінка недержавних акторів атрибутується державі «лише якщо вона керувала або контролювала конкретну операцію і поведінка, на яку скаржилися, була невід'ємною частиною цієї операції» [107, с. 47]. Отже, дії недержавних кіберакторів можна атрибутувати лише тоді, коли будуть задоволені вимоги тесту ефективного контролю.

Недержавні актори загалом досить неоднорідна категорія, і у випадку з кібератаками ця категорія включає як окремих осіб, так і групи, зокрема – хакерів, неформальні групи на кшталт «Анонімус» (децентралізована група хакерів), злочинні організації, що займаються кіберзлочинністю, юридичних осіб (комерційні IT-сервіси, компанії з розробки програмного забезпечення, апаратних засобів тощо), кібертерористів, повстанці та інших [209, с. 95], чиї інтереси та мотиви можуть повністю чи частково співпадати з інтересами держав.

Міжнародний Суд ООН у рішенні щодо військової та напіввійськової діяльності у Нікарагуа зазначив, що для задоволення вимог тесту ефективного контролю, важливо встановити, що «держава здійснює такий ступінь контролю у всіх сферах, що виправдовує поводження з [приватними акторами] як з особами, що діють від її імені». Тест ефективного контролю також передбачає наявність конкретних вказівок з боку держави щодо вчинення певної дії, тобто необхідною умовою є наявність конкретних наказів держави або визначення напрямків діяльності щодо кожної окремої операції [62, п. 86].

Складно, якщо взагалі можливо, уявити собі ситуацію, коли постраждалі держави зможуть досягнути порогу тесту ефективного контролю у випадку з кібератаками проти об'єктів критичної інфраструктури. І хоча міжнародна група експертів Талліннського керівництва не робить згадок про розробку альтернативного тесту атрибуції кібератак державі, все ж таки існує вірогідність

того, що практика держав сприятиме його виробленню. Так, наприклад, в доктрині згадується тест «контролю та спроможностей», який може розглядатися в якості *lex specialis* по відношенню до тесту ефективного контролю, що є принципом *lex generalis* [223, с. 7].

Фактично цей тест оцінює наявні політичні та технічні індикатори для встановлення автора кібератаки, а саме: зв'язок між недержавним суб'єктом і державою; вплив держави на недержавного суб'єкта; методи виконавця кібератаки; мотиви обох сторін; технічні можливості; географічне розташування тощо [223, с. 8-9]. Справедливості заради відзначимо, що попри відсутність згадки альтернативного тесту в Талліннському керівництві, експерти наголошують на необхідності врахування різних факторів під час здійснення атрибуції кібероперацій *ex ante*. До прикладу, серед таких факторів згадується «надійність, кількість, безпосередність, характер (наприклад, технічні дані та розвідка) і конкретність відповідної доступної інформації, якщо розглядати її у світлі супутніх обставин і важливості права, що підлягає застосуванню» [209, с. 82].

Аналіз практики публічної атрибуції кібератак з початку 2013 року дійсно свідчить про врахування таких факторів державами (як тих, що згадуються в Талліннському керівництві, так і тих, що відносяться до сформульованого в доктрині тесту контролю та спроможностей), але мова про цей вид атрибуції йтиме трохи пізніше.

Загалом ми схиляємося до думки про те, що у випадку з кібератаками вірогідність утвердження альтернативного тесту є досить високою, якщо дії приватних осіб не розцінюватимуться як такі, що становлять виконання елементів урядових функцій. Адже у випадку з кібератаками проти об'єктів критичної інфраструктури, має місце наступальна кібероперація, що загалом не входить в сферу урядових повноважень. При цьому, наступальні кібероперації входитимуть в сферу таких повноважень, якщо доктрина щодо кібероперацій зміниться і міжнародна спільнота визнає наступальну (проактивну) кібербезпеку (кібероборону).

Наразі ж достеменно не відомо яким шляхом підуть ад'юдикаційні органи. Цілком вірогідно, що все буде залежати від контексту. Якщо кібератаки застосовуватимуться в ході збройного конфлікту чи будуть пов'язані з ним, то атрибуція кібератак проти об'єктів критичної інфраструктури, що кваліфікуються в якості військових об'єктів, як видається, буде здійснюватися на підставі статті 5 Статей про відповідальність держав. Але якщо ця кібератака не буде пов'язана зі збройним конфліктом та вчинятиметься в мирний час, то, вважаємо, підлягатиме застосуванню стаття 8 Статей про відповідальність держав, яка вимагає застосування тесту ефективного контролю.

Такий висновок робиться в силу наявності заборони використання сили в міждержавних відносинах. Таким чином, в останньому випадку наступальні кібератаки приватних осіб, на нашу думку, не розглядатимуться в якості елементів урядових повноважень. І навпаки, в ході збройного конфлікту наступальні дії приватних акторів, що є інтегральною частиною операції цілком ймовірно будуть розглядатися як такі, що пов'язані з виконанням елементів урядових повноважень.

У випадку зі статтями 5 та 8 потрібно чітко розуміти межу між здійснення елементів урядових повноважень та діяльністю, що є реалізацією конкретних інструкцій. В останньому випадку відсутнє фактичне «делегування» урядових функцій недержавному актору, останній виступає в якості допоміжного органу держави. Так, наприклад, якщо приватна компанія здійснює кібероперацію на вимогу збройних сил держави для підтримки кінетичної операції, то така поведінка атрибутуватиметься державі на підставі статті 8 Статей про відповідальність держав [209, с. 96].

Загалом для атрибуції будь-якої кібератаки, що вчиняється недержавними акторами, важливо, щоб держава знаходилася в позиції здійснення «ефективного контролю» цього актору. Тобто, саме держава повинна визначати виконання та хід конкретної операції, а кібердіяльність, якою займається недержавний суб'єкт, має становити «невід'ємну частину» операції держави [107, с. 47]. У випадку з об'єктами критичної інфраструктури це означає, що саме держава стоїть за

обранням такого об’єкта в якості цілі атаки, визначає очікувану шкоду, яку має завдати кібератака та в будь-який момент може змінювати хід операції проти таких об’єктів.

Щодо дій, ціллю яких є сприяння здійсненню кібероперацій, зокрема «фінансування, організація, навчання, постачання та оснащення… вибір цілей та планування всієї операції», то їх недостатньо для встановлення ефективного контролю [62, п. 115]. Але неможливість атрибуції кібердіяльності державі у випадку загального контролю, не означає, що держава не нестиме відповідальність за сприяння здійсненню кібероперації, оскільки така підтримка сама собою є порушенням міжнародного права. Наприклад, надання шкідливого програмного забезпечення групі може становити заборонену інтервенцію у внутрішні справи держави (правило 66 Талліннського керівництва 2.0). Відтак, кібератаки проти об’єктів критичної інфраструктури, щодо яких держава здійснювала загальний контроль, все ж будуть їй атрибутуватись, хоча юридичні підстави відповідальності варіюватимуться з урахуванням наслідків конкретної поведінки держави.

У випадку з діяннями *ultra vires* вважається загальноприйнятим, що держава не нестиме відповідальність, якщо мало місце перевищення повноважень з боку недержавних акторів, щодо яких ця держава здійснює ефективний контроль. Але в ситуації з атрибуцією діянь в кіберпросторі не все так просто. До прикладу візьмемо ситуацію, коли держава доручає приватній IT компанії здійснити кібероперацію проти системи SCADA об’єкта критичної інфраструктури іноземної держави, вдаючись таким чином до контрзаходу. Припустимо, що шкідливе програмне забезпечення поширилось в кіберпросторі та завдало шкоди третім державам. В цьому випадку зараження систем третіх держав буде атрибутуватися державі, яка доручила IT компанії здійснити зараження системи SCADA, незважаючи на те, що завдання шкоди третім державам не було частиною інструкцій, наданих цією державою. На думку експертів Талліннського керівництва, дії *ultra vires,* що не пов’язані з операціями, над якими держава здійснює ефективний контроль, загалом державі не

атрибутуються. Проте, якщо вони є інтегральною та суттєвою частиною операції під ефективним контролем держави, то такі дії атрибутуватимуться державі [209, с. 98].

При аналізі коментарів групи міжнародних експертів Талліннського керівництва увагу привертає приклад, представлений в параграфі 14. Розглядається ситуація, коли в силу технічних причин приватна ІТ-компанія не може використати сервер Держави В, як того вимагала Держава А. В результаті компанія самостійно приймає рішення використати сервер Держави С, не звертаючись за дозволом Держави А, що здійснює ефективний контроль над кібероперацією. Це призводить до порушення міжнародних зобов'язань, які Держава А має перед Державою С. Тобто попри характер *ultra vires,* діяння атрибутуватиметься державі, оскільки здійснення кібероперації через сервер Держави С було невід'ємною та важливою частиною такої операції [209, с. 98].

Нарешті, стаття 11 Статей про відповідальність держав передбачає, що «[п]оведінка, яка не атрибутується державі на підставі попередніх статей, розглядається як діяння цієї держави за міжнародним правом, якщо і в тій мірі, в якій ця держава визнає і приймає дану поведінку як власну» [107, ст. 11; 209, н. 17]. Міжнародний суд ООН підтвердив звичаєвий характер цієї статі у справі про дипломатичний та консульський персонал США в Тегерані [246, п. 74].

Стандарт щодо «визнання» та «прийняття» встановлює кумулятивні умови застосування цієї норм. Крім того, необхідно більше, ніж просто схвалення або мовчазне прийняття кібероперації, що здійснюється недержавним актором [107, с. 53-54]. Висловлення схвалення, навіть якщо воно має яскраво виражений характер недостатньо. В кіберконтексті держава може «прийняти» кібероперацію шляхом прийняття рішення про використання власних кіберспроможностей для захисту недержавних акторів від контроперацій, щоб таким чином сприяти продовжуваності кібероперації. Ця норма застосовується виключно тоді, коли ціллю кібероперації є державні органи [209, с. 100].

Аналіз положень Талліннського керівництва загалом свідчить про те, що звичаєві правила атрибуції, що містяться в Статях про відповідальність держав

за міжнародно-протиправні діяння 2001 року фактично продубльовано з незначними змінами, яких вимагає кіберпростір. При цьому, складність застосування норм про атрибуцію до кібератак вимагає переосмислення і модифікації ряду положень, інакше – складно собі уявити процес здійснення атрибуції в найближче десятиліття.

2.3. Атрибуція кібератак в силу порушення обов'язку необхідної обачності (*due diligence*)

Кібератаки уже стали глобальним викликом для міжнародної спільноти, яка залежить від промислових систем управління. Вони особливо небезпечні при їх використанні проти об'єктів критичної інфраструктури, без належного функціонування яких люди можуть страждати від нестачі їжі, води, електроенергії, медичного обслуговування тощо, а держава – зазнати політичної та економічної кризи.

Як зазначалось вище, кібератаки можуть здійснюватися як державними, так і недержавними суб'єктами. В останньому випадку, коли держава діє через проксі, особливо складно атрибутувати кібератаки конкретному суб'єкту та встановити необхідний між ними зв'язок залежності. У той же час наявні технічні та людські ресурси дозволяють встановити зв'язок між конкретною кібератакою та приватною особою або групою осіб, які за нею стоять. Враховуючи те, що переважна більшість кібератак вчиняється приватними акторами, дії яких не можуть ставитися в вину державі, слід звернути увагу на обов'язок держави проявляти належну турботу (*due diligence*).

Згідно з правилом 6 Талліннського керівництва, «держава повинна проявляти належну обачність, не дозволяючи використовувати свою територію чи кіберінфраструктуру під своїм урядовим контролем для кібероперацій, які зачіпають права інших держав та спричиняють серйозні несприятливі наслідки для них» [209, с. 30]. Цей обов'язок держав неодноразово був підтверджений Міжнародним Судом ООН, який в найбільш значимій справі щодо протоки Корфу, конкретизував зміст обов'язку проявляти необхідну обачність.

Саме в рішенні по даній справі Суд зазначив, що держави не можуть дозволяти використовувати свою територію таким чином, коли це використання суперечить реалізації прав інших держав [71, п. 22]. Експерти прийшли до висновку про те, що наразі відсутнє *lex lata* [209, с. 31], яке б підтверджувало застосування цього принципу в кіберконтексті, але, як свідчить аналіз позицій держав, вони підтримують застосування принципу *due diligence* в кіберпросторі, хоча й дещо по-новому інтерпретують та застосовують, встановлюючи певні обмеження.

Використання інфраструктури третьої держави не завжди є порушенням. Воно становитиме порушення лише в тих випадках, коли держава володіла знаннями про кібератаку, яка досягає порогу завдання шкоди, і могла вжити відповідні заходи для припинення такої кібератаки. У випадку з використанням урядової кіберінфраструктури таке знання презюмується.

Відтак, держава не може уникнути відповідальності, коли, до прикладу, для кібератаки проти об’єкта критичної інфраструктури використовується урядова інфраструктура військової бази. Те саме стосується іноземних військових баз, дипломатичних будівель, платформ у відкритому морі, якщо держава контролює їх кіберінфраструктуру. При цьому, контроль над такою інфраструктурою не виникає в силу факту здійснення екстратериторіальної юрисдикції – ключовим є саме контроль, який може здійснювати та здійснює уряд над конкретною інфраструктурою [209, с. 33].

Важливою також є кваліфікація діяння в якості міжнародно-протиправного діяння. Тобто, якщо має місце кібершпигунство за діяльністю об’єкта критичної інфраструктури, яке здійснюється за допомогою кіберінфраструктури третьої держави, у третьої держави не виникає обов’язку припинити таку операцію, оскільки шпигунство в мирний час не забороняється міжнародним правом *per se*. Відтак, обов’язок проявляти необхідну обачність не буде порушено, за умови що між державами відсутній спеціальний правовий режим, який встановлює спеціальні права та обов’язки.

Для того, щоб характеризувати діяння як таке, що порушує обов'язок необхідної обачності, обов'язковим є наявність «серйозних негативних наслідків». Наразі в міжнародному праві відсутній стандарт щодо того, що підпадає під «серйозні негативні наслідки» [238, п. 1963] – оцінка в кожному разу буде залежати від контексту та конкретних наслідків і шкоди, яку завдали державі. Міжнародна група експертів Талліннського керівництва запропонувала застосовувати цей стандарт аналогічно тому, як він застосовується в контексті міжнародного екологічного права, тобто додатково наслідки мають бути «значними».

Таким чином, операції, які завдають незручностей, призводять до незначних збоїв або незначних витрат не є тією шкодою, що необхідна для порушення принципу *due diligence* [209, с. 37]. Така позиція може призвести до помилкового висновку про необхідність завдання фізичної шкоди об'єктам чи людям, але це не так. Експерти прийшли до спільної позиції про те, що втручання у роботу критичної інфраструктури або операції, які мали серйозний вплив на економіку підпадають під фактичні підстави порушення даного принципу [209, с. 38].

Але у випадку з принципом *due diligence* та його застосуванням в кіберпросторі, є ще одна перепона. Виходячи з висновків та риторики Групи урядових експертів у 2015 році, юридично обов'язкова природа даного принципу в кіберпросторі – досить суперечлива [68, п. 13(c), 28(e)]. Втім, позицію про те, що *due diligence* є загальним міжнародним зобов'язанням та становить *lex lata*, яке забороняє державам свідомо дозволяти використовувати свою територію для міжнародно-протиправних дій із використанням кіберзасобів, підтримали такі держави як Австралія [52, с. 91], Чеську Республіка [95], Естонія [111], Нідерланди [160], Фінляндія [118] та Франція [123, с. 6].

Враховуючи те, що кібератаки проти об'єктів критичної інфраструктури, особливо промислових та медичних систем, можуть призвести до порушення ряду фундаментальних прав людини, на тривалий час унеможлививши їх реалізацію, вважаємо за необхідне розглянути це зобов'язання в рамках

міжнародного права прав людини, що містить спеціальні норми щодо відповідальності та є досить сильним правовим режимом.

Міжнародний пакт про громадянські та політичні права покладає на державу зобов'язання забезпечувати права людини в межах території та юрисдикції останньої [17, ст. 2 (1)]. В своєму Зауваженні загального порядку № 31 Комітет ООН з прав людини, шляхом інтерпретації статті 2 (1) Пакту, встановив, що зобов'язання, які містяться у вказаній статті, юридично зв'язують держави та «як такі не мають горизонтальної сили з точку зору міжнародного права».

Проте Комітет також прийшов до висновку, що «позитивні зобов'язання держав-учасників щодо забезпечення дотримання передбачених Пактом прав будуть виконані повністю тільки в тому випадку, якщо люди будуть захищені державою не тільки від порушення передбачених Пактом прав представниками держави, але і від актів, що здійснюються приватними особами або недержавними утвореннями, такими, що завдають шкоди здійсненню передбачених Пактом прав в тій мірі, в якій вони можуть застосовуватися у відносинах між приватними особами або недержавними утвореннями» [12].

Що стосується прав людини, передбачених в іншому Пакті, то Комітет ООН з економічних, соціальних та культурних прав встановив, що обов'язок вживати заходів до поступової повної реалізації прав, передбачених в Пакті, включає зобов'язання уникати регресивних заходів при здійсненні прав [25]. Відтак, універсальні інструменти з прав людини визнають обов'язок держави проявляти належну турботу задля попередження порушень прав людини, які є наслідком дій приватних осіб. У випадку з кібератаками справедливо зазначити, що суттєва частина вчиняється саме індивідами, що не пов'язані з державою, але використовують інфраструктуру однієї держави з ціллю завдання шкоди важливій критичній інфраструктурі іншої держави.

Практика регіональних органів – Європейського та Міжамериканського судів з прав людини свідчить про ідентичний підхід. При цьому, МАСПЛ робив прямі посилання на доктрину «*drittwirkung der Grundrechte» (далі* – дрітвіркунг*)*,

що передбачає горизонтальний ефект прав людини. Ця доктрина була розроблена Федеральним Конституційним Судом Німеччини у справі громадянина Люта від 1958 року, який оголосив бойкот фільму «Безсмертна кохана».

Річ в тім, що цей фільм був створений нацистським режисером номер один – Вайтом Харлемом, на творах якого виховувався весь Третій Рейх. Взявши до уваги цінність права на свободу вираження своїх поглядів, Конституційний Суд встановив, що фундаментальні права – це не тільки суб'єктивні права, а й об'єктивні принципи, які поширюються на публічні та приватноправові відносин. Незалежно від характеру відносин, адресатом завжди буде виступати держава, що зобов'язана враховувати значимість таких прав при інтерпретації і застосуванні закону [101, с. 205-206].

В Латинській Америці використанню доктрини дрітвіркунг передувало визнання конвенційних прав фундаментальними та такими, що мають характер *erga omnes* в першому рішенні МАСПЛ у справі «Веласкес-Родрігес проти Гондурасу». Уже в рішенні «Мирна громада Сан Хосе де Апартадо проти Колумбії», яке стосувалось різні мирного населення напіввійськовим формуванням, Суд підкреслив, що обов'язок поважати права людини існує не тільки у відносинах між державою та індивідом, а й між приватними особами. Суддя Антоніо Тріндаде зазначив, що ситуація в регіоні, а саме наявність великої кількості воєнізованих та підпільних груп, вимагає «визнання впливу Американської Конвенції щодо третіх сторін (*Drittwirkung)*» в силу характеру конвенційних прав [127, с. 14].

Важливість доктрини в практиці МАСПЛ також підтверджує Консультативний Висновок Міжамериканської Комісії з прав людини №. 18/03. Висновок був винесений на запит Мексики щодо правового статусу та прав мексиканських мігрантів в США. Свою позицію щодо рівності всіх осіб на території ОАД Комісія аргументувала «горизонтальним ефектом фундаментальних прав», що покладає на державу позитивні обов'язки щодо наявних та потенційно можливих порушень прав людини [149, п. 140, 147, 150].

Європейський Суд з прав людини також вирішив не відставати від свого американського колеги. Зокрема, у справі «А. проти Об'єднаного Королівства» заявник скаржився на фізичне насилля проти себе і свого брата з боку вітчима. До подачі скарги в ЄСПЛ вітчиму було пред'явлено обвинувачення, але потім виправдано, оскільки на той час англійське право допускало «розумне покарання» зі сторони батьків. Проте ЄСПЛ вирішив, що по відношенню до дітей і представників найбільш вразливих груп, держава повинна гарантувати особливий захист та засоби ефективного попередження насилля, яке в даній справі досягло порушення статті 3 ЄСПЛ [64, п. 22].

Висновки Комітетів ООН, Європейського та Міжамериканського судів з прав людини є свідченням усестороннього підходу до проблеми захисту прав людини. Основоположні права, що закріплені в універсальних та регіональних інструментах захисту прав людини, були б ілюзорними у випадку їх гарантування виключно у відносинах з державою. Саме тому Міжамериканський та Європейський Суд з прав людини вимагають від держав здійснення позитивних дій, а іноді втручання в приватноправові відносини між індивідами, якщо існує ризик порушення закріплених прав з боку інших індивідів чи приватних інституцій.

В контексті кібератак проти об'єктів критичної інфраструктури цей ризик не просто існує, а вже давно став реальністю. Були деякі спроби викорінити безкарність та привернути увагу громадськості до цієї проблеми, однак із кожною кібератакою хакери стають все більш впевненими у здійсненні кібератак значних масштабів.

Серед найвідоміших кібератак на критичну інфраструктуру можна назвати наступні – кібератака на одну з американських гребель у 2013 році, німецький металургійний комбінат у 2014 році, українські системи електромереж у 2015 та 2016 роках, Національну службу охорони здоров'я у Великобританії у 2017 році, системи приладів безпеки Саудівської Аравії в 2017 році, постачальника електроенергії в Південній Африці та індійський атомний завод у 2019 році [60].

Також можна спостерігати збільшення кількості кібератак на залізничні системи. Зокрема, у 2014 році в Польщі 14-річний школяр зламав трамвайні системи. Його дії спричинили сходження трамвая з рейок та численні тілесні ушкодження [213]. У 2016 році Великобританія повідомила, що її залізничні системи постраждали в ході щонайменше чотирьох основних кібератак [166]. А в 2017 році через наслідки атаки «WannaCry» залізнична інфраструктура Німеччини зазнала системних помилок [93].

Під час першої хвилі пандемії COVID-19 приватні особи атакували навіть медичний сектор. Такі випадки, серед іншого, були зареєстровані у Франції, Чехії, Таїланді та Туреччині. Наприклад, у березні 2020 року найбільша лікарня Брно у Чеській Республіці стала жертвою кібератаки проти її систем. В результаті довелося відкласти операції та перевести важких пацієнтів в інші медичні установи. Вони також не змогли обробляти тести на наявність коронавірусної інфекції та виконувати інші необхідні функції [164]. У тому ж ключі паризька AP-HP, що представляє найбільшу мережу лікарень в Європі, стала жертвою кібератак [171].

Майже у всіх випадках для гарантування анонімності використовувалася критична інфраструктура третьої держави. Це головна причина, чому обов'язок належної обачності (турботи) заслуговує на особливу увагу. Цей обов'язок не є панацеєю проти кібератак, але може допомогти їх зменшити. І дійсно, держави будуть приділяти більше уваги, якщо атакована держава буде зацікавлена у притягненні до відповідальності третьої держави. Тому ідея перенесення обов'язку проявляти необхідну обачність з основних до похідних норм відповідальності держав має детально проаналізована та переосмислена.

Можна очікувати зацікавленість держав у контролі того, як критична інфраструктура на їх території використовується, коли відповідальність є визначеною. Згідно з відомим висловлюванням у справі Корфу, «кожна держава зобов'язана не дозволяти свідомо використовувати свою територію для дій, що суперечать правам інших держав» [71, с. 22]. Це зобов'язання виходить з

суверенітету держави над її територією та обов'язку захищати права інших держав в межах своєї території.

Щоб встановити порушення належної турботи, мають бути дотримані дві основні передумови. По-перше, необхідні знання третьої держави щодо використання кіберінфраструктури, що знаходиться на її території. Ці знання не повинні бути реальними, а скоріше конструктивними. Це означає, що знання можуть бути вважатися такими, що є у держави, якщо в межах звичайного перебігу подій держава знала б про використання своєї території для кібератаки [209, с. 41].

Якщо використовується урядова інфраструктура, то, безперечно, третя держава мала б володіти знаннями про використання своєї кіберінфраструктури. Дійсно, приписування обмежувальних знань також відбуватиметься, якщо будуть використовуватися загальновідомі вразливості або шкідливі програми, які вже було виявлено та про які повідомлено. Наприклад, третя держава не може уникнути відповідальності, стверджуючи, що не знала про вразливості Heartbleed [209, с. 41] або Zerologon [152], виявлені у 2014 та 2020 роках відповідно.

По-друге, кібератака повинна спричинити «серйозні несприятливі наслідки». Хоча поріг необхідної шкоди не встановлений у міжнародному праві, очевидно, що серйозні наслідки виключають незначні збої в роботі операційних технологій та інші незручності. У той же час немає необхідності у фізичному пошкодженні об'єктів критичної інфраструктури атакованої держави або людських травм. Серйозність нанесеної шкоди оцінюватимуть окремо у кожному конкретному випадку [209, с. 37].[3]

Тому державам доводиться активно брати участь у встановленні відповідальності держави на основі зобов'язань щодо належної обачності. Це

[3] Наукові результати, представлені в підрозділі 2.3, попередньо оприлюднено в наступних публікаціях : Відповідальність держав за порушення обов'язку належної обачності (*due diligence*) в кіберпросторі. Право і суспільство: актуальні питання і перспективи розвитку : Матеріали V Міжнародної науково-практичної конференції Частина I (10 грудня 2020 року). Полтава, 2020. С. 107-110; Attribution of cyberattacks committed through cyber infrastructure of a third state and due diligence obligation. Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe : International Scientific Conference. Baltija Publishing. (20 November 2020). Riga, Latvia. 2020. P. 111-114.

може змусити держави більш ретельно стежити за використанням критичної інфраструктури, розташованої на її території, і, як наслідок, запобігати та припиняти протиправні дії, що порушують зобов'язання перед державою, яка є ціллю кібератаки.

Отже, якщо наявність обов'язку необхідної обачності не буде визнано в кіберконтексті, у постраждалих від кібератак осіб все ж є важелі для атрибуції кібератак державі. Так, наприклад, визнаний «горизонтальний ефект» прав людини може стимулювати державу здійснювати контроль над тим, як і ким використовується її кіберінфраструктура та здійснювати всі необхідні кроки для попередження кібератак проти критичної інфраструктури. Тобто, така необачність буде атрибутуватись в рамках міжнародного права прав людини, що містить норми відповідальності, які є *lex specialis* по відношенню до загальних норм відповідальності держав, що містяться в Статтях про відповідальність держав за міжнародно-протиправні діяння 2001 року.

2.4. Технічна та політична атрибуція кібератак – альтернативний шлях, що зародився на практиці

Попри існування звичаєвих норм та конкретизації їх нормативного змісту в Статтях про відповідальність держав 2001 року, наразі ці норми жодного разу не знайшли свого застосування в практиці держав. В силу обмежених людських та технічних ресурсів, шанси постраждалої держави атрибутувати кібератаку державі протягом тривалого часу були мізерними, тому поруч із юридичною атрибуцією (саме вона є одним із елементів міжнародно-протиправного діяння), виникає технічна та політична атрибуція кібератак.

Ці два види атрибуції кібератак можна розглядати як цілком не пов'язані між собою, або, навпаки, як частини цілого. В цілому технічна атрибуція являє собою криміналістичне розслідування, яке має на меті отримання прямих доказів щодо здійсненої кібератаки, тобто цифрових криміналістичних доказів. В той час як політична атрибуція ставить на меті визначити, хто причетний до кібератаки –

індивід чи держава, та ґрунтується на політичному аналізі [240, с. 2]. Логічним завершенням цього ланцюжка атрибуції, вважаємо, повинна стати юридична атрибуція, яка не можлива без технічної та політичної атрибуції. Адже саме юридична атрибуція є важливою передумовою забезпечення відповідальної поведінки держав в кіберпросторі [4, с. 195].

Починаючи з 2007 року, близько 20 кібератак було атрибутовано конкретним державам, і тут мова йде вже про публічну атрибуцію кібератак, що базувалась на оцінці політичних та технічних індикаторів. При цьому, юридична атрибуція є кінцевим «пунктом призначення» та не можлива без технічної та політичної атрибуції.

В доктрині міжнародного права превалює думка щодо необхідності здійснення «тривимірної» атрибуції кібератак, що включає технічну, політичну та юридичну атрибуцію [239, с. 233-234; 160, с. 83-85; 66]. Як зазначає М. Росіні, для атрибуції кібератак потрібно спочатку встановити комп'ютери та сервери, які застосовувалися при їх здійсненні, ідентифікувати осіб, які мають безпосередній стосунок до цих атак, а потім – довести, що ці особи діяли від імені конкретної держави, щоб юридично присвоїти їх поведінку державі [200, с. 240; 210, с. 98-103]. Таке завдання очевидно виходить за межі юридичної площини та вимагає оцінки технічних та політичних індикаторів, таких як мотивація або стратегічні інтереси, технічні показники, рівень близькості між державними та недержавними акторами, а також географічне місце перебування джерела кібератаки.

