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 енергопостачання 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.