Загально прийнято вважати, що саме 2007 рік став роком «народження» публічної атрибуції кібератак в міжнародному житті. Адже у 2007 році три хвилі DDoS-атак було направлено проти державних та недержавних установ Естонії. Внаслідок скоординованої атаки хакерів сайти Парламенту Естонії, міністерств, банківських установ та ЗМІ на деякий час вийшли з ладу.

Важливим при цьому є контекст, в межах якого вони мали місце. Передумовою кібератак став демонтаж та перенесення «Бронзового солдата» – пам'ятника радянським солдатам, що загинули в ході Другої Світової війни. На

думку багатьох естонців, пам'ятник потрібно було перенести та здійснити перезахоронення солдат, оскільки німецька окупація була замінена на радянську, і для багатьох естонців «Бронзовий солдат» став символом депортації, вбивств та звірств Радянського Союзу [138, с. 53-55].

Докази свідчать, що хакери вважали себе росіянами, інструменти для зломів містилися на російських веб-сайтах та в чатах. Крім того, для нападу вибрали день, що має особливе значення для більшості росіян – 9 травня. Про причетність РФ говорить також те, що деякі атаки здійснено з російських IP-адрес (Інтернет-протоколів), в тому числі з державних установ, незважаючи на те, що використовувані ботнети включали комп'ютери з різних країн [200, с. 235].

Нарешті, у травні 2007 року Державна прокуратура Естонії звернулась з офіційним прохання про допомогу в розслідуванні до Генеральної прокуратури Російської Федерації з метою відстежити нападників, які, як було встановлено, проживають на території Росії. Запит був проігнорований, незважаючи на те, що цей вид співпраці передбачено Договором про взаємну правову допомогу, який укладено між Естонією та Росією [181, с. 3]. Відтак, в сукупності ці факти послужили підставою для першої в світі публічної атрибуції кібератак Російській Федерації.

В ситуації з Естонією також варто згадати факт того, що дана держава є членом НАТО. Тому в доктрині часто зустрічається думка про те, що у випадку кібератаки проти системи SCADA об'єктів критичної інфраструктури, було б досить складно її замаскувати під діяльність «російських патріотів», і найголовніше – при кібератаці на критичну інфраструктуру існував би ризик застосування Естонією статті V Північноатлантичного договору. Таким чином, можна було б очікувати на більш жорстку відповідь з боку НАТО [153, с. 240]. Цілком справедливо можна стверджувати, що недосягнення порогу для застосування статті V, ймовірно, було стратегічним завданням, яке визначила для себе Російська Федерація [134, с. 53].

Через рік після кібератаки на Естонію послідували кібератаки проти Грузії, які були здійснені не в мирний, а у воєнний час. Кібератаки проти Грузії розпочалися до і тривали протягом усього збройного конфлікту між Грузією та Російською Федерацією в серпні 2008 року.

Як видається, російські хакери знову були залучені до кібератак, оскільки координація відбувалася переважно російською мовою, а також на російськомовних чи пов'язаних з Росією форумах. Як і у випадку з Естонією, деякі коментатори заявляли, що рівень координації та підготовки вірогідно передбачав державну підтримку кібератак. Нарешті, IP-адреси, що належать російським державним компаніям, використовувались для здійснення DDoS-атак. Попри наявні технічні та політичні індикатори, Росія знову заперечувала будь-яку відповідальність [235, с. 75].

Що ж до інших потенційно активних кібердержав, то кібератаку проти «Sony Pictures Entertainment» публічно приписували Північній Кореї завдяки технічному аналізу зловмисного програмного забезпечення для видалення даних, яке до цього вже було застосовано Північною Кореєю. В результаті було виявлено подібність у конкретних рядках коду, алгоритмах шифрування, методах видалення даних та скомпрометованих мережах. Федеральне бюро розслідувань США у своєму звіті також закцентувало увагу на «значному збігу між інфраструктурою, використаною в цій атаці, та іншою шкідливою кібердіяльністю, яку раніше уряд США пов'язував безпосередньо з Північною Кореєю. Наприклад, ФБР виявило, що декілька адрес Інтернет-протоколів (IP), пов'язаних з відомою північнокорейською інфраструктурою, пов'язувалися з IP-адресами, які були жорстко кодовані в зловмисне програмне забезпечення для видалення даних, яке використовується в цій атаці». Крім того, вони виявили схожість між інструментами, які використовувались під час кібератак проти банків Sony, південнокорейських установ та ЗМІ, які, як стверджується, здійснила Північна Корея [116].

Мотивація хакерського угрупування «Охоронці миру», які взяли на себе відповідальність за атаку [116], також заслуговує на увагу. Напад нібито був

спровокований випуском скандального фільму «Інтерв'ю» про вигадане вбивство Кім Чен Ина. Це дає змогу зробити висновок, що мотивація хакерів повністю узгоджується з інтересами Північної Кореї, а саме – запобігти виходу фільму. На це вказує повідомлення, отримане компанією Sony, та лист посла Північної Кореї Джа Сонг Нама до ООН. Зокрема, пан Джа Сонг Нам назвав цей фільм «найбільш кричущим актом тероризму та війни», який «абсолютно не буде толеруватися», додавши «Якщо адміністрація США дозволить і забезпечить показ фільму, будуть вжиті безжальні контрзаходи». «Це їхня [КНДР] тверда рішучість нещадно знищити кожного, хто наважиться хоч трохи поранити чи напасти на верховне керівництво країни», – сказав він [159]. Тим часом хакери надіслали повідомлення з погрозами про те, що «світ буде сповнений страху» і натякнули на повторення атаки 11 вересня [236]. Очікуваним наслідком стало скасування показу фільму з боку компанії Sony та всіх кінотеатрів [185].

Цікаво, що 22 грудня 2014 року, через три дні після опублікування звіту ФБР, в якому зазначалася причетність Кореї до кібератаки проти компанії Sony, Північна Корея теж стає жертвою кібератаки. В результаті мало місце відключення Інтернету, яке тривало більше 10 годин. А через кілька днів президент США підписав указ про запровадження посилених санкцій проти Північної Кореї [216].

Значний прорив в публічній атрибуції був досягнутий лише 15 лютого 2018 року, коли одразу дві держави – США та Великобританія – офіційно атрибутували Російській Федерації відповідальність за шкідливе програмне забезпечення «NotPetya», що шифрувало дані без змоги їх розшифрувати. Вперше, дві держави спільно пішли на такий серйозний крок, що було реакцією на глобальні наслідки «NotPetya», які не мали територіальних обмежень.

При цьому, Сполучене Королівство Великобританії було першою державою, яка заявила, що «російський уряд, зокрема російські військові, несуть відповідальність за руйнівну кібератаку «NotPetya», що сталась у червні 2017 року» [121]. Того ж дня Сполучені Штати Америки опублікували заяву на сайті

Білого дому. США також атрибутували застосування «NotPetya» російським військовим, додаючи, що це «найбільш руйнівна і дорога кібератака в історії. […] Вона є частиною постійних зусиль Кремля щодо дестабілізації України та дедалі чіткіше демонструє причетність Росії до триваючого конфлікту. Це також була необачна і недискримінаційна кібератака, яка зустрінеться міжнародними наслідками» [218].

Оскільки «NotPetya» вплинув не тільки на Україну, а й на країни Європи, Азії та Америки, інші держави – Австралія, Канада, Нова Зеландія приєдналися до США та Великобританії, публічно атрибутувавши «NotPetya» Росії після проведеної власної перевірки. Зокрема, австралійський уряд дійшов висновку, що «суб'єкти, які фінансуються російською державою, відповідальні за інцидент» в результаті розслідування австралійських спецслужб та консультацій зі США та Великобританією [167]. І нарешті, Канада публічно заявила, що «суб'єкти Росії відповідальні за розробку NotPetya», засудивши нерозбірливі атаки на «критичні фінансові, енергетичні, урядові та інфраструктурні галузі в усьому світі в червні 2017 року» [90].

Аналіз *opinio juris* держав свідчить про бажання та готовність атрибутувати кібератаки відповідальним державам, але юридична атрибуція, очевидно, є останнім кроком, які держави готові зробити. У своєму зверненні від 2018 року міністерство національної безпеки Нідерландів підкреслило факт зростання кіберзагроз, що «вимагає рішучої міжнародної реакції на основі міжнародних угод. Статус-кво є недостатній. Кабмін хоче (публічно) протистояти виконавцям кібератак. Це вимагає виявлення, а потім політичної, а можливо, і юридичної атрибуції» [232, с. 7]. Це звернення прекрасно демонструє те, до чого держави вже зараз готові, а до чого ні.

Притягнення держави до відповідальності – досить складний та, як правило, тривалий процес, але враховуючи можливість застосування контрзаходів у відповідь на ворожу кібератаку або навіть можливість вдатися до реалізації права держави на самозахист, міжнародна спільнота має створити всі умови для

створення спеціального режиму, який би враховував особливості атрибуції кібератак.

По-перше, створення спеціального правового режиму для кібератак та їх атрибуції зумовлено їх особливою природою, транскордонним характером та необхідністю здійснення ряду технічних експертиз для встановлення технічних та людських ресурсів, залучених до здійснення кібератак. По-друге, коли мова йде про кібератаки проти об'єктів критичної інфраструктури, які потенційно можуть призвести до серйозних кінетичних наслідків, існує гостра необхідність у правовому врегулюванні та визначенні тих об'єктів, які входять в поняття критичної інфраструктури, якщо дане питання залишатиметься на розсуд держав. Що ж до Талліннських керівництв 2013 та 2017 років, то, незважаючи на їх авторитетність, їм бракує обов'язкової сили і загального визнання, про що свідчить позиція окремих держав. Крім того, вони досить часто підпадають під критику в силу того, що підготовлені та розроблені експертами НАТО, а також не передбачали залучення інших експертів-міжнародників з різних регіонів та держав світу.

Як вище згадувалося, атрибуція кібератак має здійснюватися в трьох вимірах – технічному, політичному та юридичному. Технічна атрибуція стосується криміналістичного розслідування шкідливого інциденту – встановлення походження платформи для атаки та пов'язаних із нею інструментів та інфраструктури. Тобто, вона передбачає оцінку технічних індикаторів. Політична атрибуція стосується політичної детермінації того, хто стоїть за кібератакою – особа чи держава – та ґрунтується на політичному аналізі, оцінці та судженнях. Отже, передбачається оцінка як технічних, так і політичних індикаторів.

Може виникнути логічне питання щодо доцільності оцінки політичних індикаторів, але без їх врахування важко гарантувати достовірність атрибуції. І держави, і приватний сектор визнають, що технічні індикатори можуть бути сфальсифіковані [97, с. 16]. Крім того, досить часто політичний контекст, в межах якого була здійснена кібератака та мотиви сторін сприяють здійсненню

атрибуції. Так, наприклад, якщо конкретна держава задовольняє свої політичні, економічні чи інші потреби завдяки кібератаці проти іншої, це може враховуватися при атрибуції. До політичних індикаторів також належить характер обраної цілі, потреба в спеціалізованих знаннях тощо [97, с. 12].

Разом з тим, політичних індикаторів загалом не достатньо і висновки, отримані на їх основі, не можуть бути остаточними. Міждержавні відносини є досить делікатною матерією, тому не завжди мотиви держави для здійснення кібератаки є очевидними, як і ті переваги, що така держава отримує у випадку успішної кібератаки. Зокрема, спочатку вважалося, що атака на «TV5Monde» була здійснена Ісламською державою. З одного боку, використовувалися сфальсифіковані технічні прапори, з іншого – атака проти основної західної станції новин, як видавалось, цілком відповідає мотивам Ісламської держави посіяти страх. Хакери не тільки завдали атаки по мережах «TV5Monde», а й розмістили про-ісламський напис в соціальній мережі каналу, замінивши зображення профілю на чорне фонове зображення з написом «CYBERCALIPHATE» та «Je suIS IS».

Враховуючи те, що атака проти «TV5Monde» була здійснена на початку квітня 2015 року, через три місяці після атаки на Шарлі Ебдо, політичні індикатори вказували на Ісламську державу та її новий метод боротьби. Проте пізніше виявилося, що Ісламська держава не має відношення до цієї атаки. В червні 2015 року група держав «FireEye» повідомила, що на підставі таких технічних індикаторів як інфраструктура, шкідливе програмне забезпечення та часові показники встановлена причетність російської групи «APT28», яку пов’язують з урядом Російської Федерації [161; 181].

Таким чином, не можна повністю покладатися на політичні індикатори, оскільки держава, яка стоїть за кібератакою може скористатися політичними індикаторами, щоб повністю відвести від себе підозри. В кіберконтексті недоліки політичних та технічних індикаторів також можуть компенсуватися, наприклад, існуванням високонадійної людської розвідки [209, с. 82].

В цілому публічна атрибуція кібератак продемонструвала свою здатність стримувати держав-правопорушниць, сигналізуючи про те, що їх поведінка не є непоміченою, тому не дивно, що навіть таке наддержавне інтеграційне об'єднання як Європейський Союз фактично скористалось можливостями публічної атрибуції кібератак. 30 липня 2020 року Рада Європейського Союзу ввела санкції проти фізичних та юридичних осіб, причетних до кібератак, що загрожують Європейському Союзу та походять з Союзу або інших держав, що не входять в його склад. Зокрема, обмежувальні заходи зачепили шість індивідів та три юридичні особи, пов'язані з такими кібератаками як «WannaCry», «NotPetya», «Operation Cloud Hopper» та кібератаками проти Організації з заборони хімічної зброї [74, с. 12-17]. Введені санкції передбачають заборону на виїзд, замороження активів та заборону для осіб та структур ЄС надавати кошти тим, хто перерахований в рішенні.

Загалом не можна говорити, що мова йде про публічну атрибуцію кібератак державі в її традиційному розумінні, але використовуючи інструмент кіберсанкцій проти індивідів, які є державними агентами, очевидним є встановлення джерела кібератаки – держави. Цей факт також підтверджує «Заява МЗС Росії про чергові нелегітимні обмежувальні заходи Європейського союзу проти Росії» [21]. Вже з самої назви заяви випливає, що РФ розглядає індивідуальні санкції як такі, що стосуються держави, оскільки складно уявити собі ситуацію, за якої військовослужбовці Збройних сил Російської Федерації діють з власної ініціативи, особливо в таких масштабах.

Найважливішим для України є наявність в списку Головного центру спеціальних технологій Головного Управління Збройних сил Російської Федерації (військова частина 74455, що знаходиться за адресою вул. Кірова, 22, м. Москва). По-перше, встановлена відповідальність центру за кібератаки, що завдали значної шкоди та представляють зовнішню загрозу для Союзу або його держав-членів, а також мали значний вплив на треті держави (зокрема, «NotPetya» або «EternalPetya» у червні 2017 року та кібератаки, спрямовані проти українських енергосистем взимку 2015 та 2016 років) [74, с. 12-17].

Особливий резонанс серед держав викликала кібератака «NotPetya» або «EternalPetya», що зробила для ряду компаній в Європейському Союзі, Європі та в усьому світі дані недоступними. Блокування доступу до таких даних спричинило, серед іншого, значні економічні втрати. В той час як кібератака на українську електромережу призвела до відключення її частин взимку виключно в Україні. Звичайно той факт, що кібератака «NotPetya» зачепила інтереси країн-членів ЄС стала важливим тригером для застосування та прийняття кіберсанкцій та здійснення атрибуції кібератаки.

Таким чином, розглядаючи питання застосування звичаєвих норм до кібернетичних атак проти об'єктів критичної інфраструктури, важливо пам'ятати, що юридична атрибуція є тим пунктом призначення, до якого не можна дістатись без здійснення технічної та політичної атрибуції. Останні два види атрибуції є взаємно компенсуючими, оскільки технічні індикатори можуть бути сфальсифікові, і у держави не завжди наявні необхідні людські та технічні ресурси для їх ідентифікації. Напроти, оцінка виключно політичних індикаторів не завжди може привести до держави-правопорушниці. Крім того, позитивним є те, що цей вид атрибуції створює певне поле для реакції держави, яка звинувачується у здійсненні міжнародно-протиправного діяння.

Як зазначалося вище, пандемія COVID-19 значно активізувала шкідливу діяльність в кіберпросторі, зокрема проти об'єктів охорони здоров'я. Така статистика щодо закладів критичної інфраструктури, що ведуть боротьбу з коронавірусною інфекцією, добре демонструє як збільшення шкідливої діяльності в Інтернеті, так і потребу у відповідній реакції. Звичайно, ми не стверджуємо, що за всіма цими атаками стоять держави, але важко встановити, що могло стати мотивацією індивідів чи груп, які стоять за ними. Крім того, в світлі пропаганди, яку поширювали державні медіа певних країн, складається враження, що такі атаки були спрямовані на досягнення держаних стратегічних цілей щодо посилення позиції держави у світі. В будь-якому випадку ці атаки ще раз підтверджують необхідність механізму, який би займався технічною і юридичною атрибуцією.

Важливим кроком у формуванні міжнародно-правового регулювання поведінки держав в кіберпросторі стала Заключна Доповідь Групи урядових експертів ООН щодо заохочення відповідальної поведінки в кіберпросторі в контексті міжнародної безпеки від 28 травня 2021 року, включена в Резолюцію Генеральної Асамблеї від 14 липня 2021 року. Попри відсутність юридично обов'язкового характеру, в підготовці доповіді брали участь експерти з 25 країн: Австралії, Бразилії, Німеччини, Індії, Індонезії, Йорданії, Казахстану, Кенії, Китаю, Маврикія, Марокко, Мексики, Нідерландів, Норвегії, Російської Федерації, Румунії, Сінгапуру, Сполученого Королівства Великобританії та Північної Ірландії, Сполучених Штатів Америки, Уругваю, Франції, Швейцарії, *Естонії*, Південної Африки та Японії.

Список держав дає підстави вважати, що у порівнянні з 2013-2015 роками все-таки вдалось досягти певного консенсусу щодо застосування норм міжнародного права в кіберпросторі. Так, наприклад, відповідно до норми 13 (b) «у разі виникнення інцидентів у сфері ІКТ держави мають вивчити всю відповідну інформацію, у тому числі ширший контекст події, проблеми встановлення відповідальності в ІКТ-середовищі, а також характер та масштаби наслідків». Ця норма є літературним перекладом з російської на українську, в якій, як видно, акцент робиться на «встановленні відповідальності» [11, с. 11]. Втім, в англомовній версії мова про «проблеми *атрибуції* в ІКТ-середовищі» («the challenges of *attribution* in the ICT environment») [194, с. 9]. Цікаво, що, попри офіційний характер англійської та російської версій, їх аналіз свідчить про деякі розбіжності в розумінні тих норм, що були включені в доповідь. Адже не варто ототожнювати «встановлення відповідальності» з «атрибуцією», оскільки перше поняття є більш широким та включає в себе атрибуцію.

Незважаючи на необов'язковий характер цього документа, одразу відзначимо певні переваги. У доповіді не згадуються кібератаки, фактично вона ґрунтується на нейтральному підході до інформаційно-комунікаційних технологій, що гарантує захист від швидкого розвитку ІКТ-технологій. Якщо юридично обов'язковий інструмент буде прийнято, то саме включення цього

принципу може забезпечити його «актуальність» після того, як він вступить в силу. Водночас складно уявити як і ким цей інструмент буде розроблятися в силу наявності двох паралельних процесів для обговорення відповідальної поведінки держав у кіберпросторі, а саме – Групи урядових експертів ООН та Відкритої робочої групи, що були створені Першим комітетом Генеральної Асамблеї ООН в 2018 році.

Водночас параграф 24 цієї Доповіді, свідчить про визнання необхідності врахування технічних та політичних індикаторів при зловмисному використанні ІКТ. Наприклад, Група урядових експертів підкреслює, що постраждала держава повинна враховувати всі аспекти при оцінці інциденту, а саме: «аспекти, підкріплені фактами, які можуть включати технічні характеристики інциденту; сферу охоплення, масштаби та вплив; більш широкий контекст, включаючи вплив інциденту на міжнародний мир і безпеку; і результати консультацій між зацікавленими державами» [194, п. 24].

Таким чином, здійснення технічної та політичної атрибуції кібератак є важливим для встановлення джерела кібератаки, оскільки в сукупності ці індикатори сприяють встановленню відповідальної держави. Важливо також, щоб держави слідували практиці публічної атрибуції кібератак. З одного боку, це дозволяє стримувати кібератаки, сигналізуючи про можливість атрибуції кібератаки конкретній державі. З іншого боку, атрибуція кібератаки зі згадкою про порушені норми може стати підтвердженням наявності юридичного спору, який пізніше може бути розглянутий в міжнародних судових інстанціях. Логічним завершення технічної та політичної атрибуції кібератак, як вже неодноразово зазначалося, має стати юридична атрибуція кібератак.

2.5. Кібератаки проти об’єктів критичної інфраструктури України в контексті збройного конфлікту на сході України як приклад атрибуції на підставі оцінки технічних та політичних індикаторів

Небезпеку та потенційні наслідки кібератак неможливо переоцінити, особливо тоді, коли їх основною ціллю є критична інфраструктури держави. Наша залежність від об’єктів критичної інфраструктури беззаперечна – такі об’єкти не просто лежать в основі повсякденного життя людей, а й стали його важливою частиною. Так, наприклад, електромережі, які розподіляють електроенергію серед населення, підтримують опалення та обслуговують державну економіку. Без належної роботи систем електропостачання країна та її жителі можуть зіткнутися з проблемою відсутності їжі, медичного обслуговування, питної води, опалення взимку або кондиціонування влітку.

Беручи до уваги їх критичну важливість для функціонування держави та забезпечення добробуту населення, атрибуція таких кібератак має знаходити свого «адресата», що фактично стоїть за ними, особливо коли за такими кібератаками стоїть держава. В протилежному випадку, культура безкарності призведе до толерування кібератак проти критичної інфраструктури, в результаті чого світ ризикує зіткнутись з серйозними гуманітарними наслідками.

Збільшення кількості кібератак проти систем електропостачання та інших індустріальних систем показує, що хакери стали більш майстерними в використанні кіберпростору проти таких систем, незважаючи на те, що такі системи відносно відключені від Інтернету. Окрім атак на українські електромережі, кібератаки на промислові системи здійснювались і в інших країнах. Зокрема, напади на постачання електроенергії в Південній Африці, ядерну установку в Індії, а також напади на металургійний комбінат у Німеччині та нафтохімічну компанію в Саудівській Аравії [60].

З кожним днем кібератаки проти індустріальних систем, зокрема електроенергетичних, стають дедалі складнішими, і, враховуючи ресурси та час, необхідні для вчинення таких кібератак, існує висока вірогідність того, що за

виконавцями стоять уряди, які їх прямо чи опосередковано підтримують та/або контролюють хід кібероперацій.

Актуальність атрибуції кібератак проти об'єктів критичної інфраструктури ще більше підвищується, коли такі кібератаки пов'язані зі збройним конфліктом або є його складовою. В цьому плані кібератаки на українські електромережі виділяються із-поміж подібних, оскільки кібератаки проти об'єктів критичної інфраструктури України пов'язані зі збройним конфліктом. Такі кібератаки цілком вірогідно могли б розглядатися в якості воєнних злочинів [209, с. 391], заборона яких має статус *jus cogens* та характер *erga omnes* [53, с. 63-64].

Перед тим як перейти до безпосереднього аналізу кібератак 2015 та 2016 років зазначимо, під системами електропостачання України розуміються системи та їх об'єкти, пов'язані з виробництвом, передачею, розподілом та постачанням електричної енергії (системи передачі, системи розподілу, електростанції, електроустановки тощо) в розумінні Закону України «Про ринок електричної енергії» [30]. Всі ці системи та об'єкти входять в поняття «критична інфраструктура», що міститься в Проекті Закону «Про критичну інфраструктуру» від 09.03.2021, що наразі очікує на друге читання [27].

Офіційною датою початку агресії Російської Федерації проти України вважається 20 лютого 2014 року – захоплення Збройними Силами РФ Автономної Республіки Крим. Ця дата фактично підтверджується Міністерством оборони Російської Федерації, яке зазначає її на відомчій нагороді «За повернення Криму» [43]. Попри засудження на міжнародному рівні [39], окупація Криму стала лише початком широкомасштабної операції проти України, що загалом включає різноманітні елементи гібридної війни проти України (включаючи кібератаки), та перекинулась на східну частину України. Відтак, в даному підрозділі увага приділятиметься кібератакам проти систем енергопостачання України, що сприяли просування цілей Російської Федерації, та політичним індикаторам, які демонструють причетність Росії до кібератак 2015 та 2016 років проти об'єктів енергетичного сектору України.

Відповідно до офіційної позиції Прокурора Міжнародного кримінального суду збройних конфлікт міжнародного характеру на Сході України почався якнайпізніше з 14 липня 2014 року [23, п. 169]. В той час як кібератаки мали місце в 2015 та 2016 роках, що виключає будь-які сумніви щодо наявності збройного конфлікту на час здійснення кібератак.

Кібератаки 2015 та 2016 років не спричинили фізичного руйнування, але є досить показовими. Попри те, що деструктивний потенціал даних кібератак не вдалось в повній мірі реалізувати, вони не можуть розглядатися в якості простої зловмисної діяльності, оскільки безпосередньо пов'язанні з досягненням поставлених воєнних цілей.

23 грудня 2015 року група хакерів здійснила кібератаку на електростанції України – це була перша підтверджена кібератака, яка вивела з ладу систему електропостачання держави. Кібератака була спрямована насамперед на три регіональні електророзподільні компанії (обленерго). Зловмисники використовували фішингові листи, що містили вкладення Microsoft Office, заражені шкідливим програмним забезпеченням BlackEnergy 3, викрадення облікових даних, доступ до VPN та інші технічні засоби, щоб отримати доступ до комп'ютерів компанії та систем SCADA. В результаті втручання в систему обленерго сталося кілька відключень, які торкнулися близько 225 тисяч споживачів у різних регіонах і тривали кілька годин.

Під час спільного аналізу кібератаки проти українських енергосистем Центр обміну та аналізу інформації про електроенергію (Electricity Information Sharing and Analysis Center) та експерти Промислової системи управління (SANS Industrial Control System) SANS дійшли висновку, що «[к]іберопераційна була високо синхронізованою, і противник був готовий шкідливим чином керувати системою SCADA, щоб спричинити перебої з електроживленням з послідуючими руйнівними атаками задля відключення системи SCADA та системи комунікації. Руйнівна складова – перший випадок у світі, коли спостерігається такий тип атаки як атака на системи операційних технологій критичної інфраструктури країни» [237].

Що важливо, експерти атрибутують кібератаку 2015 року групі хакерів Sandsworm [82, с. 10]. Ця група хакерів добре відома тим, що використовує шкідливі програми BlackEnergy та атакує різні мережі, що управляють промисловим фізичним обладнанням. Коли інженери FiveEye в 2014 році отримали доступ до незахищених командно-адміністративних серверів Sandsworm, вони виявили спосіб роботи BlackEnergy завдяки інструкціям та іншим файлам, написаним російською мовою. Мова файлів та той факт, що атаки, розпочаті Sandsworm, відображають стратегічні інтереси Російської Федерації, є одними із основних причин, чому ця група хакерів, як вважають, має міцний зв'язок з Російською Федерацією [136]. Крім того, за даними Міністерства енергетики України, хакери здійснювали телефонні дзвінки з Російської Федерації та в ході кібератаки на українську систему електропостачання використовували російського провайдера Інтернету [188].

Кібератаки на українські установи та об'єкти критичної інфраструктури не виглядають випадковими у світлі триваючого збройного конфлікту. 29 грудня 2015 року Президент України зробив офіційну заяву та повідомив, що протягом останніх двох місяців було здійснено 6500 кібератак проти 5 агентств та 31 державного інформаційного ресурсу. Він також додав, що слідство свідчить про пряму чи опосередковану участь Російської Федерації [24].

Час, вибраний для кібератаки 2015 року та воєнні дії, що мали місце в даний проміжок часу, також можуть пролити світло на деталі кібератаки. По-перше, день нападу повинен був стати днем припинення вогню, оскільки Тристороння контактна група домовилася про припинення вогню на час Різдва та Нового року, починаючи з опівночі 23 грудня 2015 року.

22 грудня 2015 року Міністерство оборони України повідомило, що важко озброєна група ДНР увійшла в село Комінтернове, яке на той час знаходилось у сірій зоні, поблизу стратегічного порту міста Маріуполя. Присутність озброєних членів «ДНР» у селі підтвердила місія ОБСЄ, якій було відмовлено у доступі в це село [156]. Присутність групи «ДНР» у сірій зоні розцінювалася як своєрідна помста за операцію українських сил у с. Павлополі, що протягом кількох місяців

перебувало в сірій зоні, та за отримання контролю над сімома селами в грудні [242].

Однак серйозна ескалація до та під час кібератаки спостерігалася також у Луганській області. Наближаючись до контрольованого «ЛНР» с. Калинове, «СММ спостерігала, як одна ракета була випущена із системи багаторазового запуску (РСЗВ, ВМ-21 «Град», 122 мм) […]. СММ оцінила, що ракету, яку вона побачила, було випущено в північно-західному напрямку. Це було вдруге за менше ніж тиждень, коли СММ спостерігала використання РСЗВ у с. Калинове» [156].

Верховний головнокомандувач Об'єднаних сил НАТО Ф. Брідлов також зауважив підтримку Росією проксі на Сході України та численні конвої на Донбасі, позначені як гуманітарна підтримка в цей проміжок часу [110]. Навряд чи можна повірити, що збільшення «гуманітарної підтримки», вхід ДНР до сірої зони за день до кібератаки та використання забороненої зброї в Луганській області – звичайний збіг обставин, який не має нічого спільного зі скоєною кібератакою в день припинення вогню. На противагу цьому, логічним є висновок про те, що ці заходи здійснювалися з метою зміцнення позицій збройних формувань; і що кібератака могла зіграти ключову роль у дестабілізації політичної ситуації та воєнних позицій України.

Нарешті, ситуацію навколо Кримського півострова можна розглядати як каталізатор відключення електромереж 2015 року. Незабаром після анексії Криму місцева влада розпочала процес націоналізації українських енергетичних компаній. Група невстановлених людей напала на лінії електропередач, які постачали електроенергію з України до Криму. Хоча проукраїнські активісти так званої «Громадянської блокади Криму» та кримських татар перешкоджали ремонту пілонів, підірваних 22 листопада 2015 року, вони заперечували свою відповідальність за підрив. У будь-якому випадку, кібератака 2015 року може бути прямим наслідком і реваншем за відключення Криму [87].

Майже одразу після першої кібератаки на електромережу в 2015 році Служба безпеки України заявила, що за цією атакою стоять російські спецслужби [205].

За традицією 17 грудня 2016 року українська критична інфраструктура була знову атакована. У порівнянні з кібератакою 2015 року, кібератака 2016 року на українську електромережу мала менший масштаб та наслідки. Однак, з точки зору намірів виконавців, атака 2016 року була більш складною і могла призвести до більш серйозних наслідків [83, с. 2, 13-15]. Фактично кібератака призвела до відключення в певних районах столиці, яке тривало одну годину п’ятнадцять хвилин.

Також є різниця в обраній цілі. У 2015 році кібератаку було направлено на електророзподільну систему. При найгіршому сценарії це могло спричинити відключення в обмежених географічними рамками районах. Напад на систему передачі, який стався в 2016 році, навпаки, потенційно міг призвести до миттєвих неконтрольованих каскадних відключень енергосистем. Відтак, внаслідок каскадних відключень постраждала б набагато більша кількість населення в межах більш широкого географічного району, а компоненти енергосистеми могли бути настільки серйозно пошкоджені, що їх неможливо або важко було б замінити [137].

На думку експертів Dragons Inc., «CRASHOVERRIDE з миттєвої аварії переходить в стан відкладеної атаки, що передбачає фізичне знищення. […], порушення в системі передачі через маніпуляції з віддаленим термінальним блоком (RTU) є попередником завершального, більш серйозного етапу: гальмування систем захисту, тому при відновленні обслуговування цільова схема перестає бути безпечною і піддається пошкодженню» [83, с. 9].

Дослідники фірми Dragon також дійшли висновку, що мета використання CrashOverride полягала не в короткочасному відключенні, а в створенні тривалого руйнівного сценарію, який міг призвести до каскадного відключення протягом тижнів або навіть місяців. Цей факт ставить це зловмисне програмне забезпечення в один рядок з найнебезпечнішими кодами, які коли-небудь

використовувались для знищення фізичних компонентів промислових систем (зокрема, поряд зі шкідливим програмним забезпечення Stuxnet, яке наприкінці 2009 року – на початку 2010 року знищило п’яту частину іранських збагачувальних центрифуг, та зловмисним програмним забезпечення Triton, яке було розроблено та використано для атаки на нафтопереробний завод у Саудівській Аравії у 2017 році) [131].

Якщо придивитись до збройного конфлікту на Донбасі у відповідний проміжок часу, помітно, що в день атаки 2016 року конфлікт значно загострився. Зокрема, про збільшення кількості обстрілів повідомив прес-центр АТО 17 грудня [13], тоді як 18 грудня неурядові збройні угруповання розпочали наступ, щоб відтіснити позиції українських військових [34]. Звіт СММ ОБСЄ підтверджує загострення ситуації та наводить досить важливі цифри: «СММ зафіксувала більше порушень режиму припинення вогню в Донецькій області як 17, так і 18 грудня, у тому числі 700 та 2900 вибухів відповідно, порівняно зі 100 вибухами у попередньому звітному періоді» [157]. Як і у випадку з кібератакою 2015 року, така активізація в день кібератаки та одразу після неї не виглядає випадковою і може розглядатися як частина цілісної операції проти України.

Важливо, що небезпечні можливості CrashOverride можуть бути використані для автоматизованих кібератак, що здатні відключати системи подачі енергії, проти інших держав та водних, транспортних і газопровідних об’єктів критичної інфраструктури. Для цього код достатньо трохи переписати та адаптувати до протоколів певної держави. Роберт М. Лі, засновник фірми Dragos і колишній аналітик розвідки, що займався безпекою критичної інфраструктури, прийшов до такого висновку: «Те, як воно [програмне забезпечення] створене, розроблене та запущене дозволяє припустити, що його планують використовувати багато разів. І не лише проти України» [81].[4]

[4] Наукові результати щодо атрибуції кібератак проти об’єктів електропостачання України у 2015 та 2016 року були висвітлені в наступній публікації: Analysis of cyber-attacks on Ukrainian power grid systems in the context of armed conflict in Donbas. Constitutional State. № 39. 2020. С. 78-85.

Хоча розслідування кібератак 2015 та 2016 років проводилося державними та приватними агентами (українськими та закордонними), ці атаки не привернули достатньої уваги. Фактично до 30 липня 2020 року було взагалі не зрозуміло, як оцінювати ці атаки з юридичної точки зору. Попри те, що в 2015 році близько 250 тисяч людей залишилися без електропостачання на годину, жоден національний уряд не висловив офіційне засудження даної кібератаки. Така практика, на думку науковців та IT-спеціалістів, призвела до нормалізації цих кібератак, тобто стала «новим нормально» або «прийнятною девіацією (відхиленням)». Аналогічний підхід був продемонстрований після кібератаки 2016 року, але з урахуванням того, що дану кібератаку було виконано одним мережевим пластом нижче, вона все-таки повернула увагу до кібератак через декілька років [154].

Така практика нормалізації кібератак проти об'єктів критичної інфраструктури породила, зокрема, кібератаку «NotPetya» та сприяла тому, що виконавці кібератак почали шукати нові, більш прогресивні шляхи для нападу на інфраструктуру держав. Як зазначила в інтерв'ю тодішня міністр охорони здоров'я Уляна Супрун, кібератака повернула Міністерство на 30 років назад. Так, наприклад, міністерство здійснює централізований розподіл ліків на територію всіх областей України в ситуаціях, коли лікарнях, що знаходяться на їх території, відсутні необхідні для пацієнтів ліки. В такому випадку міністерство направляє їх самостійно або це робиться з території іншої області, якщо в міністерстві відсутні запитувані ліки. Для запиту та передачі ліків загалом достатньо одного електронного листа, в копію якого додаються відповідальні особи з 24 областей України. Але в день кібератаки єдиним засобом зв'язку був телефон, тому співробітникам Міністерства замість написання і відправки одного листа потрібно було зробити 24 дзвінка в області для отримання інформації щодо наявності запитуваних ліків. Складнощі також були з формуванням звітної інформації щодо кількості медичних установ, які постраждали внаслідок «NotPetya», оскільки не було можливості з ними зв'язатися [57]. І це лише приклад одного міністерства. Складно уявити наслідки

кібератак 2015 та 2016 років проти електроенергетичних систем, якби задум щодо їх використання вдалось реалізувати в повній мірі.

Водночас розуміння потенційних наслідків цих та інших кібератак кібератак дало сильний імпульс для збільшення кількості централізованої публічної атрибуції кібератак з боку держав. У 2017 році кібератаку «WannaCry» атрибутували Північній Кореї та Lazarus Group, які нібито діяли від імені уряду Північній Кореї. А у 2018 році кампанія кібератак групи APT 10, спрямована на об'єкти інтелектуальної власності та конфіденційні комерційні дані в Європі, Азії та США, була публічно присвоєна уряду Китаю. Тоді ж у 2018 році Великобританія, Данія, США, Канада та Австралія публічно атрибутували кібератаку «NotPetya» Уряду Російської Федерації. Важливо, що Великобританія була першою державою, яка заявила, що «російський уряд, а саме російські військові, несуть відповідальність за руйнівну кібератаку NotPetya, що мала місце у червні 2017 року» [136]. Нова Зеландія, Норвегія, Литва, Естонія, Латвія, Швеція та Фінляндія приєдналися до них, поширивши відповідні заяви про підтримку. Білий дім США теж визнав, що атака NotPetya «... була частиною постійних зусиль Кремля щодо дестабілізації ситуації в Україні і все чіткіше демонструє участь Росії у триваючому конфлікті» [218].

Нарешті, через більш ніж три роки після кібератаки 2015 року Європейський Союз приймає важливе рішення, що передбачає використання цілеспрямованих обмежувальних санкцій за кібератаки, що становлять зовнішню загрозу для ЄС або його членів. В якості таких, відповідно до рішення Ради від 17 травня 2019 року, розглядають кібератаки зі значним ефектом, джерело походження яких не знаходиться на території ЄС. Рішення Ради охоплює не лише кібератаки, «спрямовані» чи здійсненні «під контролем», але й кібератаки, що «підтримуються» фізичними або юридичними особами [73].

30 липня 2020 року Європейський Союз підтвердив відповідальність Головного управління Збройних Сил РФ за кібератаки 2015 та 2016 років. Відповідно до рішення Ради, «Головний центр спеціальних технологій Головного управління Генерального штабу Збройних Сил Російської Федерації

(ГРУ)... несе відповідальність… за кібератаки зі значним ефектом проти третіх держав, включаючи кібератаки, публічно відомі як «NotPetya» або «EternalPetya» у червні 2017 року та кібератаки, спрямовані на українську електромережу взимку 2015 року та 2016 року» [78]. Важливо одразу відмітити позитивний вплив такого рішення ЄС, адже встановлення правди та відповідальності є особливо актуальним для держав, що втягнуті в збройні конфлікти [187, с. 60-61].

Аналіз даних кібератак і результатів атрибуції демонструє важливість співпраці на початковому етапі з приватним сектором, який може допомогти з атрибуцією – підтвердивши або спростувавши її. Крім того, ситуація України, а саме здійснення кібератак в контексті збройного конфлікту на сході України демонструє важливість оцінки політичних індикаторів – оцінки контексту, зв'язку між приватними акторами та іноземною державою тощо.

Важливо розуміти, що кібератаки не можна відділяти від політичного контексту. Їх не вчиняють просто так, і кожна кібератака має свою ціль. У випадку з досить складними кібератаками гіпотеза щодо причетності вороже налаштованої держави повинна детально розроблятися, а формування юридичної позиції щодо атрибуції кібератак мають стати логічним завершення для боротьби з міжнародно-протиправними діяннями.

На відміну від неурядових акторів, держави ніколи не вдаються до кібератак без будь-яких на те причин. Адже такі кібератаки вимагають значних ресурсів, витрачати які безцільно сучасна держава навряд чи буде. Наявна практика свідчить про те, що в кіберпросторі держави завжди переслідують свої геополітичні цілі, і саме ці цілі на початковому етапі є ключем до ідентифікації держави-правопорушниці, що стоїть за кібератакою. Відтак, приклад України є показовим та демонструє важливість врахування політичних індикаторів для атрибуції кібератак, зокрема загального контексту.

Висновки до другого розділу:

1. Наразі конвенційні поняття «об’єкт критичної інфраструктури» або «критична інфраструктура» в міжнародному праві відсутні, що зумовлює необхідність звернення до підходів держав, які надають відповідні дефініції в своєму національному законодавстві. Залежно від країни, законодавство якої аналізувалося, згадка про «об’єкти критичної інфраструктури» або «сектори (підсектори) критичної інфраструктури» не завжди була присутня. Іноді використовувалося виключно поняття «критична інфраструктура». Проте, поняття «критична інфраструктура» охоплює всі об’єкти критичної інфраструктури, які можуть бути об’єднанні в сектори (підсектори) та/або мають спільну функціональну спрямованість.

2. Важливо, що визначення критичної інфраструктури є першим необхідним кроком у формуванні політики безпеки та стійкості критичної інфраструктури до кібератак. Деякі визначення характеризують критичну інфраструктуру як інфраструктуру, функціонування якої є життєвонеобхідним або важливим для економічного та соціального добробуту, тоді як інші – наголошують на їх важливості для функціонування держави або національної безпеки. Крім того, кількість секторів критичної інфраструктури варіюється від країни до країни – одні держави визначають лише 2 сектори в якості критичних, інші – доходять до 16-18. Вважаємо, що перший підхід є надто вузьким, а другий – занадто інклюзивним.

Не дивлячись на те, що Група урядових експертів залишає категоризацію об’єктів критичної інфраструктури на розсуд держав, підходи держав свідчать про необхідність прийняття поняття «критична інфраструктура». При розробці конвенційного поняття «критична інфраструктура» необхідно також визначити критерії оцінки критичної окремих об’єктів, зокрема, масштаб потенційних наслідків у випадку порушення нормального функціонування об’єкта критичної інфраструктури, вразливість та взаємозалежність з іншими об’єктами критичної інфраструктури, тривалість та серйозність наслідків, що викликані

пошкодженням, знищенням, поломкою або функціональним збоєм тощо. Важливим є також відокремлення транснаціональних (міждержавних) об'єктів критичної інфрастуктури від національних.

3. Підвищення поваги та підтримання авторитету норм міжнародного права не можливе без встановлення відповідальності держав, які стоять за міжнародно-протиправними діяннями. Це випливає із правосуб'єктності держав та з факту того, що держави є головними носіями міжнародних зобов'язань, які вправі створювати правила поведінки та впливати на міжнародний правопорядок. В силу того, що спеціальні правила щодо атрибуції кібератак в міжнародному праві відсутні, застосовуються підстави атрибуції поведінки державі, що містяться в Статтях про відповідальність за міжнародно-протиправні діяння. Статті про відповідальність не мають юридичного обов'язкового характеру, оскільки є доктриною та розроблені Комісією ООН з міжнародного права, але більшість норм набула звичаєвого характеру, що виправдовує їх застосування до кібератак.

В контексті кібератак, в першу чергу, у фокус аналізу потрапляє стаття 4 щодо поведінки органів держави, стаття 5 щодо поведінки індивідів чи юридичних осіб, що уповноважені здійснювати елементи урядових повноважень, стаття 8 щодо поведінки осіб чи групи осіб, що діють під керівництвом чи контролем держави.

4. Дії кіберармій чи інших державних суб'єктів атрибутуються державам відповідно до норм міжнародного права відповідальності держав, навіть якщо національному органу у такому статусі відмовлено за національним законодавством (стаття 4). Діяння цього органу в кіберпросторі, що має характер, *ultra vires,* також атрибутуватиметься державі, як це встановлює загальне право відповідальності держав, закріплене в статті 7 Статей про відповідальність.

Атрибутуватись державі в кіберконтексті буде і поведінка індивідів чи юридичних осіб, що уповноважені здійснювати елементи урядових функцій. В кіберконтексті серед звичних для держави функцій, *inter alia*, виділяється кіберрозвідка та оборонні кібероперації. Лише поведінка, яка пов'язана із

виконання елементів урядових функцій, буде атрибутуватись держави. Діяльність приватної компанії, яка не пов’язана з урядовими функціями та здійснюється цією приватною компанію на вимогу приватних корпорацій, неурядових організацій або є проявом кіберзлочинної діяльності атрибутуватись державі не буде.

Стаття 8 Статей про відповідальність держав передбачає, що поведінка недержавних акторів атрибутується державі лише якщо вона керувала або контролювала конкретну операцію і поведінка, на яку скаржилися, була невід’ємною частиною цієї операції. Відтак, необхідним є здійснення ефективного контролю. Саме держава повинна визначати виконання та хід конкретної операції, а кібердіяльність, якою займається недержавний суб’єкт, має становити «невід’ємну частину» операції держави.

5. В силу обмежених людських та технічних ресурсів, шанси постраждалої держави присвоїти кібератаку державі були досить мізерними, тому поруч із юридичною атрибуцією (саме вона є одним із елементів міжнародно-протиправного діяння), виникає технічна та політична атрибуція кібератак. Їх можна розглядати як цілком не пов’язані між собою, або, навпаки, як частини цілого. Технічна атрибуція представляє криміналістичне розслідування, яке має на меті отримання прямих доказів щодо здійсненої кібератаки, тобто цифрових криміналістичних доказів. В той час як політична атрибуція ставить на меті визначити, хто причетний до кібератаки – індивід чи держава, та ґрунтується на політичному аналізі. Логічним завершенням цього ланцюжка атрибуцій повинна стати юридична атрибуція, яка не можлива без технічної та політичної атрибуції. Аналіз *opinio juris* держав свідчить про бажання та готовність атрибутувати кібератаки відповідальним державам, але юридична атрибуція, очевидно, є останнім кроком, який держави готові зробити.

6. В ході політичної та технічної атрибуції здійснюється оцінка політичних та технічних індикаторів. Може виникнути логічне питання щодо доцільності оцінки політичних індикаторів, але без їх врахування важко забезпечити достовірність атрибуції. І держави, і приватний сектор визнають, що

технічні індикатори можуть бути сфальсифіковані, тому паралельно мають оцінюватися політичні індикатори і за наявності враховуватися дані розвідки.

7. Відповідно до принципу необхідної обачності (*due diligence*) держава повинна проявляти належну обачність, не дозволяючи використовувати свою територію чи кіберінфраструктуру під своїм урядовим контролем для кібероперацій, які зачіпають права інших держав та спричиняють серйозні несприятливі наслідки для них. Юридично обов'язкова природа даного принципу в кіберпросторі часто ставиться під питання. Разом з тим, позицію про те, що *due diligence* є загальним міжнародним зобов'язанням та становить *lex lata*, підтримали такі держави як Австралія, Чеську Республіка, Естонія, Нідерланди, Фінляндія та Франція.

8. Кібератаки на промислові системи управління особливо небезпечні при їх використанні проти об'єктів критичної інфраструктури, без належного функціонування яких люди можуть страждати від нестачі їжі, води, електроенергії, медичного обслуговування тощо. Відтак, потенційне порушення низки фундаментальних прав, яке на тривалий час унеможливлює їх реалізацію, дозволяє розглядати це зобов'язання в рамках міжнародного права прав людини, яке є спеціальним та досить сильним правовим режимом. Горизонтальний ефект прав людини та зобов'язання *due diligence* в контексті прав людини не одноразово було підтверджено у висновка спеціалізованих міжнародних установ, включаючи судові. Зобов'язання необхідної обачності в межах міжнародного права прав людини, що є спеціальним та жорстким міжнародно-правовим режимом, дозволяє говорити про атрибуцію кібератак проти об'єктів критичної інфраструктури у випадку потенційної загрози для життя та здоров'я населення.

9. Дослідження кібератак 2015 та 2016 років проти України демонструє їх небезпеку для об'єктів критичної інфраструктури та важливість вивчення загального контексту, в якому були здійснені кібератаки. Хоча кібератаки на українські енергосистеми не спричинили фізичного руйнування, досвід України є прикладом того, як кібератаки можуть бути використані проти об'єктів

критичної інфраструктури. Такі кібератаки не повинні розглядатися як проста шкідлива кібердіяльність, оскільки вони мали місце у воєнний час. Вони не виглядають випадковими у світлі триваючого збройного конфлікту. Час, обраний для кібератак, та воєнні дії на сході Донбасу до та після кібератак, свідчать про пряму чи опосередковану участь Російської Федерації.

Аналіз даних кібератак і результатів атрибуції демонструє важливість співпраці на початковому етапі з приватним сектором, який може допомогти з атрибуцією – підтвердивши або спростувавши її. Крім того, ситуація України, а саме здійснення кібератак в контексті збройного конфлікту на сході України демонструє важливість оцінки політичних індикаторів, а саме – контексту, зв’язку між приватними акторами та іноземною державою, мотивацію останньої та стратегічні інтереси тощо.

РОЗДІЛ 3. ШЛЯХИ ВИРІШЕННЯ ОСНОВНИХ ПРОБЛЕМ, ПОВ'ЯЗАНИХ З АТРИБУЦІЄЮ КІБЕРАТАК

3.1. Співпраця з приватним сектором задля подолання перешкод атрибуції кібератак проти об'єктів критичної інфраструктури

Публічна атрибуція стала важливим кроком на шляху притягнення до юридичної відповідальності, але, незважаючи на її важливість, вона залишається в політичній площині. Відтак, держави змушені задуматись над шляхами вирішення проблеми атрибуції кібератак, які здійснюються як державою, так і приватними компаніями, ніяк не пов'язаними з державою.

Борючись з кібератаками здійсненими недержавними акторами за підтримки чи фінансування держав, держави-жертви кібератак не тільки зіштовхнулись з новими «ворогами», а й знайшли нових «партнерів» в середовищі компаній, що займаються питаннями кібербезпеки.

З одного боку, держави, які володіють значними кіберспроможностями, здатні самостійно здійснити атрибуцію кібератак, про що свідчать заяви та стратегії держав. Зокрема, найбільш активними в цьому плані є США та Великобританія. З промови міністра оборони США від 2012 року вбачається, що США має в своєму розпорядженні всі необхідні ресурси для того, щоб здійснювати атрибуцію та має намір притягнути винних до відповідальності в ситуації завдання шкоди державі та її громадянам [184]. Аналогічним чином канцлер Великобританії виразив позицію щодо того, що безкарності за здійснені кібератаки більше не існує [180].

З іншого боку, досить рідко централізована урядова атрибуція здійснюється самостійно, без взаємодії з приватним сектором та обміну інформацією [109, с. 528-530]. І це є цілком виправданим, оскільки, по-перше, у приватних ІТ-компаній чи компаній, що займаються кібербезпекою, може бути більше ресурсів, ніж у держав. По-друге, вони діють незалежно від них, здійснюють технічну атрибуцію в значно коротші строки та не стикаються з викликами на політичному рівні.

Логічним є запитання щодо мотивів приватного сектору, оскільки у більшості випадків приватні компанії приєднуються до процесу атрибуції за власною ініціативою. На нашу думку, такі дії вмотивовані як з гуманних міркувань, так і намаганнями підвищити репутацію та власну значимість на ринку. Так, наприклад, у 2013 році компанія Мандіант опублікувала безпрецедентний звіт, викриваючий діяльність китайської кібергрупи APT1, яка займалась тривалим кібершпигунством. Звіт готувався протягом 7 років та враховував активність групи проти 141 організацій, які були скомпрометовані APT1 та охоплювали 20 основних галузей промисловості. Він містив:

1. Докази, що пов'язують APT1 з 2-м бюро Народно-визвольної армії Китаю (PLA), відділом Генерального штабу, 3-м відділенням (найменування для прикриття військового підрозділу PLA 61398);
2. Хронологію економічного шпигунства APT1, починаючи з 2006 року;
3. Опис інструментів, тактики, процедури роботи APT1, включаючи компіляцію відео, що показують фактичну активність APT1;
4. Хронологію та відомості про понад 40 сімейств шкідливих програм APT1;
5. Хронологію та деталі розгалуженої інфраструктури атаки APT1 [165, с. 3-4].

Цікаво, що до цього, у 2010 році, Мандіант опублікував свій перший звіт щодо APT (Advanced Persistent Threat). Розслідування, які проводились з 2004 року для підготовки цього звіту, дозволили висунути гіпотезу про те, що близько двадцяти груп APT знаходяться в Китаї (APT1 – найбільш активна і успішна). Тоді Мандіант виразив позицію щодо того, що діяльність цієї кібергрупи могла санкціонуватися Урядом Китаю, визнаючи, що на той момент не представлялось за можливе встановити рівень причетності.

Звіт 2013 року, навпаки, містить докази причетності та наступний висновок: «Ми вважаємо, що APT1 здатний вести таку тривалу та розгалужену кампанію з кібершпигунства значною мірою тому, що отримує пряму підтримку уряду… [Н]аше дослідження дозволило встановити, що підрозділ 61398

Народно-визвольної армії (PLA) в своїй місії, можливостях та ресурсах аналогічний APT1. Підрозділ 61398 PLA також розташований у точно тій самій зоні, з якої розпочинається активність APT1» APT1 [165, с. 2]. Такий детальний звіт, представлений на оцінку широкому загалу, породив так званий «ефект Мандіанту»: відтепер компанії, що займаються кібербезпекою, переконані в тому, що задля загального визнання здійсненого аналізу та поваги, їх звіти не повинні поступатись деталізованому звіту від Мандіант.

Уже в 2014 році CrowdStrike, приватна компанія з кібербезпеки, публікує свій звіт, який заперечує твердження Китайського уряду щодо його непричетності до кібершпигунства [54] та наполягає на широкомасштабних кампаніях проти урядів та компаній, що базуються в різних країнах світу [89]. Цим самим, демонструючи системність проблеми та існування ряду небезпечних кібергруп.

Крім того, як видається з аналізу атрибуції кібератак 2014-2018 року, звіт Мандіант також призвів до активізації урядів. Можемо справедливо зробити висновок про те, що держави не хочуть втрачати свою позицію в кіберпросторі, який вони, хоча і не можуть контролювати в рамках власного суверенітету, не хочуть визнавати з домінуючою роллю приватного сектору. Але тут також важливим є той факт, що децентралізована атрибуція з боку недержавних акторів та їх готовність обмінюватися інформацією та спільно взаємодіяти, зводить до мінімуму ризик помилкової атрибуції.

Помилкова атрибуція внаслідок спуфінгу є тим, чого держави дуже бояться, адже, якщо держава здійснить помилкову атрибуцію та вдасться до реторсій чи контрзаходів або, що ще гірше, до застосування сили, то її дії розглядатимуться в якості міжнародно-протиправного діяння, яке не можна буде виправдати помилкою. Більш того, це може привести до відкритого реваншу з боку держави, яка стала жертвою спуфінгу. Тому державам варто визнати, що епоха державоцентризму залишилась в минулому, і для забезпечення власних інтересів та безпеки необхідно об’єднатися з тими компаніями, які готові співпрацювати.

На нашу думку, сценарій за яким і держави, і недержавні кіберактори проводять атрибуцію окремо один від одного має свої плюси, але більш ефективним буде об'єднати зусилля, оскільки кожна із сторін володіє перевагами, які не доступні іншій. Перевага, яка є у держав при атрибуції, полягає в тому, що вона прекрасно обізнана з власним історичним, соціальним, політичним та економічним контекстом, в якому була здійснена кібероперація проти її критичної інфраструктури.

Що ж до приватних компаній, то в їх розпорядженні часто знаходяться відомості низки компаній, що стали жертвами кібератак в різних країнах. Фактично, це і є тією причиною, яка, на нашу думку, дозволяє приватному сектору здійснити атрибуцію в короткі строки. Але і ці строки можуть скоротитися, якщо буде проходити періодичний обмін інформацією з державою. Тому, вважаємо, що доцільним є об'єднання зусиль державних та недержавних акторів, адже співпраця може стати тим важелем, який запустить юридичну атрибуцію кібератак для цілей притягнення держав до міжнародної відповідальності.

Експерти «Microsoft» пропонують найбільш оптимальний варіант міжнародного механізму, який би займався питаннями атрибуції. Зокрема, пропонується створити організацію, яка б включала не тільки державних, а й приватних технічних експертів, науковців, представників громадянського суспільства, що можуть оцінити тактику та прийоми, які використовують державні кіберактори, та інші індикатори, що демонструють причетність держави до кібератаки [66, с. 11].

Така централізована атрибуція при участі всіх зацікавлених сторін сприяла б не тільки здійсненню технічної атрибуції, а й досягненню стандарту доказування, який необхідно досягнути для цілей юридичної атрибуції. Завдяки атрибуції з високим рівнем підтвердження державам-жертвам кібероперацій вдасться притягнути іншу державу до міжнародної відповідальності, якщо остання фінансує та підтримує такі операції. Разом з тим, для міжнародної спільноти це шанс зменшити зростаючу кількість кібератак та ефективно

реагувати на порушення норм міжнародного права, зокрема в ситуаціях, коли кібероперації досягають порогу використання сили.

Цікаво, що, пропонуючи такий міжнародний механізм, експерти «Microsoft» надихнулися прикладом Міжнародної агенції з атомної енергії (МАГАТЕ). І тут важко не погодитися, оскільки цей механізм добре відомий своєю технічною експертизою.

Наразі до Ради керуючих МАГАТЕ входять 35 країн-членів (за географічною приналежністю), які змінюються на ротаційній основі, а процес прийняття Радою рішень, як правило, визначається консенсусом, що також є бажаним для майбутнього механізму з питань кібероперацій. Оскільки серед основних напрямів діяльності здійснення ядерних перевірок (зокрема, верифікаційної та моніторингової діяльності в Ірані з ціллю виконання резолюції РБ ООН 2231(2015)), виробництво медичних радіоізотопів та радіаційних технологій в рамках ядерного застосування, діяльність пов’язана з технологіями ядерного паливного циклу і матеріалів, тощо, діяльність організації неможлива без залучення технічних експертів, які проводять інспекції та розробки. Тому, фактично, історія наводить приклад механізму, який може бути використаний в якості моделі для механізму, що здійснюватиме атрибуцію кібератак.

Позитивним також буде створення виключно технічного механізму, який не прийматиме політичних рішень, а лише встановлюватиме факти. Оскільки навіть між приватними фірмами існує розрив в тим методах та інструментах, які вони використовують для здійснення атрибуції. Так, наприклад, Лабораторія Касперського (Kaspersky Lab) зазначила, що аналіз, проведений BAE та Anomali щодо зв’язку між групою Лазарус (Lazarus Group) та Північною Кореєю та їх причетністю до пограбування Центрального банку Бангладешу, невиправдано вузько зосереджений лише на коді інструмента «wiper». Що ж до аналізу та технічної атрибуції від Symantec, то причетність Lazarus Group виявлено завдяки повторному використанню ряду зловмисних програм під час атаки на польський фінансовий сектор [129; 96, с. 20].

На увагу також заслуговує пропозиція, що виключає участь агентів держави. Проте складно повірити в можливість створення такого механізму, який виключає роль держави в процесі здійснення атрибуції. По-перше, з суто політичних міркувань, держави не хочуть відходити на другий план та втрачати контроль над сферою, в якій вони зацікавлені. По-друге, відсутність урядових експертів позбавить можливості здійснювати обмін інформацією між державними агентами та приватним сектором. Разом з тим, пропозиції створення «бездержавного» міжнародного механізму для здійснення технічної атрибуції все ж існують.

Так, наприклад, Корпорація РЕНД (RAND) запропонувала створення Глобального консорціуму з кібератрибуції. Згідно із пропозицією Корпорації РЕНД цей консорціум повинен включати (1) технічних експертів компаній з питань кібербезпеки та інформаційних технологій, а також науковців та (2) експертів з кіберпростору, юристів-науковці та експертів з міжнародної політики з різних наукових та дослідницьких організацій. В консорціум повинно входити від 20 до 40 експертів з різноманітних організацій, серед яких РЕНД називає Лабораторію Касперських, Symantec, CrowdStrike, Microsoft, Huawei, ZTE, Інженерну Раду Інтернету (Internet Engineering Task Force – IETF), Інститут інженерів електротехніки та електроніки, Спільноту Інтернету (Internet Society), групу експертів Талліннського Керівництва.

На думку корпорації РЕНД, є три основні причини, чому держави не повинні допускатись до процесу атрибуції в межах створеного міжнародного механізму.

По-перше, держави здійснюють атрибуцію на підставі доказів та матеріалів розвідки, які вони не готові публічно оприлюднювати. Як наслідок, виникають обґрунтовані побоювання щодо достовірності та повноти доказів. По-друге, держави переслідують свої політичні інтереси. Представники РЕНД припускають можливий тиск з боку державних акторів, щоб отримати бажаний висновок від Консорціуму [97, с. 19]. І це дійсно можливо, якщо враховуватимуться не лише технічні індикатори, а й політичні індикатори та

інформація із різних джерел. Опиратись ж виключно на технічні індикатори стратегічно не правильно, оскільки технічні індикатори можуть бути сфальсифіковані [97, с. 16].

По-третє, у випадку членства в Консорціумі держави зможуть впливати на вибір справ для розслідування. Тобто, можливий варіант, коли кібероперації за участі конкретних держав будуть відсіюватися.

Але, незважаючи на відмову від постійної участі держав в діяльності Консорціуму, РЕНД не виключає можливість співпраці з державами. Таким чином, останні зможуть надавати інформацію, яка може допомогти в розслідуванні та встановленні винних, але на Консорціум не покладатиметься обов'язок щодо використання цієї інформації, особливо в ситуації, коли виникатимуть сумніви щодо достовірності переданої інформації.

Що ж до можливого впливу на організації-учасники, які попри свою незалежність від держав, створенні відповідно до національного законодавства та діють в межах території держави, наявність значної кількості технічних експертиз та процедур розслідування дозволить мінімізувати можливий вплив [97, с. 30].

Створення організації, яка не передбачає постійне членство держав, дійсно має своє плюси, але далеко не завжди приватний сектор володіє необхідними ресурсами для здійснення атрибуції. Історія знає приклади, коли приватним організаціям приходилось призупиняти процес атрибуції через потребу у даних урядової розвідки. Так, наприклад, компанія Novetta під час підготовки звіту щодо операції «Блокбастер» виразилась стосовно можливості підтримати роботу інших акторів, зазначивши відсутність ресурсів для самостійної атрибуції. Це пояснюється тим, що відомі хакерські групи, які підтримуються державами, як правило, не одразу впадають в поле зору приватних компаній. Крім того, нападники не є ізольованою та єдиною групою, а масштаб їх діяльності досить значний і може охоплювати значну кількість країн та сфер.

Важливим моментом, який не дозволяє просто так виключити державу з процесу атрибуції є політичний фактор. В своїх звітах приватний сектор визнає необхідність оцінки політичних індикаторів, і це зумовлено не лише можливістю фальсифікації технічних даних. Встановлення низки держав, які мають політичні, економічні чи інші мотиви у здійсненні кібератаки може пришвидшити процес атрибуції. Адже, як правило, ціль атаки та знання, які необхідні для її здійснення, свідчать про участь держав, а не випадкові атаки хакерів заради розваги [97, с. 12].

Наприклад, дизайнерам вірусу «Stuxnet» потрібне було не лише глибоке розуміння мережевої архітектури чутливого ядерного об'єкта, але розуміння досить складного процесу збагачення урану. Отже, мова йде не лише про збір розвідувальних даних, а також про залучення фахівців з глибоко спеціалізованими знаннями в конкретній галузі [66, с. 10]. У випадку зі Stuxnet мотиви США та Ізраїлю щодо іранської ядерної програми послужили додатковим політичним індикатором причетності цих країн. Аналогічно у випадку з кібератаками на систему електропостачання України у 2015 та 2016 роках мотиви, обрана ціль та використані знання стали додатковим підтвердженням причетності російських державних акторів.

Максимально показовою в цьому плані є ситуація зі звітом CrowdStrike щодо «Використання шкідливого програмного забезпечення групи «Fancy Bear» для платформи Android з ціллю відстеження української польової артилерії», опублікований 22 грудня 2016 року. Відповідно до звіту цієї компанії програма «Попр-Д30.apk» («поправки для гаубиці Д30»; на сторінці розробника програма згадується як «Укроп»), що використовувалася українськими артилеристами для здійснення артилерійського обстрілу, була інфікована та розповсюджена групою російських хакерів «Fancy Bear» ще в 2013 році.

Дана програма пов'язувала в єдину мережу смартфони та планшети, на яких здійснювалися артилерійські розрахунки відповідно до балістичних таблиць, враховуючи, серед іншого, такі параметри як погоду. Російські хакери, на думку «CrowdStrike», не тільки зламали цей мобільний додаток, а й активно

використовували. Код модуля X-Agent (бекдор вірус), що містився в додатку, дозволив артилеристам противника отримати геопозиційні дані смартфонів та планшетів. В звіті зазначається, що з 2013 по 2016 роки українська армія втратила приблизно 80% гаубиць Д-30. Не зрозумілим залишається, чому підрахунок втрат одиниць гаубиць починається з 2013 року, коли бойові дії ще не розпочались на сході України.

Після публікації даного звіту на них одразу відреагував програміст-розробник додатку, офіцер української армії Ярослав Шерстюк, який заперечив такий сценарій, зазначивши, що програма «Укроп», яка використовується українськими артилеристами, знаходиться під його повним контролем. В пості 22 грудня 2016 року він зазначив, що поширення такої неправдивої інформації є результатом діяльності «хакерів ФСБ РФ». Водночас закликав всіх артилеристів видалити всі попередні версії програми, такі як «РУ(батр), Попр, ТОПО» [33].

В ще одному пості за 22 грудня 2016 року Ярослав Шерстюк написав: «Щоб усім було зрозуміло, поширення ПЗ залишається під моїм контролем і не знаходиться у відкритих джерелах, так само активація ПЗ здійснюється особисто мною. Прочитавши статтю [*прим*. – автор додає в публікацію посилання на статтю Republic.ru щодо злому додатку для української армії], можете без сумніву продовжувати скачувати ОСОБИСТО У МЕНЕ ДОДАТОК «УКРОП» і далі захищати країну» [32].

Командування Сухопутних військ ЗС України також спростувало висновки зроблені «CrowdStrike» та поширені рядом ЗМІ. У своєму офіційному повідомлені Міністерство оборони України наголосили на наступному: «За інформацією Командування ракетних військ і артилерії Сухопутних військ Збройних Сил України, втрати озброєння артилерії за час проведення АТО в рази менші за згадані і не пов’язані із зазначеною причиною. На даний час військові частини ракетних військ і артилерії Сухопутних військ ЗС України цілком боєздатні, укомплектовані та спроможні виконувати завдання за призначенням […]. Поширення неправдивої інформації призводить до посилення соціальної напруги в суспільстві та підриває довіру населення до Збройних Сил України»

[14]. Цей випадок є підтвердженням того, наскільки важливою є протидія неправдивої інформації, що має негативний зовнішній інформаційно-психологічний вплив [2, с. 25].

Цікаво, що після значної критики з боку українських військових, компанія CrowdStrike публікує оновлену версію свого звіту, де зазначаються принципово інші дані про втрати артилерійських гаубиць. Якщо в грудні 2016 року втрати гаубиць становили 80% – найбільша частка серед всіх видів бойової техніки, то в оновленій версії звіту за 23 березня 2017 року зазначалося, що «Збройні Сили України втратили в бойових діях від 15% до 20% свого довоєнного запасу гаубиць Д-30» [248, с. 2].

Такі різка зміна цифр свідчить про невідповідальність осіб, які займалися підготовкою даного звіту. Примітно, що Міжнародний інститут стратегічних досліджень повідомив, що компанія CrowdStrike помилково використала дані Інституту для свого звіту. МІСД також зазначив, що ніяким чином не пов'язаний зі звітом CrowdStrike [155]. В дійсності дані для розрахунку втрат гаубиць були взяті з публікації сімферопольського блогера та відомого проросійського пропагандиста Colonel Cassad в Livejournal, якому «один з його читачів вислав порівняльний аналіз звітів Military Balance, виданий Міжнародним інститутом стратегічних досліджень». Порівнявши дані за 2013 та 2016 роки Colonel Cassad приходить до висновку про 80% втрат гаубиць Д-30. Міжнародна волонтерська спільнота InformNapalm в своїй замітці від 9 березня 2017 року вказує, що англомовна стаття Colonel Cassad зазначається в джерелах до звіту «CrowdStrike» [36], проте наразі оригінальна версія звіту за 22 грудня 2016 року замінена оновленою за 23 березня 2017 року і не містить даного посилання.

Цей приклад свідчить про недосконалість підходу приватних компаній до атрибуції кібероперацій в просторі. Попри те, що втручання в програмні забезпечення, що використовуються військовими теоретично є можливим, воно не може оцінюватися без участі держави, у віданні якої міститься найбільш достовірна інформація щодо втрат бойової техніки. Відтак, складно уявити, що

міжнародний механізм, який займатиметься атрибуцією кібератак діятиме ефективно без сприяння з боку державних агентів.

У 2016 році хакери також показали свою здатність втручатися у політику, і в цьому випадку приватний сектор також відіграв важливу роль в процесі атрибуції. Напередодні виборів 2016 року в США Демократичний національний комітет США отримав численні фішингові листи. За допомогою них хакери отримали доступ до близько 60 000 електронних листів в приватному акаунті gmail Джона Подести, який на той момент був головою кампанії Хілларі Клінтон. Існують думки, що ця кібератака представляє собою втручання у виборчий процес і нібито вплинула на результати виборів 2016 року.

У своєму звіті про розслідування, компанія з кібербезпеки CrowdStrike виявила дві ворожі хакерські групи у мережі – COZY BEAR та FANCY BEAR. Компанія також з'ясувала, що ці два суб'єкти пов'язані з Російською Федерацією. Обґрунтуванням такого висновку було «широке політичне та економічне шпигунство на користь уряду Російської Федерації», що, як наголошується, свідчить про те, що вони «тісно пов'язані з потужними та високо професійними спецслужбами російського уряду [ГРУ, Головне розвідувальне управління]» [46].

Співробітники CrowdStrike також прийшли до висновку, що, наприклад, FANCY BEAR застосовується з середини 2000-х років проти галузей аерокосмічного, оборонного, енергетичного, урядового та медіа-секторів. Вони встановили, що це зловмисне програмне забезпечення загалом було використано проти Сполучених Штатів, Західної Європи, Бразилії, Канади, Китаю, Грузії, Ірану, Японії, Малайзії та Південній Кореї, і що «така сильна спрямованість на міністерства оборони та інші військові цілі..., профіль, який чітко відображає стратегічні інтереси російського уряду» можуть свідчити про причетність Головного розвідувального управління РФ. Поряд із мотивацією (стратегічні інтереси держави) CrowdStrike покладався на імплантати (капельниці Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer та DownRage) та шкідливі програми, які використовуються для телефонів Linux, OSX, IOS, Android та Windows, а також

на техніку реєстрації доменів та створення фішинг-сайтів на цих доменах для викрадення облікових даних жертв [46].

У січні 2017 року Департамент національної безпеки та ФБР опублікували Спільний звіт про аналіз «GRIZZLY STEPPE – Злочинна кібердіяльність Росії», який також публічно приписував втручання у вибори США Російській Федерації: «Попередній аналіз не відносив зловмисну кібердіяльність до конкретних країн або суб'єктів. Однак публічне віднесення цих заходів до [російських цивільних і військових розвідувальних служб] підтверджується технічними показниками з боку Служби розвідки США, МВС ФБР, приватного сектору та інших організацій» [100].

Ці випадки публічної атрибуції чітко свідчать про нові тенденції, продиктовані збільшенням кількості кібератак на критичну інфраструктуру та ключові сектори. Атрибуція, зроблена державами-жертвами, не може розглядатися лише як політична атрибуція, оскільки вона передбачала технічне розслідування, проведене різними зацікавленими сторонами (державними та приватними). Таким чином, це підтверджує можливість з'ясувати, хто стоїть за певною кібератакою, особливо коли держави готові вдатися до певних юридичних дій.

В травні 2021 року Президент США прийняв Виконавче розпорядження щодо покращення національної кібербезпеки. Цей документ фактично виводить ідею державно-приватного партнерства на якісно новий рівень. Але його прийняття не було чимось запланованим, а реакцією на кібератаки проти об'єктів критичної інфраструктури, що мали місце в 2020-2021 роках.

13 грудня 2020 року стало відомо про те, що хакери зламали системи Міністерства фінансів та Національного управління з телекомунікацій та інформації. Дану кібератаку охрестили «Спалахом на сонці», оскільки в результаті постраждало чимало федеральних агентств США, інфраструктура та приватні компанії, а для того, щоб осягнути масштаби та наслідки цієї операції знадобляться роки.

Проникнення в систему, яке стало можливим завдяки злому SolarWinds, було тривалим та складним, і почалося не пізніше березня 2020 року [55]. А вже 7 травня 2020 року США засвідчили кібератаку на Colonial Pipeline, що поставляє бензин, дизельне паливо і авіагаз, та забезпечує потреби близько 45% східного узбережжя. В результаті атаки робота трубопроводів була зупинена та оголошено надзвичайний стан в США.

Розслідування, проведене в США, дозволило атрибутувати кібератаку SolarWinds Російській Федерації, встановивши, що кібератака була здійснена Головним розвідувальним управлінням Збройних сил РФ. Президент США також прийняв рішення про накладення санкцій на РФ [140]. Того ж дня, опубліковано заяву Австралії, відповідно до якої «Уряд Австралії приєднується до міжнародних партнерів, щоб підтримати заяву США від 15 квітня 2021 року про притягнення Росії до відповідальності за шкідливу кіберкампанію проти американської фірми з програмного забезпечення SolarWinds» [51]. Аналогічним чином вчинила Великобританія, підтвердивши, що за кібератакою SolarWinds, від якої постраждали 18 тисяч організацій по всьому світі, стоїть ГУ/ГРУ РФ, відоме в кіберпросторі як APT29 Cozy Bear The Dukes [203].

Саме ці дві кібератаки – проти SolarWinds та Colonial Pipeline – пришвидшили розвиток державно-приватного співробітництва. Виконавче розпорядження щодо покращення національної кібербезпеки від 21 травня 2021 року на державному рівні закріпило співробітництво між Урядом США та приватним сектором [115], адже така взаємодія є взаємовигідною для обох сторін, що неодноразово ставали жертвами кібератак. Крім того, Уряд визнає, що захист нації залежить від такої співпраці в протидії шкідливим кібератакам [115, сек. 1].

Так, наприклад, Національний інститут стандартів та технологій зобов’язаний протягом року від опублікування розпорядження консультуватися з приватним сектором щодо пілотних програм, що пов’язані із підвищенням безпеки ланцюжків поставок програмного забезпечення [115, 4(w)]. Секція 5 передбачає створення Ради з перевірки кібербезпеки, в яку входитимуть урядові

посадовці та представники приватних компаній, що займаються питаннями кібербезпеки або поставок програмного забезпечення. Важливо також те, що міністр внутрішніх справ кожні два роки призначатиме голову та заступника Ради з числа її членів: одного із числа федеральних посадовці, іншого – з представників приватного сектору [115, 5(f).].

При державно-приватній співпраці також важливо залучати міжнародні механізми, що діють в межах спеціальних режимів та мають досвід у здійсненні атрибуції. Наприклад, Міжнародний союз електрозв'язку може стати платформою для забезпечення такої співпраці. Наразі членами МСЕ є 193 держави, а також близько 900 компаній, університетів, універсальних і регіональних організацій [20]. Діяльність МСЕ спрямована на покращення готовності країн до кібероперацій, захисту та реагування на кібероперації шляхом проведення кібертренувань на регіональному, національному та глобальному рівнях [144]. Крім того, Міжнародний союз електрозв'язку надає рекомендації щодо збору доказів, які стосуються кіберінцидентів [197].

Не існує підстав вважати, що МСЕ виходить за рамки технічної атрибуції, але, незважаючи на це, союз є ідеальною платформою для здійснення атрибуції при залученні держав та приватного сектору. Крім того, за умови тісної співпраці з юристами-міжнародниками МСЕ може стати не тільки платформою для технічної атрибуції, але й для здійснення юридичної кваліфікації кібератак. Разом з тим, створення спеціального механізму, який би здійснював атрибуцію кібератак проти об'єктів критичної інфраструктури є більш реальним та бажаним: окрім технічної атрибуції, в кожному конкретному випадку потрібно здійснювати політичну та юридичну атрибуцію, кваліфікацію кібератак та вирішення питання віднесення об'єктів до критично важливих. Як видається, це серйозно розширить і обтяжить мандат МСЕ. Втім, залучення представників МСЕ до роботи спеціалізованого механізму підвищить ефективність останнього.

Таким чином, державно-приватна співпраця матиме позитивні результати для держави, яка, навіть попри значні технічні та людські ресурси, не може самостійно забезпечувати кіберстійкість своєї критичної інфраструктури, захист

інших державних установ та приватних компаній. Що ж до приватного сектору, то така співпраця дозволить йому отримувати перевагу від раннього попередження з боку держави та розвідки урядових партнерів держави, щоб ідентифікувати потенційну загрозу та посилити захист перед лицем кібератаки. У свою чергу, уряд держави та його партнери можуть скористатися підвищеною комунікацією з боку приватного сектору, коли напади відбудуться.

3.2. Забезпечення стійкості інфраструктури в ЄС: кіберсанкції та інші інструменти кібердипломатії Європейського Союзу

Проблема захисту об'єктів критичної інфраструктури з'явилась в повістці європейських інституцій ще на початку двадцять першого століття. Після терактів 2004 року в Мадриді та 2005 року в Лондоні, Європейська Комісія розпочала дискусію, присвячену питанням захисту критичної інфраструктури, від нормального функціонування яких залежить як життя людей, так і національна та міжнародна безпека [113; 215, с. 2-17].

Наразі можливості, які надає кіберпростір та інформаційно-комунікаційні технології, змінили спосіб функціонування урядів, бізнесу, вплинули на життя людей та міждержавні відносини в цілому. Порівняно недавнє «народження» кіберпростору змінило динаміку та характер глобальних загроз. Так, наприклад, зловмисна діяльність у вигляді кібератак, попри свій віртуальний характер, може призвести до серйозних кінетичних наслідків. Нові можливості кіберпростору та загрози, пов'язані з його використанням, також фактично встановили знак рівності між державними та недержавними кіберакторами, що змусило членів міжнародної спільноти змінити підхід до питання кібербезпеки, зокрема задля підвищення кіберстійкості критичної інфраструктури.

Зобов'язання та відповідальність держави і приватного сектору, а також конвергенція їх знань та навичок в питаннях кібербезпеки переконали політиків перейти від державоцентризму до ідеї партнерства між державами та приватним сектором з ціллю мінімізації наслідків, попередження кібероперацій і зміцнення міжнародної безпеки. З огляду на прогресивну позицію Європейського Союзу в

питаннях, пов’язаних з кібербезпекою, актуальним є дослідження напрямів діяльності ЄС та його спрямованість на забезпечення кіберстійкості критичної інфраструктури, що досить часто досягається за рахунок партнерства з приватним сектором та спільної атрибуції кібератак. Крім того, факт лідерства ЄС в питаннях кібербезпеки викликає потребу проаналізувати основі положення прийнятої наприкінці 2020 року Стратегії кібербезпеки ЄС.

В грудні 2020 року Європейський Союз представив нову Стратегію кібербезпеки, яка передбачає підвищення стійкості секторів критичної інфраструктури та протидії кібератакам ззовні [174]. Під час презентації стратегії високий представник ЄС із закордонних справ і політики безпеки Жозеп Боррель зазначив, що «у минулому році зафіксовано близько 450 інцидентів, направлених на об’єкти європейської критичної інфраструктури, включаючи фінансовий та енергетичний сектори. З пандемією загроза стає все більш помітною. Лише минулого тижня на Європейське агентство з лікарських засобів був здійснений напад» [94].

Нова Стратегія кібербезпеки охоплює п’ять напрямків зовнішньої політики Європейського Союзу, серед яких основне місце займає лідерство в сфері формування норм щодо відповідальної поведінки держав в кіберпросторі та зміцнення довіри. Наразі ЄС має найкращі можливості для просування, координації та закріплення позицій держав-членів ЄС на міжнародній арені, тому цілком обґрунтованим є намагання ЄС виробити позицію щодо застосування міжнародного права в кіберпросторі. Зокрема, в Стратегії робиться акцент на подальшому сприянні дотримання Статуту ООН, міжнародного права прав людини та юридично не обов’язкових норм, правил та принципів відповідальної поведінки держав в кіберпросторі, розроблених Групою урядових експертів у 2015 році [229].

Для цього ЄС спільно з рядом інших держав запропонували Організації Об’єднаних Націй «Програму дій щодо підвищення відповідальної поведінки держави у кіберпросторі» («Programme of Action to Advance Responsible State Behavior in Cyberspace») [231]. Пропозиція має на меті ліквідувати паралельні

обговорення в Групі урядових експертів ООН з питань підвищення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки, в якій беруть участь представники 25 держав, і Відкритій робочій групі з питань розвитку ІКТ в контексті міжнародної безпеки, в якій беруть участь всі зацікавлені держави.

Згідно з пропозицією Програма має стати єдиною, довгостроковою, всеохоплюючою та орієнтованою на прогрес платформою, тоді як реалізація та подальші заходи схвалюватимуться Генеральною Асамблеєю ООН. Відтак, взаємодія в рамках запропонованої Програми допоможе створити певні межі та політичні зобов'язання на підставі існуючих міжнародних рекомендацій, норм та принципів, які вже узгоджені та зокрема містяться у звіті Групи урядових експертів ООН за 2015 рік, прийнятому Резолюцією Генеральної Асамблеї ООН 70/237.

В контексті кібератак проти об'єктів критичної інфраструктури це означає підтримку закріплених в Резолюції Генеральної Асамблеї ООН 70/150 спеціальних норм та принципів, що не мають юридично обов'язкового характеру. Так, наприклад, згідно з пунктами 13 (h) та (g) держави повинні вживати відповідних заходів для захисту своєї критичної інфраструктури від загроз, створених в ході використання інформаційно-комунікаційних технологій, а також реагувати на запити про допомогу інших держав, критична інфраструктура яких стала об'єктом зловмисних дій при використанні ІКТ.

Тобто, мова йде про забезпечення кіберстійкості національної критичної інфраструктури та кіберстійкості критичної інфраструктури держав, що звертаються із запитом. Держави також повинні реагувати на відповідні прохання щодо пом'якшення зловмисної діяльності, спрямованої проти критичної інфраструктури іншої держави у випадку, коли джерело походження знаходиться в межах території держави, якій направлено запит (13 (h)) [195].

Будучи прихильником зазначених в Резолюціях ООН норм, Європейський Союз в своїй Стратегії кібербезпеки від 2020 року не випадково робить акцент на кіберстійкості «усіх відповідних секторів, державних та приватних, що

виконують важливу функцію в економіці та суспільстві» [229]. Для реалізації цієї цілі передбачається формування «європейського кіберщита», здатного виявляти та реагувати на потенційні загрози до того, як вони можуть завдати масштабної шкоди. В системі такого «щита» ключова роль належить центрам обміну інформацією та аналізу, командам реагування на випадки комп'ютерної небезпеки та операційним центрам безпеки. Останні функціонують не тільки на базі державних інституцій, а й створенні у ряді приватних компаній, некомерційних організаціях тощо.

Тобто, побудова «європейського кіберщита» сприятиме обміну інформацією між державними та приватними структурами, а також більш швидкому та ефективному виявленні кіберзагроз для їх подолання. Такий підхід є послідовним продовженням реалізації ідеї партнерства між приватним та публічним секторами заради підвищення кіберстійкості критичної інфраструктури, адже переважна більшість мережевих та інформаційних систем належить приватному сектору. Відтак, посилення взаємодії з ним є надзвичайно важливим напрямом діяльності. Якщо приватний та публічний сектори будуть розвивати технічні можливості щодо кіберстійкості, а потім обмінюватимуться передовим досвідом та інформацією, – кіберщит стане не тільки ефективним механізмом захисту від кіберзагроз в контексті міжнародної безпеки, а також інструментом взаємодії для встановлення відповідальних за кібератаки акторів.

В Програмі дій ЄС щодо підвищення відповідальної поведінки держави у кіберпросторі також передбачається необхідність активізувати співпрацю та розбудову потенціалу, а також організувати консультації з іншими зацікавленими сторонами, регіональними організаціями та установами ООН, приватними компаніями, неурядовими організаціями, громадянським суспільством, представниками інших інституцій ООН та відповідними багатосторонніми ініціативами, що займаються проблемами, пов'язаними з питаннями кібербезпеки у контексті міжнародної безпеки [231]. Європейський Союз планує налагодити структурований обмін з такими регіональними організаціями як Африканський союз, регіональний форум АСЕАН, Організація

американських держав та Організація безпеки та співробітництва в Європі [229]. Беручи участь у таких організаціях як ООН і НАТО та шляхом взаємодії з вище перерахованими регіональними організаціями, ЄС фактично прагне встановити універсальні «правила гри в кіберпросторі» та принципи відповідальної поведінки держави при його використанні, співпрацювати, обмінюватися досвідом та найкращими практиками, а також розробити відповідні засоби для вирішення загроз та викликів, пов'язаних з кібербезпекою.

Серед напрямів зовнішньої політики в Стратегії ЄС зазначається і такий напрям як «Співпраця ЄС у галузі кіберзахисту та ініціативи з розвитку можливостей», що передбачає використання потенціалу кіберпроектів в межах Постійного структурованого співробітництва (PESCO), зокрема «Кіберкоманд швидкого реагування та взаємодопомоги». Основне завдання таких кіберкоманд полягає у забезпеченні більш високого рівня кіберстійкості та колективного реагування на кіберінциденти. При цьому, кіберкоманди будуть оснащені розробленим інструментарієм для виявлення, розпізнавання та мітігації кіберзагроз.

В свою чергу, спільний кіберпідрозділ («Joint Cyber Unit») стане центром оперативного співробітництва ЄС з питань кібербезпеки. Цей підрозділ буде співпрацювати з державами-членами та відповідними установами, органами та агентствами ЄС, включаючи ENISA, CERT-EU та Європол, з метою просування поступового та всеохоплюючого підходу. Отже, підрозділ може сприяти подальшій співпраці між учасниками певної кіберспільноти, де учасники цього потребують.

Значного прогресу Європейський Союз також досяг в сфері реагування на кібератаки, яка є частиною зовнішньополітичного напряму «Інструментарій з кібердипломатії» («Cyber Diplomacy Toolbox»). Інструментарій включає реагування у формі політичних декларації, демаршів та діалогу, а також застосування вибіркових санкцій. Важливо, що Європейський Союз уже почав застосовувати санкції, і в новій Стратегії мова йде про можливість розширення інструментарію.

30 липня 2020 року Рада Європейського Союзу вперше ввела санкції проти фізичних та юридичних осіб, причетних до кібератак, що загрожують Європейському Союзу та походять з Союзу або інших держав, що не входять в його склад. Обмежувальні заходи зачепили шість індивідів та три юридичні особи, пов'язані з такими кібератаками як «WannaCry», «NotPetya», «Operation Cloud Hopper» та кібератаки проти Організації із заборони хімічної зброї. Введені санкції передбачають заборону на виїзд, замороження активів та заборону для осіб і структур ЄС надавати кошти тим, хто перерахований в рішенні [74, 12-17; 78, с. 4-9]. Ще дві фізичні та одна юридична особи були додані рішенням Ради ЄС в жовтні 2020 року [75, с. 5-7].

Найважливішим для України є наявність в списку Головного центру спеціальних технологій Головного Управління Збройних сил Російської Федерації (військова частина 74455, що знаходиться за адресою вул. Кірова, 22, м. Москва). Була встановлена відповідальність центру за кібератаки, що завдали значної шкоди та становили зовнішню загрозу для Європейського Союзу або його держав-членів, а також за кібератаки зі значним ефектом проти третіх держав, включаючи такі кібератаки як «NotPetya» або «EternalPetya» у червні 2017 року та кібератаки, спрямовані проти українських енергосистем взимку 2015 та 2016 років.

Враховуючи те, що їх ціллю були вразливості комп'ютера, кібератака «NotPetya» або «EternalPetya» зробила дані недоступними для ряду компаній в ЄС, Європі та в усьому світі. Блокування доступу до таких даних спричинило, серед іншого, значні економічні втрати. А кібератака на українську електромережу призвела до відключення її частин взимку.

Такий висновок та його офіційне опублікування є важливим кроком на шляху встановлення відповідальності держав за кібератаки. Водночас вибіркові обмежувальні заходи мають стримуючий і попереджувальний характер, тому, як зазначається в прес-релізі Ради ЄС, «їх слід відрізняти від атрибуції відповідальності третій державі» [112]. Залишається не зрозумілим, який ефект має таке «застереження», оскільки Головний центр спеціальних технологій

Головного Управління Збройних сил Російської Федерації є офіційним державним органом, уповноваженим на виконання урядових функцій в області оборони та розвідки.

Навіть, якщо допустити, що кібератака є актом *ultra vires*, вона в будь-якому випадку атрибутується державі. Але таке припущення є безпідставним, оскільки Головний центр спеціальних технологій ГУЗС РФ є виконавчим органом і органом управління Міністра оборони та Генерального штабу Збройних сил РФ. Навряд чи можна прийти до висновку стосовно необізнаності Міністра оборони та Генерального штабу Збройних сил РФ щодо запланованих Головним центром спеціальних технологій кібератак проти України, і їх здійснення без відома суб'єктів, яким центр підпорядковується.

Попри те, що Рада ЄС намагається відокремити відповідальність цілого державного органу від відповідальності держави, таке рішення може зіграти позитивну роль при вирішення спорів між Україною та Російською Федерацією, адже за загальним правом відповідальності – поведінка *de facto* та *de jure* державних органів, уповноважених на виконання урядових функцій, атрибутується останній.

Що ж стосується санкцій, то Верховний представник прагне розглянути пропозиції щодо розширення заходів реагування в межах набору інструментів кібердипломатії, включаючи можливість застосування додаткових обмежувальних заходів, шляхом прийняття рішення про їх застосування кваліфікованою більшістю держав-членів Європейського Союзу [229]. В будь-якому випадку, конкретний приклад демонструє можливості ЄС щодо встановлення відповідальних осіб за здійсненні кібератаки проти об'єктів критичної інфраструктури, а також перспективність інструментарію кібердипломатії.

З огляду на здійснений аналіз, видається, що Європейський Союз має намір всіляко заохочувати відповідальну поведінку в кіберпросторі, шляхом підвищення поваги до міжнародного права та не обов'язкових для виконання норм відповідальної поведінки в кіберпросторі.

Загалом діяльність Європейського Союзу в сфері виявлення та реагування на кіберзагрози демонструє принципово важливу позицію цього об'єднання до взаємодії з приватним сектор задля обміну інформацією та формування «європейського щита» кіберстійкості критичної інфраструктури. Такий підхід у разі його ефективної апробації можна було б застосувати на міжнародному рівні. Зокрема, привертає увагу ідея створення регіональних кіберщитів по аналогії з «європейським щитом». Функціонування таких щитів сприяло б посиленню безпеки як на регіональному, так і на міжнародному рівнях. Більш того, залучення різноманітних кібератакторів, співпраця з ООН, НАТО та регіональними організаціями, які зазначені в Стратегії, сприятимуть мітігації існуючих кіберзагроз, а також створенню універсальної системи виявлення та реагування на зловмисну діяльність в кіберпросторі.

Що ж до ефективності інструментарію кібердипломатії, то факт встановлення відповідальних осіб в межах Європейського Союзу є однозначно позитивним кроком, який підкреслює неможливість безкарності за кібератаки на об'єкти критичної інфраструктури держав, що є джерелом основних послуг, а значить – забезпечення прав та свобод людини і нормального функціонування держав.[5] У зв'язку з цим позитивним кроком може стати перейняття даного досвіду. Так, наприклад, кіберсанкції можна було б застосовувати на рівні Організації Об'єднаних Націй, але з ціллю посилення їх ефективності пропунується застосовувати як вибіркові санкції проти індивідів, так і секторальні санкції, особливо коли деструктивний потенціал кібератак був досить значним.

[5] Наукові результати, представлені в підрозділі 3.2, попередньо оприлюднено в наступній публікації : Політика ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки. Evropský politický a právní diskurz. 2021. Том 8 (1). С. 46-51.

3.3. Вироблення підходу до атрибуції кібератак за результатами розгляду міждержавного спору

Кібератаки, ціллю яких була критична інфраструктура, свідчать, *inter alia*, про два важливі моменти. По-перше, вірогідність успішних кібератак проти об'єктів критичної інфраструктури з деструктивними наслідками з кожним разом зростає. Д. Вагнер та Б. Швайцер, на нашу думку, обрали досить вдале порівняння роботи експертів з кібербезпеки та хакерів, назвавши її грою в «кішки-мишки» [249], адже важко запобігти кібератаці, враховуючи те, з якою легкістю можна знайти невідому вразливість віртуальних систем. Успішна кібератака – це питання часу, а не потенційної можливості. По-друге, ефект стримування можливо досягнути тоді, коли держави будуть обізнані у невідворотності відповідальності. Тому вважаємо за доцільне проаналізувати перспективи розгляду міжнародно-правового спору на підставі результатів наявних доказів.

Для цього був обраний Міжнародний суд ООН, який розглядає міждержавні спори. Такий вибір обґрунтований природою цього органу та наявністю значної кількості договірних та не договірних інструментів, які можуть «запустити» його юрисдикцію. Юрисдикція представляє, мабуть, найперше і найосновніше питання, але не менш важливим є процес доказування, на якому ми хочемо сконцентрувати основну увагу.

У справі Нікарагуа, серед іншого, міститься важливе твердження Міжнародного Суду ООН про те, що «проблемою є... не... правовий процес присвоєння («imputing») діяння певній державі... а попередній процес пошуку матеріального підтвердження ідентифікації винної поведінки» [62, п. 57]. В кіберпросторі ця проблема стає ще більш яскравою, адже держави та їх проксі для здійснення кібератаки можуть використовувати ніки, проксі-сервери, різні комп'ютери тощо. У все тій же справі Нікарагуа Суд також підкреслив необхідність встановити, що саме сталось перед тим як перейти до наступної стадії атрибуції поведінки державі, якщо наявні конфліктуючі між собою докази

[62, п. 57]. Адже спочатку будь-якій судовій інституції потрібно розібратися з тим, що саме сталося та які факти потрібно враховувати, і лише потім вирішувати питання відповідальності держав.

Як зазначив професор Вестмінстерського Університету М. Россіні, для атрибуції потрібно спочатку встановити комп'ютери та сервери, які застосовувалися задля здійснення кібератак, ідентифікувати осіб, які мають безпосередній стосунок до цих атак, а потім – довести, що ці особи діяли від імені конкретної держави, щоб атрибутувати їх дії державі [200, с. 240; 210, с. 98-103].

Крім того, важливим є стандарт доказування, яким буде керуватись Міжнародний суд ООН. Єдиний стандарт відсутній як в Статуті Суду, так і в його Регламенті. Що ж до практики, то вона свідчить про індивідуальний підхід Суду, який в значній мірі залежить від характеру справи. При цьому, Суд сповідує свою традиційну культуру обережності з ціллю уникнення згадок стандарту, яка зазнала неодноразової критики, навіть з боку окремих суддів. Зокрема, в своїй думці у справі щодо нафтових платформ між Іраном та Сполученими Штатами суддя А. Хіггінс висловила наступну думку: «Розглядаючи параграф 1 (d) статті XX, Суд стверджує, що Сполучені Штати несуть «тягар доказування існування збройної атаки», щоб виправдати застосуванням сили для самозахисту. […] у справі, в якій так багато обертається навколо доказів, логічно було очікувати, що Суд чітко визначить стандарт для доказів, необхідний для того, щоб сторона досягла тягар доказування» [178]. Ця справа не є унікальною в цьому плані. У справі щодо Нікарагуа Суд також не оминув стандарт, вказавши, що докази були «недостатніми» («insufficient») для встановлення ключових фактів [62, п. 54].

Підхід Суду очевидно змінився після такої критики, і зараз майже в кожному рішенні можна знайти посилання на стандарт доказування, яким керувався Суд, і який був покладений на сторін. Водночас є всі підстави стверджувати, що про цей стандарт сторони дізнаються лише тоді, коли отримують рішення.

Аналізуючи практику Міжнародного Суду ООН, можна виділити декілька стандартів, які він застосовує. По-перше, коли мова йшла про звичайні порушення міжнародно-правових зобов'язань, Суд часто наполягає на представленні «переконливих доказів» («convincing evidence») [62, п. 24-25; 49, п. 83; 65, п. 119] або «вирішальних доказів» («conclusive evidence») [71, с. 17; 49, п. 303], а іноді більш легкого стандарту «балансу вірогідностей» («balance of probabilities») [63, п. 248] або «балансу доказів» («balance of evidence») [178, п. 57]. Тобто навіть у випадку звичайних порушень, Суд зберігає свою гнучкість та автономність, оскільки згадані стандарти фактично містить декілька більш жорстких та м'яких підходів, що очевидно з урахуванням граматичної інтерпретації висловлювань Суду.

По-друге, коли мова йде про обтяжену відповідальність, тобто порушення імперативних норм *jus cogens*, правовим інтересом щодо виконання яких наділена вся міжнародна спільнота (*erga omnes*), поріг стандарту доказування значно вищий. Зокрема, у справі про Боснійський геноцид Міжнародний Суд ООН наголосив на тому, що «позови проти держав, які передбачають звинувачення виняткової важкості, повинні бути доведені доказами, які є повністю переконливими» («fully conclusive») [48, п. 209].

У випадку з кібератаками проти об'єктів критичної інфраструктури, вважаємо, що вирішальну роль при виборі стандарту доказування будуть відігравати наслідки та масштаб такої кібератаки. Адже саме наслідки атаки є тим фактором, який розмежовує «найбільш серйозні форми застосування сили» від «менш серйозних» [62, п. 191], тобто збройну агресію, яка наділяє державу правом на самозахист відповідно до Статуту ООН, від інших, менш значних проявів погрози або використання сили.

Згідно з Енциклопедією міжнародного публічного права Макса Планка, «Кібервійна охоплює військову діяльність, яка в першу чергу використовує комп'ютерні системи та мережі з метою нападу на противника» [251, п. 2]. Зазвичай кібервійна порівнюється з атаками на комп'ютерні мережі («CNA»). Такі атаки можуть бути визначені як «дії, що здійснюються за допомогою

використання комп'ютерних мереж для зриву, відмови в доступі, погіршення чи знищення інформації, яка знаходиться в комп'ютерах та комп'ютерних мережах, або самих комп'ютерах та мережах» [147]. В даному випадку мова йде про кібератаку, що досягла рівня збройної атаки. При цьому, кібератака не повинна обов'язково супроводжуватись кінетичним використанням сили, щоб кваліфікуватись як збройна атака. Водночас важливо розуміти, що не кожне використання сили у формі кібератаки буде розглядатись в якості збройної атаки. Кваліфікація в якості збройної атаки залежатиме від низки факторів, таких як серйозність нанесеної шкоди та масштаб атаки [210, с. 53; 62, п. 195].

Так, наприклад, по аналогії з озброєнням та підготовкою повстанців у справі Нікарагуа [62, п. 228], дії держави щодо забезпечення організованої групи вірусом та навчання тому, як його застосувати в ході кібератаки проти іншої держави – представляють собою використання сили [210, с. 48]. Крім того, такі дії потенційно можуть досягти рівня збройної атаки, навіть якщо здійсненні недержавними акторами, та, як наслідок, наділяти постраждалу державу правом на самозахист відповідно до статті 51 Статуту ООН. Про це свідчить підхід держав після атаки 9 вересня 2001 року з боку Аль-Каїди, який призвів до прийняття Резолюцій 1368 та 1373, що визнали право США на самозахист відповідно до Статуту ООН. Цілком можливо, що причиною цьому послужила відсутність в статті 51 обмежень, хоча стаття 2(4) та норми звичаєвого міжнародного права свідчать на користь того, що право на самозахист існує лише в площині держава *vis-à-vis* держава.

Залежно від характеру кібератаки, а точніше від її наслідків, буде визначатися стандарт доказування. Якщо спір буде розглядатися в Міжнародному Суді ООН, на кожну із сторін буде покладатися тягар доказування тих фактів, на яких ця сторона наполягає [193, п. 162]. Крім того, не виключено, що сторін буде більше, ніж одна. Так, наприклад, у випадку, коли постраждала держава представить докази щодо того, що кібератака була здійсненна із територій Держави А та Держави Б (що потенційно можливо), до цих держав перейде тягар доказування, що вони: а) не причетні до кібератаки,

б) попередили можливість використання власної інфраструктури для здійснення кібератаки.

У випадку використання інфраструктури держави, особливо коли про це було відомо відповідній державі, також виникає відповідальність держави. Разом з тим, це не говорить про атрибуцію державі кібератаки, а швидше про порушення обов'язку проявляти належну обачність (*due diligence*). По аналогії з рішенням у справі щодо «Військових дії на території Конго» [49, п. 301], не можна зробити висновок про те, що відсутність реакції з боку держави, інфраструктура якої була використана, прирівнюється до толерування таких дій чи до погодження з ними. Але, як говорилось на початку даного підрозділу, тягар доказування буде лежати на тій державі, яка висуває обвинувачення. Такий висновок, втім, не виключає вірогідність зворотного тягаря доказування, тобто можливість перекласти тягар з позивача на відповідача. В такому випадку відповідач повинен буде почати з представлення фактів, які підтверджують його непричетність до здійсненої кібератаки або необхідну обачність стосовно використання національної інфраструктури.

Окрім визначення стандарту доказування та того, на кому лежить тягар доказування, для Суду виникає ще одне складне завдання – встановити чи мав місце конкретний факт і хто його здійснив. Враховуючи відсутність міжнародного незалежного та об'єктивного механізму, який би здійснював атрибуцію, одразу виникає питання щодо того, які докази враховуватиме Суд в ході розгляду справи.

Статті 48-52 Статуту Міжнародного Суду ООН присвяченні доказам. Суд, зокрема, «вживає всіх заходів, які стосуються збирання доказів» [245, ст. 48], «може, навіть до початку слухання справи, вимагати від представників пред'явлення будь-якого документа або пояснень» [245, ст. 49], «в будь-який момент доручити здійснення розслідування або експертизи будь-якій особі, колегії, бюро, комісії або іншій організації на власний розсуд» [245, ст. 50], вислуховувати свідків та експертів [245, ст. 51].

Крім того, «[п]ісля отримання доказів у встановлені для цього терміни, Суд може відмовити в прийнятті всіх подальших усних і письмових доказів, які одна зі сторін побажала б пред'явити без згоди іншої» [245, ст. 52]. При цьому, положення Статуту не містять обмежень щодо виду доказів, які сторони можуть надавати на розгляд Суду. Єдиним обмеженням є заборона подавати докази після закінчення встановленого строку.

Важливо також те, що Суд може зайняти активну позицію щодо збирання доказів, що, звичайно, не звільняє сторони від надання доказів на підтримку власної позиції, але фактично сприяє встановленню істини у справі.

Для того, щоб розібратись в тому, які докази Суд вірогідно буде застосовувати при здійсненні атрибуції для цілей міжнародної відповідальності, спробуємо розглянути ті, які, на нашу думку, уже відіграють ключову роль в практиці Суду, а саме – документальні докази.

В практиці Суду та, відповідно, в Статуті Міжнародного Суду, відсутнє поняття документальних доказів, а також їх перелік. Разом з тим, інколи Суд дає перелік тих документів, які йому надали сторони для оцінки та прийняття рішення у справі. Так, наприклад, у справі про Боснійський геноцид, Суду було надано «доповіді, резолюції та висновки різних органів Організації Об'єднаних Націй, включаючи Генерального секретаря, Генеральної Асамблеї, Ради Безпеки та її Комісії експертів, Комісії з прав людини, Підкомісії з питань запобігання дискримінації та захисту меншин, та Спеціального доповідача з прав людини в колишній Югославії; документи інших міжурядових організацій, таких як Конференція з безпеки та співробітництва в Європі; документи, докази та рішення МТКЮ; публікації урядів; документи неурядових організацій; ЗМІ, статті та книги» [48, п. 211].

Аналогічно при вирішенні спору між Демократичною Республікою Конго та Угандою Суд отримав від двох сторін наступні документи:

«Обидві Сторони представили Суду велику кількість документації. Документи, що підкріплюють підтвердження фактів у цій справі, включають, зокрема, резолюції Ради Безпеки ООН, доповіді Спеціального доповідача Комісії

з прав людини, доповіді та інструктажі ОАЕ, комюніке глав держав, листи сторін до Ради Безпеки, доповіді Генерального секретаря з питань МООНУС (MONUC), доповіді експертних комісій ООН з питань незаконної експлуатації природних ресурсів та інших багатств Демократичної Республіки Конго (далі «Групові звіти ООН»), Білу книгу, підготовлену конголезьким Міністерством з прав людини, Звіт Комісії Портера, Білу книгу Уганди щодо Звіту Комісії Портера, книги, звіти неурядових організацій та звіти ЗМІ» [49, п. 60].

Вірогідно завдяки відкритості Суду та його готовності прийняти перелік тих доказів, на яких сторони вибудовують свою позицію по справі, стало за можливе розробити класифікацію документальних доказів. Зокрема, професор міжнародного права Університету Бар-Ілан Ш. Розенн, виділяє чотири групи документальних доказів:

1. опубліковані договори, що входять до однієї з визнаних міжнародних або національних збірок текстів договорів;
2. офіційна документація (записи засідань) міжнародних організацій та національних парламентів;
3. опубліковане та неопубліковане дипломатичне листування, комюніке та інші матеріали, включаючи книги, карти, плани, схеми, рахунки, архівні матеріали, фотографії, фільми, юридичні думки та думки експертів тощо;
4. афідативи та декларації (заяви) [201, с. 1246].

Відповідно до прецедентного права, Суд «визначає документи, на які посилаються, та робить власну чітку оцінку їх ваги, надійності та цінності» [49, п. 58-59; 243].

Що стосується ваги, надійності та цінності вторинних доказів, Суд на практиці керується наступними принципами. Так, наприклад, Суд поводиться досить обережно з доказами, які були спеціально підготовлені для представлення фактів справи, коли такі докази надходять із одного джерела [62, п. 41]. Як наголошував Суд у справі про нафтові платформи, «[ч]исленні звіти щодо факту при більш детальному дослідженні можуть виявитися такими, що отриманні із

одного джерела, і такі звіти, наскільки б вони не були численними, у такому випадку не матимуть більшої ваги, ніж першоджерела» [178, п. 60].

У справі про боснійський геноцид, Суд також зробив важливі практичні висновки щодо цінності та значимості звітів офіційних чи незалежних органів, які надають інформацію про відповідні факти. Зокрема, Суд встановив, що цінність документів залежить від трьох змінних факторів. По-перше, Суд вивчає джерело доказів на предмет його упередженості [48, п. 223]. Наприклад, у справі про Військову діяльність Суд часто розглядав доповіді преси та радіо як такі, що є ненадійними [49, п. 152]. По-друге, Суд завжди звертає увагу на процес зібрання доказів. Наприклад, Суд, як правило, надає більшої ваги доповідям, що є продуктом ретельного (подібного до судового) процесу збору та аналізу доказів – як ось рішення МТКЮ або Комісії Портера – в порівняні з анонімними звітами. Нарешті, Суд оцінює якість та характер доказів. З цього приводу Суд вважає особливо цінними та неоспорюваними факти та заяви сторін, які суперечать власним інтересам держав [48, п. 227]. Після цього Суд оцінює всі ці три елементи разом, щоб визначити значимість конкретного документа в ході доведення певних фактів [48, п. 230].

У випадку з кібератаками кількість офіційних документів міжнародних організацій щодо даного феномену постійно зростає і, звичайно, з високою вірогідністю Суд буде використовувати їх в якості документальних доказів. Вони включають в себе як резолюції Генеральної Асамблеї, так і документи Групи урядових експертів, Відкритої робочої групи, що створені для вивчення загроз в кіберпросторі та обговорення спільних заходів для подолання таких загроз. А враховуючи активність Європейського Союзу, який з 30 липня 2020 року продемонстрував свою готовність здійснювати атрибуцію кібератак для застосування вибіркових кіберсанкцій, досить імовірним є те, що Суд за необхідності опиратиметься на рішення Ради ЄС, а також інші документальні підтвердження, що є релевантними в конкретній справі.

Офіційні документи держави, такі як національне законодавство, кібердоктрина, посібники, стратегії, директиви та правила взаємодії, також

можуть відігравати важливу роль при встановленні відповідальності держави за кібератаки. У справі щодо Нікарагуа, наприклад, відповідальність США за заохочення порушень міжнародного гуманітарного права встановлена на основі публікації посібника з психологічних операцій [62, п. 113]. На думку Суду, «публікацію та розповсюдження посібника, що фактично містить рекомендації, наведені вище... слід розглядати як заохочення, яке, ймовірно, було ефективним, вчиняти дії, що суперечать загальним принципам міжнародного гуманітарного права, відображеним у договорах» [62, п. 256]. Разом з тим, не всі національні документи мають однакову доказову вагу. У рішенні щодо спору між Демократичною Республікою Конго та Угандою Суд відхилив значимість деяких документів внутрішньої військової розвідки, оскільки вони були не підписані, не засвідчені (їх автентичність не була підтверджена) або відсутні пояснення того, як була отримана інформація, що в них містилася [49, п. 125, 127-128, 133-134, 137]. У випадку з кібератаками такий підхід теж може застосовуватися, адже відсутність необхідних підписів на документах, що містять дані розвідки, віз та печаток часто може свідчити про те, що такі документи неякісно сфальсифіковані.

Важливо також розуміти, що у випадку з розглядом справи щодо певної кібератаки, деякі документи можуть бути засекречені державою. І тут досить цікавою є практика Суду, яка повністю протилежна висновкам міжнародних кримінальних трибуналів. Якщо останні інтерпретують відмову держави щодо надання документів, які є засекреченими, не на користь звинуваченого, то Міжнародний Суд ООН утримується від висновків відносно такої відмови.

Так, наприклад, у справі про боснійський геноцид, Суд відмовив Боснії та Герцеговині у задоволенні запиту щодо представлення Сербією та Чорногорією певних документів, віднесених до військової таємниці. Однак, Суд залишив за собою право запросити ці документи в майбутньому з власної ініціативи [48, п. 44]. При цьому, як нам видається, Суд не розглядав відмову згаданих держав надати документи в добровільному порядку [48, п. 206] як значимий для розгляду справи факт. Суд фактично обмежився альтернативними доказами, наявними у

справі. Знову ж таки, в кіберконтексті використання даних розвідки є досить популярним, і держави навряд чи проявлятимуть інтерес до афішування зібраної інформації. Найімовірніше, така інформація буде засекречена, а з нею і рішення, які приймались на підставі таких даних.

Не останню роль відіграватимуть звіти неурядових організацій та незалежних ІТ-компаній чи компаній, що займаються питаннями кібератаки. Що стосується перших, то Суд досить недовірливо відноситься до документів, підготовлених міжнародними неурядовими групами. Так, наприклад, у справі щодо військової діяльності на території Конго Суд висловився про звіт Міжнародної кризової групи як про «недостовірний доказ» [49, п. 129]. Часто такий підхід критикується з боку науковців, оскільки Суд не хоче застосовувати критерії, напрацьовані раніше, до звітів неурядових організації. І видається, що стосовно документів таких організацій існує більше вимог для того, щоб їх можна було вважати доказом у справі. Але у випадку з кібератаками та їх атрибуцією (політичною та технічною), яку здійснюють неурядові організації та приватні компанії, цілком можливо, що Суд змушений буде змінити свою позицію. Так, наприклад, звіти, підготовані Об'єднаним центром передових технологій з кібероборони НАТО, щодо Естонії, Грузії, Ірану та інших кіберінцидентів містять технічну атрибуцію та юридичний аналіз. Аналогічним чином звіти приватних кіберкомпаній, як видно з попереднього розділу, надають деталі щодо того хто і як здійснив кібератаку. Очевидно, що Суду необхідно використовувати доповіді приватних організацій та залучати їхніх експертів до встановлення фактів справи, тому що, навряд чи, держава погодиться добровільно надати класифіковані документи чи правдиві відомості стосовно власних кіберслужб.

Позитивним є те, що кількість таких звітів, підготовлених приватними компаніями з кожною кібератакою лише зростає. Ми згадували звіти від Mandiant, CrowdStike, Kaspersky та ін., що фактично підтверджують цю тенденцію, але на увагу також заслуговує проєкт «Grey Goose», заснована у 2008 році для здійснення розвідки на основі відкрити джерел (Open source intelligence,

OSINT). З 2009 року ця ініціатива переросла в формальну бізнес компанію «GreyLogic», що консультує уряди та є провайдером інформації для них. Їх звіти містять детальний аналіз атак на об’єкти критичної інфраструктури та ідентифікацію акторів, які до них причетні [190]. Звіти містять принципи аналізу інформації, а також до їх підготовки залучаються «ветерани» кібербезпеки, які і здійснюють розслідування. Серед них, Джефрі Карр, що є засновником проекту «Grey Goose» та «GreyLogic».

Що стосується повідомлень та публікацій засобів масової інформації, то потенційно вони можуть використовуватись в якості доказів, але їх роль буде досить обмеженою. Якщо такі статті чи повідомлення ґрунтуються лише на одному джерелі, яке має певний інтерес та не є цілком об’єктивним, або взагалі не містить посилань, його цінність буде рівнозначна нулю [49; п. 68]. У справі щодо Боснійського геноциду Суд вказав, що стаття у французькій щоденній газеті «Le Monde» є другорядним джерелом інформації [48, п. 357]. А у справі Нікарагуа висловив свою позицію щодо повідомлень у статтях преси та витягів із книг: «Суд зі значною обачністю ставився до них; навіть якщо вони, як видається, відповідають високим стандартам об’єктивності, Суд розглядає їх не як докази, здатні доводити факти, а як матеріал, який, проте, може за певних обставин сприяти підтвердженню існування факту, тобто, як додатковий ілюстративний матеріал до інших джерел доказів» [62, п. 62].

Разом з тим, інформаційні повідомлення можуть слугувати в якості підтвердження публічного знання про певний факт [62, п. 63]. Так, наприклад, було в справі про Дипломатичний та консульський персонал США в Тегерані, де наявність фактів, на які посилався Суд, «здебільшого відносяться до загальнодоступних знань, які отримали широке висвітлення у світовій пресі та в радіо- та телевізійних передачах з Ірану та інших країн» [246, п. 12].

Важлива роль в процесі доказування належить офіційним заявам. На думку Суду, заяви, що надходять від високопоставлених офіційних політичних діячів (іноді найвищого рангу) «мають особливу доказову цінність, коли вони визнають факти або поведінку, несприятливу для держави, яку представляє особа, яка їх

вчинила» [62, п. 64]. Такі заяви представників Іранської влади та США щодо фактів та обставин справи, зокрема, були враховані у вищезгаданій справі [246; п. 123].

При цьому, не всі заяви мають однакове значення. Важливим буде те, де вони висловлені чи опубліковані – в національних чи міжнародних публікаціях, книзі чи новинах, а також від того, чи заява опублікована на мові оригіналу, чи є перекладом [62, п. 64]. Тобто, не має виникати сумнівів щодо двох фактів. По-перше, можливість атрибутувати заяву безпосередньо державі. По-друге, впевненість в тому, що дійсно мало місце визнання конкретного факту і виключена вірогідність помилки в інтерпретації заяви, якщо остання була перекладена.

Наразі жодна із держав не визнала підтримку чи фінансування діяльності приватних кібератакорів чи безпосередню причетність держави до кібероперацій. У випадку з атаками на Грузію та Естонію були лише заяви щодо непричетності Російської Федерації. Цікавою є позиція США та Ізраїлю, оскільки вони не виразили заперечення щодо присвоєння їм кібератаки проти ядерної установки Ірану. Але поки що не зрозуміло, чи можуть якісь висновки робитись із факту відсутності заперечень.

Суд також може заслухати свідків з власної ініціативи або з ініціативи сторін спору. Доказова цінність таких свідчить буде залежати від ряду факторів, зокрема, наявності інтересу у особи, що надає свідчення, а також від того, посилається особа на певний факт чи представляє думку щодо факту, який мав місце. Значення такого доказу зменшується, якщо свідок розповідає про певний факт зі слів інших осіб. Загалом Суд досить бережно відноситься до таких доказів [227, п. 244]. Свідки заслухувались у справі про протоку Корфу [71, с. 7-8, 10], військову та напіввійськову діяльність в Нікарагуа [62, п. 13] тощо.

Цікаво, що мала місце 14-річна прогалина між справою щодо спору між Сальвадором та Нікарагуа [63], де останній раз були заслухані свідки, та спором між Боснією та Герцеговиною проти Сербії та Чорногорії [48], де вперше за 14 років виникла необхідність у свідках. І хоча були побоювання стосовно сотні

свідків та того, чи Суд справиться з перехресним допитом та забезпеченням перекладу, лише відповідач мав шість свідків та одного свідка-експерта. Категорія «свідок-експерт» фактично не згадується в Статуті чи Регламенті Суду, але була визнана у справі про канал Корфу і згодом застосовувалася у справах про Храм Преавіах та у справах щодо Південно-Західної Африки. Загалом цей термін позначає особу, яка може давати свідчення як щодо знання певних фактів, так і надавати експертний висновок (думку).

Як зазначалося вище, відповідно до статті 50 «Суд може в будь-який час доручити розслідування або проведення експертизи будь-якій особі, колегії, бюро, комісії або іншій організації за своїм вибором» [245, ст. 50]. Наразі Суд жодного разу не вдавався до можливості доручити комусь проведення розслідування, але активно використовував звіти, що мали на меті встановлення певних фактів. За це Суд неодноразово піддавався критиці та зазнавав закидів щодо необхідності реформувати практику встановлення фактів, які мають принципове значення для прийняття рішення.

Що стосується залучення експертів, то таку практику ми можемо спостерігати у випадку технічної природи спору, коли у суддів відсутня необхідна експертиза та, відповідно, комплексне розуміння. Так, наприклад, експертна думка була необхідна у спорі Ботсвани проти Намібії щодо впливу річкових меандрів на виявлення головного русла. Вивчивши докази щодо глибини, ширини, потоку, видимості, конфігурації профіля русла та судноплавства, Суд дійшов висновку, що північний канал річки Чобе навколо острова Касікілі/Седуду повинен розглядатися як її основний канал.

У справі стосовно Менської затоки Канада та Сполучені Штати просили Палату в їхній Спеціальній угоді призначити технічного експерта, спільно обраного сторонами, для надання допомоги Суду, зокрема, підготовки опису морської межі та мап (графіка), на яких був би вказаний курс затоки. Суд належним чином призначив експерта, і його технічний звіт було додано до рішення у справі.

Також важливо, щоб експерти та свідки не були включені в команду представників однієї із сторін. Як підкреслив Суд, «особи, які подають до Суду докази, ґрунтуючись на своїх наукових або технічних знаннях та на особистому досвіді, повинні свідчити перед Судом в ролі експертів, свідків або в деяких випадках в обох ролях, а не як адвокати, щоб вони могли предстати на допит перед іншою стороною та Судом» [193, п. 167]. Як наслідок, у справі про китобійний промисел в Антарктиці експерти, яких викликала Австралія та Японія, давали свідчення як свідки-експерти і були допитані на перехресному допиті [250, п. 20-21]. Можна прослідкувати, що, виносячи рішення, Суд досить ґрунтовно опирався на їхні заяви та зробив висновок, що спеціальні дозволи, видані Японією на вбивство і вивезення китів не були для цілей наукових досліджень.

Нарешті, цифрові докази також можуть бути використані Судом, але вірогідність того, що вони сприятимуть юридичній атрибуції досить низька. Загалом цифрові чи електронні докази представляють собою будь-який доказовий матеріал, що зберігається або передається в цифровій формі (у вигляді ряду цифр 0 і 1), що може бути використаний у судовому розгляді з метою доведення певного факту [130, с. 165].

Їх джерелом можуть бути жорсткі диски стаціонарних комп’ютерів, мобільні телефони, флеш-накопичувачі USB, супутники та Інтернет. Вони також можуть мати різні форми, наприклад, представляти собою текстові документи (файли Word, електронні листи, таблиці тощо), карти, бази даних, цифрові зображення, відео та аудіофайли, дані GPS, історії та метадані Інтернет-браузера. Загалом, як зазначає професор М. Розсіні, такі докази не регулюються положеннями Статуту чи Регламентом Суду, але вони не завжди створюють складнощі в оцінці. Крім того, вони можуть сприяти здійсненню атрибуції, а отже – встановленню відповідальності держави за кібератаку [199, с. 542, 554].

Загалом розгляд міждержавного спору щодо застосування кібератак, зокрема проти об’єктів критичної інфраструктури, має значні перспективи. Як було встановлено в Розділі 1, міжнародне право в повному обсязі (хоч і з деякими

відмінностями в силу природи кіберпростору) застосовується до кіберпростору та кібератак. Водночас Міжнародний Суд ООН приймає різноманітні докази для здійснення атрибуції міжнародно-протиправного діяння та встановлення релевантних фактів. Можна очікувати певні складнощі, що виникнуть при отриманні та оцінці цифрових доказів, але саме тут Суд зможе проявити свою дискрецію та сформувати вимоги щодо належності та достовірності таких доказів.

В ході розгляду міждержавного спору Міжнародному Суду прийдеться вирішити ряд принципово важливих в кіберконтексті питань. По-перше, щодо атрибуції кібератак проти об'єктів критичної інфраструктури. Спочатку необхідно буде встановити, чи об'єкт проти якого здійснено кібератаку, може розглядатися в якості об'єкта критичної інфраструктури. Для цього будуть використані доповіді Групи урядових експертів та Відкритої робочої групи, що займаються встановленням необов'язкових норм та принципів щодо відповідальної поведінки в кіберпросторі. Попри відсутність юридичного характеру, їх доповіді містять певні вказівки щодо того, як держави повинні діяти в кіберпросторі та згадки про об'єкти критичної інфраструктури. При наявності міжнародного спору важливо буде встановити, чи категоризовано об'єкт, що постраждав в ході кібератаки, як критично важливий. Але якщо національне законодавство не регулює питання віднесення об'єктів до критично важливих, Суд вірогідно керуватиметься загальною логікою та підходом, виробленим та представленим в доповідях Групи урядових експертів та Відкритої робочої групи.

По-друге, Міжнародному Суду ООН, швидше за все, прийдеться визнати неможливість здійснення атрибуції без попередньої технічної та політичної атрибуції. Як раніше зазначалося, врахування технічних індикаторів не компенсує і не виключає використання політичних індикаторів. І навпаки, не можна опиратися виключно на політичні індикатори: якщо технічні індикатори можуть бути сфальсифіковані, то політичні не завжди дають чітку і коректну відповідь щодо держави, яка стоїть за кібероперацією.

По-третє, розгляд спору щодо атрибуції кібератак проти об’єктів критичної інфраструктури дозволить конкретизувати те, як звичаєві норми щодо атрибуції міжнародно-протиправних діянь застосовуються до кібератак. Залежно від справи, в Суду буде можливість виробити тест, альтернативний тесту «ефективного контролю», що передбачає непосильний поріг для встановлення контролю держави по відношенню до проксі, які є приватними хакерами-виконавцями кібератак, або ж, наприклад, вирішити питання щодо того, чи існує в кіберконтексті обов’язок проявляти необхідну обачність.

В будь-якому випадку, міжнародна спільнота підійшла до того моменту, коли на кібератаки потрібно реагувати в юридичній площині. Попри те, що технічна та політична атрибуції в певній мірі можуть стримувати зростання кількості кібератак, ефект такого стримування порівняно незначний. Відтак, юридична атрибуція, навпаки, може підтвердити серйозне відношення держав до питання використання кібератак проти об’єктів критичної інфраструктури та сприяти атмосфері безпеки на регіональному та універсальному рівнях.

Висновки до третього розділу:

1. Борючись з кібератаками здійсненими недержавними акторами за підтримки чи фінансування держав-правопорушниць, держави-жертви кібератак не тільки зіштовхнулись з новими ворогами, а й знайшли партнерів в середовищі компаній, що займаються питаннями кібербезпеки. З одного боку, держави, які володіють значними кіберспроможностями, здатні самостійно здійснити атрибуцію кібератак. З іншого боку, досить рідко централізована урядова атрибуція здійснюється самостійно, без взаємодії з приватним сектором, що передбачає обмін інформацією. Саме державно-приватна співпраця може стати тим важелем, який запустить юридичну атрибуцію кібератак для цілей притягнення держав до міжнародної відповідальності.

Існує декілька пропозицій, які передбачають створення спеціалізованого механізму для здійсненню атрибуції, наприклад за моделлю МАГАТЕ. Наявні також пропозиції, які передбачають повне недопущення держави до процесу атрибуції в межах створеного міжнародного механізму. Такий підхід зводиться до пояснення через три ключові причини: не готовність держави публічно оприлюднювати докази, що використані в ході атрибуції, в силу того, що вони отримані в результаті розвідувальної діяльності; держави переслідують свої політичні інтереси; у випадку членства в такій міжнародній установі держави зможуть впливати на вибір справ для розслідування.

2. При вирішенні проблеми атрибуції, окрім державно-приватної співпраці, увагу привертає практика Європейського Союзу щодо сприяння відповідальній поведінці в кіберпросторі. З огляду на здійснений аналіз, видається, що Європейський Союз має намір всіляко заохочувати таку поведінку шляхом підвищення поваги до міжнародного права та впровадження не обов’язкових для виконання норм відповідальної поведінки в кіберпросторі.

Загалом діяльність Європейського Союзу в сфері виявлення та реагування на кіберзагрози демонструє принципово важливу позицію цього об’єднання до взаємодії з приватним сектор задля обміну інформацією та формування «європейського щита» кіберстійкості критичної інфраструктури. Залучення

різноманітних кіберакторів, співпраця з ООН, НАТО та регіональними організаціями, які зазначені в Стратегії кібербезпеки ЄС, сприятиме мітігації існуючих кіберзагроз, а також створенню універсальної системи виявлення та реагування на шкідливі кібератаки.

Що ж до ефективності інструментів кібердипломатії, зокрема кіберсанкцій, то факт встановлення відповідальних осіб в межах Європейського Союзу є однозначно позитивним кроком, який підкреслює недопустимість безкарності у випадку кібератак проти об'єктів критичної інфраструктури держави, які є джерелом основних послуг, а значить – забезпечення прав та свобод людини і нормального функціонування держав. Вважаємо, що міжнародна спільнота може перейняти досвід та практику ЄС щодо співпраці з різним акторами з ціллю встановлення джерела кібератаки (атрибуції). Крім того, міжнародна спільнота може вдатися до застосування кіберсанкцій в межах ООН, замінивши вибіркові (індивідуальні) кіберсанкції на секторальні з метою підвищення їх ефективності.

3. Кібератаки, ціллю яких була критична інфраструктура, свідчать про високу вірогідність успішних кібератак проти об'єктів критичної інфраструктури з деструктивними наслідками, що зростає з кожним днем. Ефект стримування можливо досягнути тоді, коли недержавні актори та держави будуть обізнані у невідворотності відповідальності, тому важливо розуміти перспективи розгляду міждержавного спору та процес доказування з ціллю атрибуції поведінки держава.

Перед розглядом міждержавного спору потрібно спочатку встановити комп'ютери та сервери, які застосовувалися задля здійснення кібератак, ідентифікувати осіб, які мають безпосередній стосунок до цих атак, а потім – довести, що ці особи діяли від імені конкретної держави, щоб атрибутувати їх дії державі. Відтак, судовий процес не можливий без попередньої технічної та політичної атрибуції кібератак. Також є важливим наявність спору, тому, вважаємо, що держави мають здійснювати публічну атрибуцію з вказівкою на конкретні порушення міжнародно-правових зобов'язань, що стали наслідком шкідливої діяльності держав в кіберпросторі (кібератаки).

4. Єдиний стандарт доказування відсутній. У випадку з Міжнародним Судом ООН, коли мова йде про звичайні порушення міжнародно-правових зобов'язань, Суд часто наполягає на представленні «переконливих доказів» або «вирішальних доказів», а іноді більш легкого стандарту «балансу вірогідностей» або «балансу доказів». Тобто навіть у випадку звичайних порушень, Суд зберігає свою гнучкість та автономність, оскільки згаданий стандарт фактично містить декілька більш жорстких та м'яких, що очевидно в результаті звичайної інтерпретації висловлювань Суду. Що ж до вирішення справ, які стосуються порушення імперативних норм *jus cogens*, правовим інтересом щодо виконання яких наділена вся міжнародна спільнота (*erga omnes*), звинувачення виняткової важкості, повинні бути доведені доказами, які є «повністю переконливими». Тобто, у випадку з кібератаками проти критичної інфраструктури саме їх наслідки визначатимуть стандарт, який застосовуватиметься.

5. Окрім визначення стандарту доказування та того, на кому лежить тягар доказування, перед Судом постане ще одне складне завдання – встановити чи мав місце конкретний факт і хто його здійснив. Враховуючи відсутність міжнародного незалежного та об'єктивного механізму, який би здійснював технічну атрибуцію, вважаємо, що Суд прийматиме докази без особливих обмежень. Відтак, оцінюватимуться положення релевантних договорів, офіційна документація (записи засідань) міжнародних організацій та національних парламентів; опубліковане та неопубліковане дипломатичне листування, комюніке та інші матеріали, включаючи книги, карти, плани, схеми, рахунки, архівні матеріали, фотографії, фільми, юридичні думки та думки експертів тощо; афідативи та декларації (заяви).

Не останню роль вірогідно відіграватимуть звіти неурядових організацій та незалежних ІТ-компаній чи компаній, що займаються питаннями кібербезпеки. Суд досить «недовірливо» відноситься до документів, підготовлених міжнародними неурядовими групами, але йому, очевидно, прийдеться змінити свій підхід. У випадку з кібератаками та технічною атрибуцією, яку здійснюють неурядові організації та приватні компанії, Суду необхідно буде

використовувати доповіді приватних організацій та залучати їхніх експертів до встановлення фактів справи, тому що, навряд чи, держави погодяться добровільно надати класифіковані документи чи правдиві відомості стосовно власних кіберслужб.

Важлива роль в процесі доказування також належатиме офіційним заявам. На думку Суду, заяви, що надходять від високопоставлених офіційних політичних діячів (іноді найвищого рангу) мають особливу доказову цінність, коли вони визнають факти або поведінку, несприятливу для держави, яку представляє особа, яка їх вчинила. Нарешті, цілком вірогідним є залучення свідків та експертів, які здійснюватимуть незалежну експертизу щодо встановлення достовірності представлених сторонами фактів.

6. Підсумовуючи, може зазначити, що Міжнародний Суд ООН, швидше за все, визнає неможливість здійснення атрибуції без попередньої технічної та політичної атрибуції. Враховуючи той факт, що оцінка технічних та політичних індикаторів згадується експертами Талліннського керівництва 2.0 та Групою урядових експертів ООН, цілком вірогідно, що Суд розробить тест альтернативний ефективному контролю.

Нарешті, розгляд міжнародного спору щодо атрибуції кібератак проти об’єктів критичної інфраструктури дозволить конкретизувати те, як звичаєві норми щодо атрибуції міжнародно-протиправних діянь застосовуються до кібератак. Відтак, це сприятиме формуванню єдиного підходу, що матиме позитивний вплив на атрибуцію кібератак в юридичній площині.

ВИСНОВКИ

1. Стрімкий розвиток ІКТ сприяв виникненню кіберпростору, який є віртуальним інформаційно-комунікаційним простором. Саме кіберпростір є середовищем реалізації кібератак та забезпечує їх необхідними засобами здійснення – технічними можливостями кіберпростору. Він складається з трьох різних рівнів (пластів): фізичного, логічного та соціального – в межах яких або проти яких можна здійснювати кібератаки. Серед основних характеристик кіберпростору: відсутність суверенної влади; тісний взаємозв'язок між системами та мережами, які використовуються як цивільними, так і військовими; віртуальний характер, який максимально обмежує можливість здійснення ідентифікації.

Кібератака є наступальною чи оборонною кібероперацією, яка цілком очікувано може призвести до завдання трав чи смерті осіб або шкоди чи знищення об'єктів. Кібероперацією також є кіберексплуатація, але, на відміну від кібератаки, кіберексплуатація не спрямована на порушення звичного функціонування комп'ютера або мережі, вона є актом спостереження та/чи копіювання даних.

2. Наразі відсутнє *lex specialis*, яке містило б спеціальне регулювання кібератак. Експерти Талліннського керівництва зробили значний внесок в розуміння того, як міжнародне право застосовується до кіберпростору, але керівництву, підготованому ними, бракує юридичної сили. Разом з тим, Група урядових експертів щодо досягнень в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки наголосила, що міжнародне право, і зокрема Статут Організації Об'єднаних Націй, застосовується у межах діяльності, пов'язаної з використанням ІКТ, а також підтвердила юрисдикцію держав над ІКТ-інфраструктурою на їх території.

Залежно від наслідків, кібератаки проти об'єктів критичної інфраструктури, в першу чергу, можуть призвести до порушень таких зобов'язань як: принципу суверенної рівності держав; принципу вирішення міжнародних суперечок мирними засобами; заборони погрози силою або її

застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і будь-яким іншим чином, несумісним з цілями Організації Об'єднаних Націй; принципу поваги до прав людини і основних свобод; принципу невтручання у внутрішні справи інших держав. Крім того, залежно від об'єкта кібератаки та її наслідків можна говорити про порушення норм спеціальних міжнародно-правових режимів. Попри заперечення низки держав, міжнародне право в повній мірі застосовується до кібератак, включаючи норми *jus in bello* та *jus ad bellum.*

4. Позиції держав, які опублікували офіційні заяви щодо того, як міжнародне право застосовується до кіберпростору, свідчать про загальну підтримку ідеї того, що воно застосовується. Коли ж мова йде про конкретні зобов'язання, держави не завжди спроможні виробити чітку позицію. Більшість держав в *opinio juris* характеризують суверенітет як принцип і норму міжнародного права. Але попри фундаментальне значення цього принципу, уряд Великобританії наполягає на тому, що не існує такої норми в межах сучасного міжнародного права. Ізраїль та США досі не визначились. Крім того, позиція Великобританії фактично йде врозріз з практикою держави.

Всі держави, які висловили свою офіційну позицію щодо застосування міжнародного права у кіберпросторі, зійшлись на тому, що принцип заборони інтервенції безсумнівно застосовується. Відтак, втручання у виборчий процес, що є втручанням у внутрішні справи держави та характеризується наявністю примусу (маніпулювання результатами голосування), втручання у фундаментальну діяльність парламенту або стабільність фінансових систем держав є поведінкою, що вимагає атрибуції.

В своїх заявах держави також підтверджують різні варіанти реагування на поведінку іншої держави в кіберпросторі, які міжнародне право їм надає (реторсії, контрзаходи, самооборона та застосування принципу необхідності). При цьому, застосування цих заходів реагування визначатиме вид атрибуції. Нарешті, в своїх позиціях держави не оминули увагою питання застосування норм звичаєвого права щодо атрибуції до кібератак. Вони сходяться на тому, що

для атрибуції потрібно, щоб діяльність здійснювалась органом держави; фізичними або юридичними особами, які здійснюють елементи урядових повноважень, або недержавними суб'єктами, які діють під керівництвом або під контролем держави, а також враховувала політичні та технічні індикатори.

6. Наразі конвенційне поняття «об'єкт критичної інфраструктури» або «критична інфраструктура» в міжнародному праві відсутні, що зумовлює необхідність звернення до підходів держав, які надають відповідні дефініції в своєму національному законодавстві. Вже зараз визначення критичної інфраструктури є необхідним кроком у формуванні політики безпеки та стійкості критичної інфраструктури до кібератак. Крім того, кількість секторів критичної інфраструктури варіюється від країни до країни – одні держави визначають лише 2 сектори в якості критичних, інші – доходять до 16-18. Вважаємо, що перший підхід є надто вузьким, а другий – занадто інклюзивним, тому при розробці поняття «критична інфраструктура» необхідно також визначити критерії оцінки критичності.

Загалом до критичної інфраструктури держави найчастіше відносять об'єкти та активи таких секторів як: сектор енергетики, сектор фінансів, сектор транспорту, сектор водопостачання; урядовий сектор; оборонний сектор; сектор реагування на надзвичайні ситуації та сектор охорони здоров'я. З урахування особливостей об'єктів критичної інфраструктури, які використовуються декількома державами, вважаємо за необхідне виокремити транснаціональну (міждержавну) критичну інфраструктуру в окрему категорію. Це зумовлено тим, що захист певних об'єктів критичної інфраструктури держави, як правило, залежить від національних пріоритетів, а захист міждержавної інфраструктури є результатом реалізації спільних інтересів.

7. Підвищення поваги та підтримання авторитету норм міжнародного права не можливе без встановлення відповідальності держав, які стоять за міжнародно-протиправними діяннями. Це випливає із правосуб'єктності держав та з факту того, що держави є головними носіями міжнародних зобов'язань, які вправі створювати функціональні правила поведінки та впливати на

міжнародний правопорядок. В силу того, що спеціальні правила щодо атрибуції кібератак відсутні в міжнародному праві, підстави присвоєння поведінки державі містяться в Статтях про відповідальність за міжнародно-протиправні діяння 2001 року. Статті про відповідальність не мають юридичного обов'язкового характеру, оскільки є доктриною, але більшість норм набула звичаєвого характеру, що виправдовує їх застосування до кібератак.

Підсумовуючи результати дослідження, можна зробити висновок про те, що дії кіберармій чи інших державних суб'єктів атрибутуються державам відповідно до норм міжнародного права відповідальності держав (стаття 4), навіть попри характер *ultra vires* (стаття 7). Атрибутуватись державі в кіберконтексті буде і поведінка індивідів чи юридичних осіб, що уповноважені здійснювати елементи урядових функцій. В кіберконтексті серед звичних для держави функцій, *inter alia*, виділяється кіберрозвідка та оборонні кібероперації. Лише поведінка, яка пов'язана із виконанням елементів урядових функцій, буде атрибутуватись держави (стаття 5). Стаття 8 Статей про відповідальність держав передбачає, що поведінка недержавних акторів атрибутується державі «лише якщо вона керувала або контролювала конкретну операцію і поведінка, на яку скаржилися, була невід'ємною частиною цієї операції. Відтак, необхідним є здійснення ефективного контролю. Саме держава повинна визначати виконання та хід конкретної операції, а кібердіяльність, якою займається недержавний суб'єкт, має становити «невід'ємну частину» операції держави.

8. Відповідно до принципу необхідної обачності (*due diligence*) держава повинна проявляти належну обачність, не дозволяючи використовувати свою територію чи кіберінфраструктуру під своїм урядовим контролем для кібероперацій, які зачіпають права інших держав та спричиняють серйозні несприятливі наслідки для них. Юридично обов'язкова природа даного принципу в кіберпросторі часто ставиться під питання. Разом з тим, позицію про те, що *due diligence* є загальним міжнародним зобов'язанням та становить *lex lata*, підтримали такі держави як Австралія, Чеську Республіка, Естонія, Нідерланди, Фінляндія та Франція.

Кібератаки на промислові системи управління особливо небезпечні при їх використанні проти об'єктів критичної інфраструктури, без належного функціонування яких люди можуть страждати від нестачі їжі, води, електроенергії, медичного обслуговування тощо. Відтак, порушення низки фундаментальних прав, яке на тривалий час унеможливлює їх реалізацію, дозволяє розглядати це зобов'язання в рамках міжнародного права прав людини, яке є спеціальним та досить сильним правовим режимом. Горизонтальний ефект прав людини та зобов'язання *due diligence* в контексті прав людини неодноразово було підтверджено у висновка спеціалізованих міжнародних установ, включаючи судові.

9. В силу обмежених людських та технічних ресурсів, шанси постраждалої держави присвоїти кібератаку державі були досить мізерними, тому поруч із юридичною атрибуцією (саме вона є одним із елементів міжнародно-протиправного діяння), виникає технічна та політична атрибуція кібератак. Ці види атрибуції можна розглядати як цілком не пов'язані між собою, або, навпаки, як частини цілого. Технічна атрибуція представляє криміналістичне розслідування, яке має на меті отримання прямих доказів щодо здійсненої кібератаки, тобто цифрових криміналістичних доказів. В той час як політична атрибуція ставить на меті визначити, хто причетний до кібератаки – індивід чи держава, та ґрунтується на політичному аналізі. Логічним завершенням цього ланцюжка атрибуцій повинна стати юридична атрибуція, яка неможлива без технічної та політичної атрибуції. Аналіз *opinio juris* держав свідчить про бажання та готовність атрибутувати кібератаки відповідальним державам, але юридична атрибуція, очевидно, є останнім кроком, який держави готові зробити.

В ході політичної та технічної атрибуції здійснюється оцінка політичних та технічних індикаторів. Може виникнути логічне питання щодо доцільності оцінки політичних індикаторів, але без їх врахування важко забезпечити достовірність атрибуції. І держави, і приватний сектор визнають, що технічні

індикатори можуть бути сфальсифіковані, тому паралельно мають оцінюватися політичні індикатори і за наявності враховуватися дані розвідки.

10. Дослідження кібератак 2015 та 2016 років проти України демонструє їх небезпеку для об'єктів критичної інфраструктури та важливість вивчення загального контексту, в якому були здійснені кібератаки. Хоча кібератаки на українські енергосистеми не спричинили фізичного руйнування, досвід України є прикладом того, як кібератаки можуть бути використані проти об'єктів критичної інфраструктури. Такі кібератаки не повинні розглядатися як проста шкідлива кібердіяльність, оскільки вони мали місце у воєнний час. Вони не виглядають випадковими у світлі триваючого збройного конфлікту. Час, обраний для кібератак, та воєнні дії на сході Донбасу до та після кібератак, свідчать про пряму чи опосередковану участь Російської Федерації.

Аналіз даних кібератак і результатів атрибуції демонструє важливість співпраці на початковому етапі з приватним сектором, який може допомогти з атрибуцією – підтвердивши або спростувавши її. Крім того, ситуація України, а саме здійснення кібератак в контексті збройного конфлікту на сході України демонструє важливість оцінки політичних індикаторів, а саме – контексту, зв'язку між приватними акторами та іноземною державою, мотивацію останньої та стратегічні інтереси тощо.

11. Державно-приватне партнерство в ході здійснення атрибуції кібератак є не тільки бажаним, а й потрібним. З одного боку, держави, які володіють значними кіберспроможностями, здатні самостійно здійснити атрибуцію кібератак. З іншого боку, досить рідко централізована урядова атрибуція здійснюється самостійно, без взаємодії з приватним сектором та обміну інформацією, оскільки паралельна централізована та децентралізована атрибуція є більш достовірною.

Більш тісна співпраця може стати тим важелем, який запустить правову атрибуцію кібератак для цілей притягнення держав до міжнародної відповідальності. Існує декілька пропозицій, які передбачають створення спеціалізованої організації по здійсненню атрибуції, наприклад за моделлю

МАГАТЕ. Наявні також пропозиції, які передбачають повне недопущення держави до процесу атрибуції в межах створеного міжнародного механізму. Такий підхід зводиться до пояснення через три ключові причини: не готовність держави публічно оприлюднювати докази, що використані в ході атрибуції, в силу того, що вони отримані як результат розвідувальної діяльності; держави переслідують свої політичні інтереси; у випадку членства в такій міжнародній установі держави зможуть впливати на вибір справ для розслідування.

12. При вирішенні проблеми атрибуції, окрім державно-приватної співпраці, увагу привертає практика Європейського Союзу щодо сприяння відповідальній поведінці в кіберпросторі. З огляду на здійснений аналіз, видається, що Європейський Союз має намір всіляко заохочувати таку поведінку шляхом підвищення поваги до міжнародного права та впровадження не обов'язкових для виконання норм відповідальної поведінки в кіберпросторі.

Загалом діяльність Європейського Союзу в сфері виявлення та реагування на кіберзагрози демонструє принципово важливу позицію цього об'єднання до взаємодії з приватним сектор задля обміну інформацією та формування «європейського щита» кіберстійкості критичної інфраструктури. Залучення різноманітних кіберакторів, співпраця з ООН, НАТО та регіональними організаціями, які зазначені в Стратегії кібербезпеки ЄС, сприятиме мітігації існуючих кіберзагроз, а також створенню універсальної системи виявлення та реагування на шкідливі кібератаки.

Що ж до ефективності інструментів кібердипломатії, зокрема кіберсанкцій, то факт встановлення відповідальних осіб в межах Європейського Союзу є однозначно позитивним кроком, який підкреслює недопустимість безкарності у випадку кібератак проти об'єктів критичної інфраструктури держави, які є джерелом основних послуг, а значить – забезпечення прав та свобод людини і нормального функціонування держав. Вважаємо, що міжнародна спільнота може перейняти досвід та практику ЄС щодо співпраці з різним акторами з ціллю встановлення джерела кібератаки (атрибуції). Крім того, міжнародна спільнота

може вдатися до застосування кіберсанкцій в межах ООН, замінивши вибіркові (індивідуальні) кіберсанкції на секторальні з метою підвищення їх ефективності.

13. 3. Кібератаки, ціллю яких була критична інфраструктура, свідчать про високу вірогідність успішних кібератак проти об'єктів критичної інфраструктури з деструктивними наслідками, що зростає з кожним разом. Ефект стримування можливо досягнути тоді, коли держави будуть обізнані у невідворотності відповідальності, тому важливо вже зараз правильно оцінити перспективи розгляду міждержавного спору та процес доказування з ціллю атрибуції поведінки держава.

Розгляд міжнародного спору складно уявити без попередньої технічної та політичної атрибуції кібератак. Також є важливим наявність спору, тому, вважаємо, що держави мають здійснювати публічну атрибуцію з вказівкою на порушення конкретних міжнародно-правових зобов'язань, що стали наслідком шкідливої діяльності держав в кіберпросторі (кібератаки).

Що стосується доказування, то єдиний стандарт доказування відсутній. Фактично наслідки кібератаки проти критичної інфраструктури визначатимуть стандарт, який застосовуватиметься. При розгляді спору оцінюватимуться положення релевантних договорів, офіційна документація (записи засідань) міжнародних організацій та національних парламентів; опубліковане та неопубліковане дипломатичне листування, комюніке та інші матеріали, включаючи книги, карти, плани, схеми, рахунки, архівні матеріали, фотографії, фільми, юридичні думки та думки експертів тощо; афідативи та декларації (заяви).

Не останню роль вірогідно відіграватимуть звіти неурядових організацій та незалежних ІТ-компаній чи компаній, що займаються питаннями кібербезпеки. Суд досить «недовірливо» відноситься до документів, підготовлених міжнародними неурядовими групами, але йому, очевидно, прийдеться змінити свій підхід. У випадку з кібератаками та технічною атрибуцією, яку здійснюють неурядові організації та приватні компанії, Суду необхідно буде використовувати доповіді приватних організацій та залучати їхніх експертів до

встановлення фактів справи, тому що, навряд чи, держави погодяться добровільно надати класифіковані документи чи правдиві відомості стосовно власних кіберслужб.

Підсумовуючи, може зазначити, що Міжнародний Суд ООН, швидше за все, визнає неможливість здійснення атрибуції без попередньої технічної та політичної атрибуції. Враховуючи той факт, що оцінка технічних та політичних індикаторів згадується експертами Талліннського керівництва 2.0 та Групою урядових експертів ООН, цілком вірогідно, що Суд розробить тест альтернативний ефективному контролю.

Нарешті, розгляд міжнародного спору щодо атрибуції кібератак проти об’єктів критичної інфраструктури дозволить конкретизувати те, як звичаєві норми щодо атрибуції міжнародно-протиправних діянь застосовуються до кібератак. Відтак, це сприятиме формуванню єдиного підходу, що матиме позитивний вплив на атрибуцію кібератак в юридичній площині та відповідальній поведінці держав в кібепросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрейченко С. С. Концепція атрибуції поведінки держави вміжнародному праві: монографія. Одеса: Фенікс, 2015. 578 с.
2. Бабін Б. Правове програмування та планування заходів протидії інформаційної агресії з Криму. Український часопис міжнародного права. 2019. № 2. С. 24-26.
3. Громовенко К. В. Захист критично важливих об’єктів інфраструктури в контексті міжнародного миру та безпеки. *Юридичний науковий електронний журнал*. № 9. 2021. С. 329-331.
4. Грушко М. В. Атрибуція кібератак як передумова забезпечення відповідальної поведінки держав в кібепросторі. Правова держава. № 43. 2021. С. 195-201.
5. Декларація про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об’єднаних Націй. ГА ООН 2625 (XXV) від 24 жовтня 1970 року.
6. Деякі питання об’єктів критичної інформаційної інфраструктури : Постанова КМУ від 9 жовтня 2020 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.
7. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року.
8. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/70/174 от 22.07.2015. URL: https://undocs.org/pdf?symbol=en/A/70/174.
9. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция ГА ООН A/68/98*. 24 июня 2013. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.
10. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной

безопасности. Резолюция ГА ООН A/70/174. 22 июля 2015. URL: https://undocs.org/pdf?symbol=en/A/70/174.

11. Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, Резолюция ГА ООН, A/76/135 от 14 июля 2021 года. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030R-1.pdf.
12. Замечание общего порядка № 31 [80]. Характер общего юридического обязательства, налагаемого на государства-участники Пакта, CCPR/C/21/Rev.1/Add.13, 26 мая 2004 г. 29 марта 2004 года. URL: http://hrlibrary.umn.edu/russian/gencomm/Rhrcom31.html.
13. Зведення прес-центру штабу АТО станом на ранок 17 грудня 2016 року. Міністерство оборони України. URL: http://www.mil.gov.ua/news/2016/12/17/zvedennya-pres-czentru-shtabu-ato-stanom-na-ranok-17-grudnya-2016-roku/.
14. Інформація про «втрати у ЗС України 80% гаубиць Д-30» не відповідає дійсності. Міністерства оборони України. 6 січня 2017 року. URL: https://www.mil.gov.ua/news/2017/01/06/informacziya-po-vtrati-u-zs-ukraini-80-gaubicz-d-30%E2%80%9D-ne-vidpovidae-dijsnosti/.
15. Климчук О. О. Кіберпростір як нова арена воєнних дій. *Актуальні проблеми управління інформаційною безпекою держави* : зб. мат-лів наук.-практ. конф. (22 берез. 2011 р.): [у 2 ч.]. Ч. 2. К. : Наук.-вид. відділ НА СБ України, 2011. С. 29-33.
16. Консультативное заключение Международного Суда ООН относительно законности угрозы ядерным оружием или его применения. A/51/218. 19 июля 1996. URL: https://www.icj-cij.org/public/files/advisory-opinions/advisory-opinions-1996-ru.pdf.
17. Международный пакт о гражданских и политических правах. Резолюция ГА ООН 2200 A (XXI) от 16 декабря 1966 года.
18. Музика В.В. Кібератаки та міжнародне право: природа та аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі : колект. моногр.

«Проблеми публічного та приватного права» / за заг. ред. Н. В. Мішиної. 2021. С. 309-342.

19. Музика В.В. Політика ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки. *Evropský politický a právní diskurz*. 2021. Том 8 (1). С. 46-51.
20. О Международном союзе электросвязи (МСЭ). Официальный сайт Международного союза электросвязи. URL: https://www.itu.int/ru/about/Pages/default.aspx.
21. Об очередных нелегитимных ограничительных мерах Европейского союза против России: Заявление МИД России от 24.02.21. Министерство иностранных дел РФ. URL: https://malta.mid.ru/ru_RU/press-service/-/asset_publisher/ThwJuaSWCFQj/content/zaavlenie-mid-rossii-ob-ocerednyh-nelegitimnyh-ogranicitel-nyh-merah-evropejskogo-souza-protiv-rossii?inheritRedirect=true.
22. Ответственность государств за международно-противоправные деяния. Резолюция, принятая Генеральной Ассамблеей 13 декабря 2016 года [по докладу Шестого комитета (A/71/505)] 71/133. URL: https://undocs.org/ru/A/RES/71/133.
23. Отчет о действиях по предварительному расследованию. 14 ноября 2016 г. URL: https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-pe-ukraine.pdf.
24. Порошенко: Держструктури зазнали 6,5 тисячі кібератак, до деяких причетна РФ. Укрінформ. URL: https://www.ukrinform.ua/rubric-polytics/2148600-porosenko-derzstrukturi-zaznali-65-tisaci-kiberatak-do-deakih-pricetna-rf.html.
25. Природа обязательств государств участников (пункт 1 статьи 2 Пакта). Замечание общего порядка № 3 (пятая сессия,1990 год).
26. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України № 563 від 23 серпня 2016 р.
27. Про критичну інфраструктуру : законопроект № 5219 від 09.03.2021. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71355.

28. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України : Рішення Ради національної безпеки та оборони від 1 березня 2014. Відомості Верховної Ради України. 2014, № 12, ст. 214.
29. Про основні засади забезпечення кібербезпеки України: Закон України від 15.12.2021. *Відомості Верховної Ради*. 2017. № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
30. Про ринок електричної енергії : Закон України від 13.04.2017. *Відомості Верховної Ради* (ВВР). 2017, № 27-28, ст. 312. URL: https://zakon.rada.gov.ua/laws/show/2019-19#Text.
31. Про Стратегію національної безпеки України : Указ Президента України № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року».
32. Публікація Ярослава Шерстюка від 22 грудня 2016 року (10:48). Facebook. URL: https://www.facebook.com/100001918687149/posts/1374145112659432/.
33. Публікація Ярослава Шерстюка від 22 грудня 2016 року (12:34). Facebook. URL: https://www.facebook.com/100001918687149/posts/1374231455984131/.
34. Сили АТО відбили наступ ворога на Донецькому напрямку. Міністерство оборони України. 18 грудня 2016. URL: http://www.mil.gov.ua/news/2016/12/18/sili-ato-vidbili-nastup-voroga-na-doneczkomu-napryamku/.
35. Ситуація з правами людини в АР Крим та місті Севастополь (Україна), Резолюція 71/205 від 19.12.2016 року.
36. Сініцин Р. Звіт про злам українського софту для артилерії хакерами FancyBear – психологічна операція Москви. Вебсайт InformNapalm. URL: https://informnapalm.org/ua/zvit-pro-zlam-fancybear/.
37. Стратегія кібербезпеки України (2021 – 2025 роки). Безпечний кіберпростір – запорука успішного розвитку країни : затверджено Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.

38. Сурілова О.О. Публічна атрибуція кібератак державами-членами ЄС та застосування кіберсанкцій Союзом щодо кібератак, які становлять загрозу ЄС та його членам. Правова держава. № 43. 2021. С. 209-216.
39. Територіальна цілісність України, Резолюція Генеральної асамблеї ООН 68/262 від 27.03.2014 року.
40. Хлебная корзина Молотова – Molotov bread basket. Википедия. URL: https://360wiki.ru/wiki/Molotov_bread_basket.
41. Циверенко Г. П. Фактичні підстави для виникнення міжнародно-правової відповідальності. *Актуальні проблеми держави і права*. 2014. С. 152-157.
42. Шеломенцев В. Поняття та сутність кібернетичної атаки. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. № 25'2011. С. 337-344.
43. 10 фактів про збройну агресію Росії проти України. 09.12.2019. URL: https://mfa.gov.ua/10-faktiv-pro-zbrojnu-agresiyu-rosiyi-proti-ukrayini.
44. 2013-2014 Eylem Planı 20/06/2013 tarih. URL: https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf.
45. 2016-2019 Ulusal Siber Güvenlik Stratejisi. URL: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf.
46. Alperovitch D. Bears in the Midst: Intrusion into the Democratic National Committee. CrowdStrike Blog. June 15, 2016. URL: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.
47. Annex B: Australia`s position on how international law applies to State conduct in cyberspace. URL: https://www.internationalcybertech.gov.au/our-work/annexes/annex-b.
48. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, International Court of Justice, 26 February 2007.
49. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, International Court of Justice Reports 2005, p. 168.

50. Arsene L. 5 Times More Coronavirus-themed Malware Reports during March. Bitdefender website. URL: https://www.bitdefender.com/blog/labs/5-times-more-coronavirus-themed-malware-reports-during-march/.
51. Attribution of cyber incident to Russia. Minister for Foreign Affairs, Minister for Women, Senator the Hon Marise Payne. URL: Attribution of cyber incident to Russia | Australian Minister for Foreign Affairs Minister for Women (foreignminister.gov.au).
52. Australia, Australia's International Cyber Engagement Strategy. Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace. October 2017. 108 p. URL: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf.
53. Bassiouni M. Ch. International Crimes: Jus cogens and obligation erga omnes. *Law and Contemporary Problems*. Vol 59(4). 1996. P. 63-74.
54. Beyond U.S.-China Talking Points: Undiplomatic Questions That Won`t Be Asked of Xi Jinping. Hudson Institute. September 23, 2015. URL: https://www.hudson.org/research/11721-beyond-u-s-china-talking-points-undiplomatic-questions-that-won-t-be-asked-of-xi-jinping.
55. Bing Ch. Suspected Russian hackers spied on U.S. Reuters. URL: Suspected Russian hackers spied on U.S. Treasury emails - sources | Reuters.
56. Bodansky D., Crook J. Symposium on the ILC`s State Responsibility Articles: Introduction and Overview. *American Journal of International Law*. Vol. 96, No. 4. October 2002. P. 773-791. URL: https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1440&context=fac_artchop.
57. Borys C. The day a mysterious cyber-attack crippled Ukraine. BBC. Published on 4th July 2017. URL: https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine.
58. Brown K. A., McCarthy J. A. Critical path: A brief history of critical infrastructure protection in the United States. Fairfax, Va: Spectrum Pub. Group. 2006. 198 p.
59. Buttigieg J. The common heritage of mankind: from the law of the sea to the human genome and cyberspace. *Symposia Melitensia*. Vol.8. 2012. p. 81-92.

60. Caltagirone S. Industrial cyber attacks: a humanitarian crisis in the making. *Humanitarian Law & Policy*. *ICRC Blog*. 2019. URL: https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/.
61. Canada-United States Cooperation on Critical Infrastructure. Government of Canada. URL: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cnd-ntd-stts-cprtn-en.aspx.
62. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986.
63. Case concerning the Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua intervening) (El Salvador v. Honduras), I.C.J., Judgment of 11 September 1992.
64. Case of A. v. The United Kingdom. No. 25599/94. September 23, 1998. URL: http://www.cirp.org/library/legal/A_v_UK1998/.
65. Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 665.
66. Charney S., English E., Kleiner A. From Articulation to Implementation: Enabling Progress on Cybersecurity Norms. Microsoft. June 2016. 15 p. URL: query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.
67. Clark D., Landau S. Untangling Attribution. *Massachusetts Institute of Technology*. 2011. URL. http://static.cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf.
68. Combating the criminal misuse of information technologies, Resolution adopted by the General Assembly. UN GA Res 55/63. 4 December 2000. URL: https://undocs.org/A/RES/55/63.
69. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. International Red Cross Committee. 1987. 1625 p.
70. Comments by the International Committee of the Red Cross (ICRC) to Substantive Report [First Draft] of the ‘Open-ended working group on developments in the field of

information and telecommunications in the context of international security' (OEWG), dated 3 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/ICRC-Comments-on-the-First-Draft-of-the-OEWG-Report.pdf.

71. Corfu Channel Case (United Kingdom v. Albania); Merits, International Court of Justice, 9 April 1949. URL: https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf.
72. Corn G. Cyber National Security: Navigating Gray Zone Challenges. *In Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare (2018, Forthcoming).* 71 p. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089071.
73. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7299/2019/INIT, OJ L 129I. 17.05.2019. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797.
74. Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (ST/9564/2020/INIT) (OJ L 246, 30.7.2020. p. 12-17. URL: http://data.europa.eu/eli/dec/2020/1127/oj.
75. Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 351I , 22.10.2020, p. 5-7). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1537.
76. Council Decision 7299/19 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. 14 May 2019. URL: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf.
77. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). URL: http://data.europa.eu/eli/dir/2008/114/oj.

78. Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (ST/9568/2020/INIT) (OJ L 246, 30.7.2020, p. 4-9). URL: http://data.europa.eu/eli/reg_impl/2020/1125/oj.
79. Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 351I, 22.10.2020, p. 1-4). URL: http://data.europa.eu/eli/reg_impl/2020/1536/oj.
80. Coynash H. Russia brings ‘humanitarian’ convoys to Ukraine by day, military trucks carrying death by night. Kharkiv Human Rights Protection Group Information Portal “Human Rights in Ukraine”. URL: https://khpg.org/en/1564595792.
81. Crash Override: The Malware That Took Down a Power Grid. URL: https://www.wired.com/story/crash-override-malware/.
82. CrashOverride: Analysis of the Threat to Electric Grid Operations. Dragos Inc. 35 p. URL: https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.
83. CrashOverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. By Joe Slowik, Dragos Inc. 16 p. URL: https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.
84. Crawford J. Historical background and development of codification. *United Nations Audiovisual Library of International Law*. 2012. 10 p. URL: https://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_e.pdf.
85. Crawford J. Responsibility to the International Community as a Whole. *Indiana Journal of Global Legal Studies*. Vol. 8 : Iss. 2. 2001. P. 303-322. URL: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1215&context=ijgls.
86. Crawford J. State Responsibility. Max Planck Encyclopedia of Public International Law. Oxford University Press, 2015. URL: https://spacelaw.univie.ac.at/fileadmin/user_upload/p_spacelaw/EPIL_State_Responsibility.pdf.

87. Crimea without power from Ukraine after electricity pylons ‘blown up’. Reuters. URL: https://www.reuters.com/article/us-ukraine-crisis-crimea-electricity-idUSKCN0TB04920151122.
88. Critical Five: Forging a Common Understanding for Critical Infrastructure. Shared Narrative. March 2014. 16 p. URL: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf.
89. CrowdStrike Intelligence Report «Putter Panda». URL: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.
90. CSE Statement on the NotPetya Malware. URL: https://www.cse-cst.gc.ca/en/media/2018-02-15.
91. Cyber and International Law in the 21st Century, From Attorney General`s Office and The Rt Hon Jeremy Wright QC MP. Published 23 May 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
92. Cyber Capabilities and National Power: A Net Assessment. International Institute for Strategic Studies research paper. Published on 28 June 2021. 174 p. URL: https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---united-states.pdf.
93. Cyberattack hits German train stations as hackers target Deutsche Bahn. URL: http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/.
94. Cybersecurity Strategy: Remarks by the High Representative / Vice-President Josep Borrell at the joint press conference with Vice-President Margaritis Schinas and Commissioner Thierry Breton (European Commission). URL: https://eeas.europa.eu/headquarters/headquarters-homepage/90700/cybersecurity-strategy-remarks-high-representativevice-president-josep-borrell-joint-press_en.
95. Czech Republic, Comments submitted by the Czech Republic in reaction to the initial ‘pre-draft’ report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security. April

2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf.

96. Czech Republic, Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace Director of Cybersecurity Department, dated 11 February 2020. URL: https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.

97. Davis J., Boudreaux B. and others. Stateless Attribution: Toward International Accountability in Cyberspace. Santa Monica, CA: RAND Corporation, 2017. 57 p. URL: https://www.rand.org/pubs/research_reports/RR2081.html.

98. Declaration by Miguel Rodriguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York, June 23, 2017. URL: https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.

99. Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace. Armed Forces Cyberspace Center - July 2020. URL: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

100. DHS-FBI Joint Analysis Report on Grizzly Steppe Russian Malicious Cyber Activity. Department of Homeland Security, Federal Bureau of Investigation. December, 29, 2016. URL: https://publicintelligence.net/dhs-fbi-grizzly-steppe/.

101. Dieter G. Values in German Constitutional Law. *An Inquiry into the Existence of Global Values: Through the Lens of Comparative Constitutional Law*. London: Bloomsbury Publishing, 2015. P. 199-214.

102. Digital Around the World. Datareportal. 7 July 2021.URL: https://datareportal.com/global-digital-overview.

103. Dinstein Y. The Conduct of Hostilities under the Law of International Armed Conflict. Cambridge University Press, Cambridge. 2004. 275 p.

104. Disruption of a GRU cyber operation in The Hague. Letter of 4 October 2018 from the Minister of Defence Ank Bijleveld-Schouten, Minister of Foreign Affairs Stef

Blok and Minister of Justice and Security Ferdinand Grapperhaus, to the House of Representatives, regarding the disruption of a GRU cyber operation in The Hague. URL: https://english.defensie.nl/downloads/parliamentary-documents/2018/10/04/disruption-of-a-gru-cyber-operation-in-the-hague.

105. DOD General Counsel Remarks at U.S. Cyber Command Legal Conference. Remarks By Hon. Paul C. Ney, Jr. March 2, 2020. URL: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

106. Dörmann K. Applicability of the Additional Protocols to Computer Network Attacks. ICRC. 2004. 12 p. URL: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm

107. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries 2001. *Yearbook of the International Law Commission*, 2001, vol. II, Part Two. P. 31-143. URL: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

108. Draft conclusions on identification of customary international law, with commentaries 2018: https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf.

109. Eichensehr K. Public-Private Cybersecurity. *Texas Law Review*. No. 95. 2017. P. 467-538.

110. Emmott R. Russia unlikely to meet Ukraine peace deal deadline, NATO says. Reuters. URL: https://www.reuters.com/article/us-ukraine-crisis-nato-idUSKBN0TL1FA20151202.

111. Estonia, President of the Republic at the opening of CyCon 2019 (29 May 2019). URL: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

112. EU imposes the first ever sanctions against cyber-attacks, Council of the EU. URL: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/pdf.

113. European Commission, COM (2001) 298. *Network and Information Security: Proposal for A European Policy Approach*. 6 June 2001. URL: https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf.

114. Executive Order 13010, U.S. Federal Register, Vol. 61, No. 138, July 17, 1996. URL: https://www.govinfo.gov/content/pkg/FR-1996-07-17/pdf/96-18351.pdf.

115. Executive Order on Improving the Nation's Cybersecurity. White House. 12.05.2021. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

116. FBI, Update on Sony Investigation, Press Release (Dec. 19, 2014). URL: https://www.fbi.gov/news/pressrel/pressreleases/update-on-sony-investigation.

117. Final OEWG report adopted on 12 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

118. Finland, Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, February 10 and 11', February 2020. URL: https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf.

119. Finland's national positions, International law and cyberspace, 2020. 8 p. URL: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.

120. First Meeting of the first substantive session of the Open-Ended Working Group (OEWG). URL: https://dig.watch/resources/1st-meeting-first-substantive-session-open-ended-working-group-oewg.

121. Foreign Office Minister condemns Russia for NotPetya attacks (15.02.2018). URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

122. Foreign Relations of the United States, The Conferences at Washington, 1941–1942, and Casablanca, 1943 Document 412. URL: https://history.state.gov/historicaldocuments/frus1941-43/d412.

123. French Ministry of the Armies, International Law Applied to Operations in Cyberspace' (9 September 2019). URL: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

124. García Amador F. V., First Report on International Responsibility 1956. *Yearbook of the International Law Commission*. UN Doc. A/CN.4/SER.A/1956/Add.1. URL: https://legal.un.org/ilc/publications/yearbooks/english/ilc_1956_v2.pdf.

125. General Assembly, Note verbale dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations addressed to the Secretary-General. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/411/07/PDF/N1341107.pdf?OpenElement.

126. Gioe D., Goodman M., Wanless A. Rebalancing cybersecurity imperatives: patching the social layer. *Journal of Cyber Policy*. 4:1. P. 117-137.

127. González M. J. The doctrine of the Drittwirkung der Grundrechte in the case law of the Inter-American Court of Human Rights. InDret. 2008. 31 p.

128. Government Facilities Sector-Specific Plan 2015. Cybersecurity & Infrastructure Security Agency. URL: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf.

129. GReAT, BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents. SecureList, Kaspersky Lab. January 28, 2016. URL: https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employspearphishing-with-word-documents/.

130. Green J. Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice. *International & Comparative Law Quarterly* Vol. 58. Issue 1. P. 163-179.

131. Greenberg A. New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. Wired website. 09.12.2019. URL: https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

132. Hathaway O., Crootof R. The Law of Cyber-Attack. *California Law Review*. Vol. 100. 2012. p. 817-885.

133. Harris D.J. Cases and Materials on International Law. 56th Edition, 1998. 1150 p.

134. Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security.* Vol. 4. No. 2. 2011. P. 49-60.

135. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Official website of Cybersecurity & Infrastructure Security Agency. December 17, 2003. URL: https://www.cisa.gov/homeland-security-presidential-directive-7.

136. How an Entire Nation Became Russia`s Test Lab for Cyberwar. WIRED. URL: https://www.wired.com/story/russian-hackers-attack-ukraine/.

137. How do you say Ground Hog Day in Ukrainian? SANS. URL: https://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian.

138. Hybrid Threats: 2007 cyber attacks on Estonia (2019). *Hybrid Threats. A Strategic Communications Perspective*. Riga: NATO Strategic Communications Centre of Excellence. P. 52-69. URL: https://stratcomcoe.org/pdfjs/?file=/publications/download/cyber_attacks_estonia.pdf?zoom=page-fit.

139. ICTY, Prosecutor v. Dusko Tadic´, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995.

140. Imposing Costs for Harmful Foreign Activities by the Russian Government. April 15, 2021. White House website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

141. Infrastructure Sector in India: Definitions; Growth and Infrastructure Linkage. Civilsdaily website. October 11, 2017. URL: https://www.civilsdaily.com/infrastructure-sector-in-india-definitions-growth-and-infrastructure-linkage/#:~:text=Infrastructure%20is%20a%20key%20driver%20of%20the%20overa

ll,blocks%20required%20for%20an%20economy%20to%20function%20efficiently%E2%80%9D.

142. Instruction Generale Interministerielle Relative a la Securite des Activitess d'Importance Vitale N°6600/SGDSN/PSE/PSN du 7 janvier 2014. Premier Ministre, Secretariat General de la Defense et de la Securite Nationale. Direction Protection et Sécurité de l'Etat N° NOR: PRMD1400503J. 71 p. URL: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf.

143. Island of Palmas Case (USA v. The Netherlands). Award, Permenent Court of Arbitration. Volume II. 4 April 1928. P. 829-871.

144. ITU contributes to global cybersecurity resilience with 2020 Global CyberDrills. URL: https://www.itu.int/ru/myitu/news/2020/09/16/20/01/cybersecurity%20resilience%202020%20itu%20global%20cyberdrills/.

145. Johnson D., Post D. Law and Borders – The Rise of Law in Cyberspace. *Stanford Law Review*. Vol. 48, No. 5. May, 1996. P. 1367-1402.

146. Joint proposal on the text of the 1st Draft. URL: https://front.un-arm.org/wp-content/uploads/2021/03/PDF-Joint-Contribution-OEWG-First-Draft-Suggested-amendments.pdf.

147. Joint Publication 3-13: Information Operations, US Joint Chiefs of Staff. 27 November 2012. 68 p.

148. Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA). January 05, 2021. URL: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

149. Juridical Condition and Rights of the Undocumented Migrants, Advisory Opinion OC-18/03, Inter-Am. Ct. H.R. (ser. A) no. 18, (17 Sep 2003). URL: http://www.refworld.org/docid/425cd8eb4.html.

150. Karniyevich N., Niemann F. The German IT Security Act 2.0 comes into force – Overview of the most significant changes to the BSI Act. URL:

https://www.twobirds.com/en/news/articles/2021/germany/the-german-it-security-act-2-0-comes-into-force.

151. Korzak E. UN GGE on Cybersecurity: The End of an Era? In The Diplomat. 31 July 2017. URL: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

152. Kovalenko I., Meydoni I. Zerologon Vulnerability: Analysis and Detection Tools. Cynet website. September 26, 2020. URL: https://www.cynet.com/zerologon/.

153. Kozlowski A. Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*. Vol. 3. February 2014. P. 239-245. URL: https://eujournal.org/index.php/esj/article/view/2941/2770.

154. Krotofil M. Casualties caused through computer network attacks: the potential human costs of cyber warfare. *Whither the Human in Armed Conflict? IHL Implications of New Technology in Warfare* : Proceedings of 42nd Round Table on Current Issues of International Humanitarian Law. Sanremo, 4th-6th September 2019. P. 73-79.

155. Kuzmenko O., Cobus P. Think Tank: Cyber Firm at Center of Russian Hacking Charges Misread Data posted on March. Voice of America News official website. URL: https://www.voanews.com/a/crowdstrike-comey-russia-hack-dnc-clinton-trump/3776067.html.

156. Latest from OSCE Special Monitoring Mission (SMM) to Ukraine, based on information received as of 19:30 hrs, 23 December 2015. URL: https://www.osce.org/ukraine-smm/212656.

157. Latest from OSCE Special Monitoring Mission (SMM) to Ukraine, based on information received as of 19:30, 18 December 2016. URL: https://www.osce.org/ukraine-smm/290026#_ftnref1.

158. Lepard B. *Customary international law: a new theory with practical applications*. Cambridge University Press. 2010. 419 p.

159. Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations addressed to the Secretary-General. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/934.

160. Letter to the parliament on the international legal order in cyberspace. Dutch Ministry of Foreign Affairs. 5 July 2019. URL: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/BZ129031A+letter+to+Parliament+-+international+law+-+cyberspace+-+NL.pdf.

161. Leyden J. Russia's to Blame for Pro-ISIS Megahack on French TV Network. The Register website. June 10, 2015. URL: https://www.theregister.co.uk/2015/06/10/russian_trolls_staged_tv5monde_megahack_shocker/.

162. Lin H. Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Columbia Journal of International Affairs.* Vol. 70, No. 1. 2016. P. 75-137.

163. Lohrmann D., Lohrmann D. 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic. Government technology website. URL: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

164. Mačák K. Rodenhäuser T., Gisel L. Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections? Just Security website. April 2, 2020. URL: https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

165. Mandiant`s Report, APT1 Exposing One of China's Cyber Espionage Units. 2013. 74 p. URL: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

166. McGoogan C., Willgress L. UK rail network hit by multiple cyber attacks last year. 12 July 2016. URL: http://www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attacks-last-year/.

167. Minister for Law Enforcement and Cyber Security Hon. Angus Taylor MP Australian Government attribution of the 'NotPetya' cyber incident to Russia

16.02.2018. URL: https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-attributesnotpetya-malware-to-russia.pdf.

168. National Cyber Security Centre, Reckless Campaign of Cyber Attacks by Russian Military Intelligence Exposed. 3 October 2018. URL: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

169. National Cyber Security Strategy 2016-2021. HM Government website. 81 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

170. National Strategy for Critical Infrastructure Protection (CIP Strategy). Federal Republic of Germany, Federal Ministry of the Interior. Berlin, 17th June 2009. URL: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1.

171. Naveen G. Failed Cyber Attack on Paris Hospital Authority // Cybersecurity Insiders website. 2020. URL: https://www.cybersecurity-insiders.com/failed-cyber-attack-on-paris-hospital-authority/.

172. Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW. Government of the Netherlands website. 04.10.2018. URL: https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw#:~:text=On%2013%20April%202018%2C%20with%20support%20from%20the,out%20by%20a%20Russian%20military%20intelligence%20%28GRU%29%20team.

173. Netherlands` Cyber Warfare, No 77, AIV/ No 22, CAVV. Advisory Council on International Affairs and Advisory Council on International Affairs. December 2011. 46 p.

174. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. Questions and Answers. European Commission website.

16.12.2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2392#cybersecurity.

175. Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guard Corps. 2018. URL: https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic.

176. North Sea Continental Shelf (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands), Judgment, I.C.J. Reports 1969, p. 3.

177. Norwegian Official Report: Når sikkerhet er viktigst - Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner. Department of Justice and Public Security . NOU 2006:6. 323 p.

178. Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I. C. J. Reports 2003, p. 189.

179. Oklahoma City Bombing. U.S. Government website. URL: https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing.

180. Osborne G. Chancellor's speech to GCHQ on cyber security. 17 November 2015. URL: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

181. Ottis R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

182. Owens W., Dam K., Lin H. Technology, Policy, Law, and Ethics. Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Committee on Offensive Information Warfare, National Research Council. 2009. 367 p.

183. Paganini P. FireEye Claims Russian APT28 Hacked France’s TV5Monde Channel. Security Affairs website. June 10, 2015. URL: http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html.

184. Panetta L. Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security. U.S. Department of Defense. 11 October 2012. URL: http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

185. Peterson A. Sony Pictures hackers invoke 9/11 while threatening theaters that show 'The Interview'. Washington Post website. 14.12.2014. URL: https://www.washingtonpost.com/news/the-switch/wp/2014/12/16/sony-pictures-hackers-invoke-911-while-threatening-theaters-that-show-the-interview/.

186. Plan maestro de infraestructura de El Salvador para el periodo 2019 -2030: Un instrumento de planeación de infraestructura multisectorial a largo plazo que permitirá potenciar el desarrollo económico y social de El Salvador. Jan 2020. URL: https://publications.iadb.org/es/plan-maestro-de-infraestructura-de-el-salvador-un-instrumento-de-planeacion-de-infraestructura.

187. Plotnikov O. V. Defining Transitional Justice: Scholarly Debate and UN Precision. *Lex Portus*. 2017. No 1(3). P. 50-63.

188. Polityuk P. Ukraine sees Russian hand in cyber attacks on power grid. Reuters website. 12 February 2016. URL: https://www.reuters.com/article/us-ukraine-cybersecurity/ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E.

189. Proietti G. Lysander's Victories, Callicratidas' Defeat (Hellenica I.v-II.i.28). *Xenophon's Sparta*. Leiden, The Netherlands. 1987. P. 10-29.

190. Project Grey Goose Report on Critical Infrastructure: Attacks, Actors and, Emerging Threats. URL: http://dataclonelabs.com/security_talkworkshop/papers/25550091-Proj-Grey-Goose-report-on-Critical-Infrastructure-Attacks-Actors-and-Emerging-Threats.pdf.

191. Prosecutor v. Dusko Tadic. International Criminal Tribunal for Former Yugoslavia. Appeals Chamber's Judgement of 15 July 1999.

192. Protecting Nationally Critical Infrastructure from Cyber Attacks: A National Resilience Policy Perspective (Melindungi Infrastruktur Kritis Nasional dari Serangan Cyber: Perspektif Kebijakan Ketahanan Nasional). January 25, 2017. URL:

https://www.wantannas.go.id/2017/01/25/melindungi-infrastruktur-kritis-nasional-dari-serangan-cyber-perspektif-kebijakan-ketahanan-nasional/.

193. Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14.

194. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UNGA Resolution, A/76/135, dated on 14 July 2021.

195. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security UNGA Resolution A/70/150. Seventieth session, dated on 22 July 2015.

196. Report of the International Law Commission, 26th Session, A/CN.4/Ser.A/1974. *International Law Commission Yearbook.* Vol. II(1). 1974. 302 p.

197. Requirements for collection and preservation of cybersecurity incident evidence. Recommendation ITU-T X.1216. URL: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14560.

198. Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/56/589 and Corr.1)] 56/83. Responsibility of States for internationally wrongful acts. URL: https://undocs.org/en/A/RES/56/83.

199. Roscini M. Digital Evidence as a Means of Proof before the International Court of Justice. *Journal of Conflict and Security Law*. Vol. 21. Issue 3. 2016. P. 541-554.

200. Roscini M. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal.* Vol. 50, Symp. Issue 2. P. 234-273.

201. Rosenne Sh. The Law and Practice of the International Court. BRILL. 2006. 1892 p.

202. Russell A. The Logic Layer. *Strategic A2/AD in Cyberspace* (pp. 40-52). Cambridge: Cambridge University Press. 2017. P. 40-52.

203. Russia: UK exposes Russian involvement in SolarWinds cyber compromise. UK`s Government official website. URL:

https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise.

204. Sassoli M. International Humanitarian Law : Rules, Controversies, and Solutions to Problems Arising in Warfare. Edward Elgar Publishing Limited. 2019. 656 p.

205. SBU Press Center, Russian Hackers Plan Energy Subversion in Ukraine. Ukrinform website. December 28, 2018. URL: http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html.

206. Schmitt M. 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*. Vol. 54. 2014. P. 697-732.

207. Schmitt M. Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*. Vol. 56, Issue 3, Art. 10. 2011. P. 569-605.

208. Schmitt M. Cyber operations and the jus in bello: key issues. *Naval War College International Law Studies.* Vol. 87. 2011. P. 89-110.

209. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. 2017. 598 p.

210. Schmitt M. Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. 2013. 215 p.

211. Schmitt, M. N. Wired warfare: computer network attack and jus in bello. *International Review of the Red Cross*. Vol. 84. 2002. P. 365-399.

212. Schöndorf R. Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law Studies*. Vol. 97. 2021. P. 395-406.

213. Schoolboy hacks into city`s tram system. Telegraph website. URL: https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

214. Service Public Fédéral Intérieur/Federale Overheidsdienst Binnenlandse Zaken F./N. 2011-1799; C-2011/00399 (2011). 43 p. URL: https://www.ibz.be/sites/default/files/media/docs/jaarverslag-ibz-2011-web.pdf.

215. Setola R., Luiijf E., Theocharidou M. Critical Infrastructures, Protection and Resilience. *Managing the Complexity of Critical Infrastructures*. *Studies in Systems, Decision and Control*. Vol 90. Springer. 2016. P. 1-18.

216. Stanglin D., Weise E. North Korea Internet hit by 2 more outages. USA TODAY website. 23.12.2014. URL: https://www.usatoday.com/story/news/world/2014/12/23/north-korea-internet-web-disrupted-goes-down/20806265/.

217. Statement by Georg Sparser, Deputy Permanent Representative Permanent Mission of the Principality of Liechtenstein to the UN. 10 February 2020. URL: https://ccdcoe.org/uploads/2020/04/Statement-on-International-Law-by-Liechtenstein-at-2nd-session-of-OEWG.pdf.

218. Statement from the Press Secretary. White House website. February 15, 2018. URL: https:// www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

219. Statement of Foreign Office Minister, Lord Ahmad, Foreign Office Minister condemns Russia for NotPetya attacks. 15 October 2018. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

220. Statement of Foreign Office Minister, Lord Ahmad, Foreign Office Minister condemns criminal actors based in Iran for cyber-attacks against UK universities'. 23 March 2018. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-criminal-actors-based-in-iran-for-cyber-attacks-against-uk-universities.

221. Statement of Global Affairs Canada. Canada identifies malicious cyber-activity by Russia. 04 October 2018. URL: https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html.

222. Statement of the Ministry of Foreign Affairs on Twitter: "Russia`s recent #cyberattack to cause destructive effects in #Georgia`s sovereign territory

demonstrates their desire to act without regard to international norms. This unlawful act must draw strong condemnation of International community http://gov.ge/s/956b4" 20 February 2020. URL: https://twitter.com/MFAgovge/status/1230479514431631363?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1230479514431631363%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2F1tv.ge%2Fen%2Fnews%2Feuropean-countries-condemn-russia-over-georgia-cyberattack%2F.

223. Stockburger P. Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents. *NATO CCD COE Publications.* 2017. 14 c. URL: https://ccdcoe.org/uploads/2018/10/Art-10-Toward-a-New-Lex-Specialis-Governing-State-Responsibility-for-Third-Party-Cyber-Incidents.pdf.

224. Strategy and governance. URL: https://ccdcoe.org/library/strategy-and-governance/?category=intl-law-statements.

225. Summary of Estonia`s Position on how International Law Applies in Cyberspace. 2019. URL: https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/ee_positions_en.pdf.

226. Switzerland`s position paper on the application of international law in cyberspace. UNGA Resolution 73/266. Annex UN GGE 2019/2021. P. 85-105.

227. Territorial and Maritime Dispute between Nicaragua and Honduras in the Caribbean Sea (Nicaragua v. Honduras), Judgment, I.C.J. Reports 2007, p. 659.

228. The Cyber Primer (2nd Edition) of the Ministry of Defence. Development, Concepts and Doctrine Centre website. UK`s Government website. 25 July 2016 (updated version). URL: https://www.gov.uk/government/publications/cyber-primer.

229. The EU`s Cybersecurity Strategy for the Digital Decade, Joint Communication to the European Parliament and the Council. JOIN/2020/18 final. 16.12.2020. URL: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.

230. The Federal Government of Germany, On the Application of International Law in Cyberspace Position Paper. March 2021. 17 p. URL:

https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf.

231. The future of discussions on ICTs and cyberspace at the UN. Submission by France, Egypt, Argentina, Canada, Colombia, Ecuador, Gabon, Georgia, Iceland, Japan, Lebanon, Montenegro, Morocco, Norway, Salvador, Singapore, the Republic of Korea, the Republic of Moldova, The Republic of North Macedonia, the United Kingdom, the EU and its member States (United Nations). 10 March 2020 (updated version). URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

232. The Netherlands, National Defence Cyber Strategy. December 2018. 18 p. URL: https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018.

233. The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21). February 12, 2013. URL: https://fas.org/irp/offdocs/ppd/ppd-21.pdf.

234. Thompson N. UN Secretary-General: US-China Tech Divide Could Cause More Havoc Than the Cold War. Wired website. 15 January 2020. URL: https://www.wired.com/story/un-secretary-general-antonio-guterres-internet-risks/.

235. Tikk E., Kaska K., Vihul L. International Cyber Incidents: Legal considerations. CCDCOE. 2010. 130 p. URL: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.

236. Timeline: North Korea and the Sony Pictures hack. December 18, 2014. URL: https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hacktimeline-interview-north-korea/20601645/.

237. TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case. March 18, 2016. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

238. Trail smelter case (United States, Canada). Reports of International Arbitral Awards. Volume III. 16 April 1938 and 11 March 1941. P. 1905-1982.

239. Tsagourias N. Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict & Security Law*. Vol. 17 No. 2. 2012. P. 229–244.

240. Tsagourias N., Farrell M. Cyber attribution: technical and legal approaches and challenges. *European Journal of International Law*. 2020. 24 p. URL: https://eprints.whiterose.ac.uk/159651/1/NTsagourias%20and%20MFarrell%20Cyber%20attribution%20EJIL%20March%202020%20final.pdf.

241. UK condemns Russia`s GRU over Georgia cyber-attacks. Press release Foreign & Commonwealth Office, National Cyber Security Centre, and The Rt Hon Dominic Raab MP. 20 February 2020. URL: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

242. Ukraine clashes signal end of truce. 5 January 2016. URL: https://www.euractiv.com/section/europe-s-east/news/ukraine-clashes-signal-end-of-truce/.

243. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023). 29 Aralık 2020. URL: https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf

244. Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences. Written by Lieutenant Colonel Jeffrey Biller and Michael Schmitt. EJIL: Talk! URL: https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/.

245. United Nations Charter. 24 October 1945. URL: https://www.un.org/en/about-us/un-charter/full-text.

246. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment, 1. C. J. Reports 1980, p. 3.

247. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act). Act of 2001. 132 p. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf.

248. Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units by CrowdStrike. December 22, 2016 (updated on March 23, 2017). 11 p.

249. Wagner D., Schweitzer B. The Growing Threat of Cyber-Attacks on Critical Infrastructure. 25.05.2017. URL: https://www.huffpost.com/entry/the-growing-threat-of-cyb_b_10114374.

250. Whaling in the Antarctic (Aust. v. Japan: N.Z. intervening), Judgment, 2014 I.C.J. 148.

251. Woltag C. Cyber Warfare. Max Planck Encyclopedia of Public International Law. 2015. 24 paras.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА,

в яких опубліковані основні наукові результати дисертації:

Статті у фахових наукових виданнях категорії «Б»:

1. Музика В.В. Проблема атрибуції кібератак проти об'єктів критичної інфраструктури та шляхи її вирішення в міжнародному праві. *Юридичний вісник*. № 4. 2020. С. 164-171. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/1985/2080.
2. Muzyka V. Analysis of cyber-attacks on Ukrainian power grid systems in the context of armed conflict in Donbas. *Constitutional State*. № 39. 2020. С. 78-85. URL: http://pd.onu.edu.ua/article/view/212983/214967.
3. Muzyka V. New wine in old bottles: applicability of the rules on attribution to cyberattacks committed against objects of critical infrastructure. *Law Review of Kyiv University of Law*. № 3. 2020. С. 388-391. URL: https://chasprava.com.ua/index.php/journal/article/view/419/400.

Стаття в періодичному науковому виданні держави, що входить до Організації економічного співробітництва та розвитку та/або Європейського Союзу:

4. Музика В.В. Кібератаки та міжнародне право: природа та аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі : колект. моногр. «Проблеми публічного та приватного права» / за заг. ред. Н. В. Мішиної. 2021. С. 309-342.

Розділ колективної монографії:

5. Музика В.В. Політика ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки. *Evropský politický a právní*

diskurz. 2021. Том 8 (1). С. 46-51. URL: https://eppd13.cz/wp-content/uploads/2021/2021-8-1/9.pdf.

Публікації, які засвідчують апробацію матеріалів дослідження:

6. Музика В.В. До питання про відсутність поняття «критична інфраструктура» в міжнародному праві. Матеріали міжнародної конференції : Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (21 травня 2021 року). Одеса, 2021. С. 359-362.
7. Музика В.В. Відповідальність держав за порушення обов'язку належної обачності (*due diligence*) в кіберпросторі. Право і суспільство: актуальні питання і перспективи розвитку : Матеріали V Міжнародної науково-практичної конференції Частина I (10 грудня 2020 року). Полтава, 2020. С. 107-110.
8. Muzyka V. Attribution of cyberattacks committed through cyber infrastructure of a third state and due diligence obligation. Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe : International Scientific Conference. Baltija Publishing. (20 November 2020). Riga, Latvia. 2020. P. 111-114.
9. Muzyka V. Human dimension of cyberoperations. Права людини – пріоритет сучасної держави : збір. матер. наук.-прак. конф. (м. Одеса, 10 грудня 2020 р.). Херсон : Видавничий дім «Гельветика», 2020. С. 179-182.
10. Muzyka Viktoriia V. Cyber-attacks attribution and EU collective cyber sanctions as a way to respond to cyber threats from outside the Union. Правова система України в умовах новітніх викликів міжнародного порядку : матеріали науково-практичної заочної конференції (м. Одеса, 20 травня 2020 р.) / за ред. М. Р. Аракеляна. Херсон : Видавничий дім «Гельветика», 2020. С. 63-65.
11. Muzyka Viktoriia V. Public Attribution of Cyber-Attacks: Toward a New Approach in International Law. Правове життя сучасної України : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Видавничий дім «Гельветика», 2020. Т. 3. С. 46-49.

Відомості про апробацію результатів дисертації

Дисертацію обговорено та виконано на кафедрі міжнародного та європейського права Національного університету «Одеська юридична академія».

Результати дисертаційного дослідження доповідалися на очних та заочних науково-практичних конференціях і семінарах, а саме: «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру» (м. Одеса, 21 травня 2021 року); «Право і суспільство: актуальні питання і перспективи розвитку» (м. Полтава, 10 грудня 2020 року); «Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe» (м. Рига, Латвія, 20 листопада 2020 року); «Права людини – пріоритет сучасної держави» (м. Одеса, 10 грудня 2020 р.); «Правова система України в умовах новітніх викликів міжнародного порядку» (м. Одеса, 20 травня 2020 р.); «Правове життя сучасної України» (м. Одеса, 15 травня 2020 р.).

У процесі здійснення дослідження здобувачка брала участь у фахових обговореннях, круглих столах, семінарах присвячених сучасним проблемам міжнародного права. Зокрема, 4-9 вересня 2019 року дисертантка взяла участь у 42-му Круглому столі з актуальних проблем МГП, присвяченому 70-літтю прийняття Женевських Конвенцій «Whither the human in armed conflict? IHL implications of new technology in warfare» (Сан Ремо, Італія). 26 червня 2020 року долучилась до міжкафедрального семінару, в якому брали участь здобувачі та науковців кафедри міжнародного та європейського права. 23 червня 2021 року результати дослідження представленні в ході семінару, присвяченого актуальним питанням міжнародного права, в рамках модулю Жана Моне, що проходив на базі Національного університету «Одеська юридична академія».

Додаток Б

«Затверджено»
Ректор
Міжнародного гуманітарного університету,
доктор юридичних наук, доцент,
Заслужений юрист України
_____ Громовенко К. В.
_____ 2021 року

АКТ
про впровадження наукових розробок дисертаційного дослідження на здобуття наукового ступеня доктора філософії Музики В.В. за темою: «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення» у навчальну та науково-дослідну діяльність Міжнародного гуманітарного університету

Акт складено комісією у складі:

Голова: директор Інституту права, економіки та міжнародних відносин, кандидат юридичних наук, доцент Тицька Я. О.

Члени комісії:

- завідувач кафедри міжнародного права та порівняльного правознавства, доктор юридичних наук, доцент Андрейченко С. С.;
- професор кафедри міжнародного права та порівняльного правознавства, кандидат юридичних наук, доцент Хендель Н. В.

Комісією було проведено роботу по визначенню фактичного впровадження результатів наукового дослідження Музики В.В. у навчальний процес та науково-дослідну діяльність Міжнародного гуманітарного університету.

Комісія розглянула наукові публікації Музики В.В.:

1. Музика В.В. Кібератаки та міжнародне право: природа та аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі : колект. моногр. «Проблеми публічного та приватного права» / за заг. ред. Н. В. Мішиної. 2021. С. 309-342.
2. Музика В.В. Політика ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки. *Evropský politický a právní diskurz*. 2021. Том 8 (1). С. 46-51. URL: https://eppd13.cz/wp-content/uploads/2021/2021-8-1/9.pdf.
3. Музика В.В. Проблема атрибуції кібератак проти об'єктів критичної інфраструктури та шляхи її вирішення в міжнародному праві.

Юридичний вісник. № 4. 2020. С. 164-171. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/1985/2080.

4. Muzyka V. Analysis of cyber-attacks on Ukrainian power grid systems in the context of armed conflict in Donbas. *Constitutional State*. № 39. 2020. С. 78-85. URL: http://pd.onu.edu.ua/article/view/212983/214967.
5. Muzyka V. New wine in old bottles: applicability of the rules on attribution to cyberattacks committed against objects of critical infrastructure. *Law Review of Kyiv University of Law*. № 3. 2020. С. 388-391. URL: https://chasprava.com.ua/index.php/journal/article/view/419/400.
6. Музика В.В. До питання про відсутність поняття «критична інфраструктура» в міжнародному праві. Матеріали міжнародної конференції : Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (21 травня 2021 року). Одеса, 2021. С. 359-362.
7. Музика В.В. Відповідальність держав за порушення обов'язку належної обачності (*due diligence*) в кіберпросторі. Право і суспільство: актуальні питання і перспективи розвитку : Матеріали V Міжнародної науково-практичної конференції Частина I (10 грудня 2020 року). Полтава, 2020. С. 107-110.
8. Muzyka V. Attribution of cyberattacks committed through cyber infrastructure of a third state and due diligence obligation. Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe : International Scientific Conference. Baltija Publishing. (20 November 2020). Riga, Latvia. 2020. P. 111-114.
9. Muzyka V. Human dimension of cyberoperations. Права людини – пріоритет сучасної держави : збір. матер. наук.-прак. конф. (м. Одеса, 10 грудня 2020 р.). Херсон : Видавничий дім «Гельветика», 2020. С. 179-182.
10. Muzyka Viktoriia V. Cyber-attacks attribution and EU collective cyber sanctions as a way to respond to cyber threats from outside the Union. Правова система України в умовах новітніх викликів міжнародного порядку : матеріали науково-практичної заочної конференції (м. Одеса, 20 травня 2020 р.) / за ред. М. Р. Аракеляна. Херсон : Видавничий дім «Гельветика», 2020. С. 63-65.
11. Muzyka Viktoriia V. Public Attribution of Cyber-Attacks: Toward a New Approach in International Law. Правове життя сучасної України : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Видавничий дім «Гельветика», 2020. Т. 3. С. 46-49.

За результатами проведеної роботи комісією встановлено, що пропозиції, сформульовані у наукових працях Музики В.В., впроваджено у навчальний процес та науково-дослідну діяльність Міжнародного гуманітарного університету, а висновки щодо особливостей атрибуції державі кібератак, використовуються під час проведення лекційних та семінарських занять з навчальних дисциплін «Міжнародне публічне право (основи теорії)» та «Міжнародне публічне право (основні галузі та інститути)».

Голова комісії:
директор Інституту права, економіки
та міжнародних відносин,
кандидат юридичних наук, доцент — Я. О. Тицька

Члени комісії:
завідувач кафедри міжнародного
права та порівняльного правознавства,
доктор юридичних наук, доцент — С. С. Андрейченко

професор кафедри міжнародного
права та порівняльного правознавства,
кандидат юридичних наук, доцент — Н. В. Хендель

Додаток В

«Затверджую»
Ректор Національного університету
«Одеська юридична академія»
_____ професор Загородній В.Є.
02 вересня 2021 року

АКТ

про впровадження результатів дисертаційного дослідження здобувачки кафедри міжнародного та європейського права Національного університету «Одеська юридична академія»

Музики Вікторії Василівни

на тему «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення»

Комісія у складі голови – першого проректора Національного університету «Одеська юридична академія», професора М. Р. Аракеляна, членів комісії: проректора з навчальної роботи Національного університету «Одеська юридична академія», професора Г. О. Ульянової, начальника навчально-методичного відділу Національного університету «Одеська юридична академія» Л. В. Кузнецової, завідувача кафедри міжнародного та європейського права, професора О. В. Бігняка, склали цей акт про те, що результати дисертаційного дослідження Музики В.В. на тему : «Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення» на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право» використовуються у навчальному процесі Національного університету «Одеська юридична академія» при викладанні навчальних дисциплін «Міжнародне право», «Міжнародне правосуддя», «Міжнародне публічне право сучасності», «Міжнародні відносини та світова політика», «Право вирішення міжнародних спорів», а

також у науково-дослідній роботі здобувачів вищої освіти, аспірантів, науковців.

Результати дослідження Музики В.В. відображені у науково-практичних і навчально-методичних матеріалах для здобувачів вищої освіти та аспірантів, де в якості джерел рекомендовані до використання у навчальному процесі наукових праць, основними з яких є наступні публікації:

1. Музика В.В. Кібератаки та міжнародне право: природа та аналіз *opinio juris* держав щодо застосування міжнародного права в кіберпросторі : колект. моногр. «Проблеми публічного та приватного права» / за заг. ред. Н. В. Мішиної. 2021. С. 309-342.
2. Музика В.В. Політика ЄС щодо забезпечення кіберстійкості критичної інфраструктури в контексті міжнародної безпеки. *Evropský politický a právní diskurz*. 2021. Том 8 (1). С. 46-51. URL: https://eppd13.cz/wp-content/uploads/2021/2021-8-1/9.pdf.
3. Музика В.В. Проблема атрибуції кібератак проти об'єктів критичної інфраструктури та шляхи її вирішення в міжнародному праві. *Юридичний вісник*. № 4. 2020. С. 164-171. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/1985/2080.
4. Muzyka V. Analysis of cyber-attacks on Ukrainian power grid systems in the context of armed conflict in Donbas. *Constitutional State*. № 39. 2020. С. 78-85. URL: http://pd.onu.edu.ua/article/view/212983/214967.
5. Muzyka V. New wine in old bottles: applicability of the rules on attribution to cyberattacks committed against objects of critical infrastructure. *Law Review of Kyiv University of Law*. № 3. 2020. С. 388-391. URL: https://chasprava.com.ua/index.php/journal/article/view/419/400.
6. Музика В.В. До питання про відсутність поняття «критична інфраструктура» в міжнародному праві. Матеріали міжнародної конференції : Наука та суспільне життя України в епоху глобальних

викликів людства у цифрову еру (21 травня 2021 року). Одеса, 2021. С. 359-362.

7. Музика В.В. Відповідальність держав за порушення обов'язку належної обачності (*due diligence*) в кіберпросторі. Право і суспільство: актуальні питання і перспективи розвитку : Матеріали V Міжнародної науково-практичної конференції Частина I (10 грудня 2020 року). Полтава, 2020. С. 107-110.
8. Muzyka V. Attribution of cyberattacks committed through cyber infrastructure of a third state and due diligence obligation. Relevant Trends of Scientific Research in the Countries of Central and Eastern Europe : International Scientific Conference. Baltija Publishing. (20 November 2020). Riga, Latvia. 2020. P. 111-114.
9. Muzyka V. Human dimension of cyberoperations. Права людини – пріоритет сучасної держави : збір. матер. наук.-прак. конф. (м. Одеса, 10 грудня 2020 р.). Херсон : Видавничий дім «Гельветика», 2020. С. 179-182.
10. Muzyka Viktoriia V. Cyber-attacks attribution and EU collective cyber sanctions as a way to respond to cyber threats from outside the Union. Правова система України в умовах новітніх викликів міжнародного порядку : матеріали науково-практичної заочної конференції (м. Одеса, 20 травня 2020 р.) / за ред. М. Р. Аракеляна. Херсон : Видавничий дім «Гельветика», 2020. С. 63-65.
11. Muzyka Viktoriia V. Public Attribution of Cyber-Attacks: Toward a New Approach in International Law. Правове життя сучасної України : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Видавничий дім «Гельветика», 2020. Т. 3. С. 46-49.

Використання зазначених результатів дозволило більш повно та ґрунтовно викласти матеріали вказаних навчальних дисциплін та надати здобувачам вищої освіти та аспірантам Національного університету «Одеська

юридична академія» можливість визначити процес здійснення атрибуції кібератак проти об'єктів критичної інфраструктури держави, основні проблеми, з якими стикається міжнародна спільнота в ході атрибуції кібератак та шляхи їх вирішення.

Голова комісії _____ М. Р. Аракелян

Члени комісії:

_____ Г.О. Ульянова

_____ Л.В. Кузнецова

_____ О. В. Бігняк