Резюме

Задорожний А.А. Частные космические полеты: правовое регулирование в США.

В статье представлен обзор и анализ законодательства США, регулирующего частные космические полеты, в частности, полеты с целью перевозки грузов и полеты в рамках космического туризма. Автором представлено хронологическое становление коммерциализации космоса, в котором четко прослеживается постепенный переход США от полного нежелания допущения частных космических полетов к признанию беспорной экономической целесообразности такой деятельности. Серьезный сдвиг в этой сфере происходит с 2015 г., когда было принято пять директив о космической политике, Национальную космическую стратегию и распоряжение об исследовании, добыча и использование космических ресурсов.

Ключевые слова: правовое регулирование, частные космические полеты, космический турист, перевозки грузов в космос, космическая политика, коммерциализация космоса.

Summary

Oleksandr Zadorozhny. Private space flights: legal regulation in the United States.

The emergence of demand for space travel, the emergence of commercial enterprises and travel agencies in the space industry, the development of vehicles designed exclusively for transporting tourists into space – all this suggests that space may soon turn from a scientific object into a common destination. Therefore, today the legal regulation of private space flights is a promising issue, given that there is no such legislation in Ukraine. We turn to the analysis of the legislation of the United States of America to assess what array of regulations we will have to master if we want to develop private space flights at home.

A private space flight is a space flight or development of space flight technology that is conducted and paid for by an entity other than a government agency. Depending on the purpose, private space flights are divided into flights for the purpose of transportation of cargoes, and flights within the framework of space tourism.

The article presents an overview and analysis of the legislation of the USA regulating private space flights, in particular, flights for the purpose of transportation of cargoes, and flights in the framework of space tourism. The author highlights a chronological formation of the commercialization of space, which clearly shows the gradual transition of the United States from a complete reluctance to allow private space flights to the recognition of the indisputable economic feasibility of such activities. A significant shift in this area has taken place since 2015, when five directives on space policy, the National Space Strategy and orders on the exploration, extraction and use of space resources were adopted.

The author analyzes the main sources of space law in the United States. It was found that mostly, the legislation does not keep up with innovations in the commercialization of space, thus, there is a situation when first comes a relationship (flight of a tourist or cargo into space), and then – the legislative regulation of such relations.

Key words: legal regulation, private space flights, space tourist, cargo transportation into space, space policy, space commercialization.

DOI: 10.36695/2219-5521.3.2020.72

УДК 341.211/214:316.276:(007:004.56)

V. MUZYKA

*Viktoriia Muzyka, Postgraduate student, Assistant of the Department of the National University "Odesa Law Academy"**

ORCID: 0000-0002-6907-0280

**NEW WINE IN OLD BOTTLES: APPLICABILITY OF THE RULES
ON ATTRIBUTION TO CYBERATTACKS COMMITTED AGAINST OBJECTS
OF CRITICAL INFRASTRUCTURE**

Identifying a problem. Today as never before, risks associated with cyberattacks and their kinetic consequences became more imminent. Private individuals or groups possesses enough resources and knowledge on how to attack objects of critical infrastructure. Some facts also evidence either direct or indirect involvement of states in planning and realization of malicious cyber activity. In particular, it was necessary for designers of the Stuxnet virus to know the network architecture of nuclear facility, as well as the process of nuclear enrichment.¹ The need for inclusion of individuals with highly specific knowledge and other political and technical indicators support a conclusion about states involvement. In the same vein, the context of cyberattacks against Ukrainian power grid systems in 2015 and 2016, as well as other data, also may testify to the nexus between hackers and a foreign state.²

COVID-19 pandemic has raised a serious concern about vulnerability of healthcare sector. On March 13, 2020, a major hospital in Brno (Czech Republic) experienced a cyberattack that forced hospital's administration to postpone urgent surgeries and reroute new patients in need of acute care. The hospital actually had been paralyzed as a

© V. Muzyka, 2020

* *Вікторія Василівна Музика, аспірантка, асистентка кафедри Національного університету «Одеська юридична академія»*

result of cyberattack, and its staff could not process coronavirus tests for several days. Other countries like France, Thailand, and the US also reported cyber incidents.³

All these examples show digital dependency of vulnerable critical infrastructure. And what is more important – the lack of appropriate attribution. This article does not tend to argue a state's involvement in all the cyberattacks launched on cyber infrastructure. However, it insists on the need of special assessment and scrutiny of attribution performed by an independent entity, especially if there are reasonable basis to presume a state's involvement.

Tallinn Manual experts have identified how rules on legal attribution should be applied to cyberspace. However, legal responsibility of states has never been established – even in situations of centralized and decentralized attribution of cyberattacks, which contain conclusions of a state's involvement – directly or through its proxy. It means that international community has to find a 'trigger' for making these rules on attribution 'live' and to put an end to impunity in cyberspace.

Analysis of recent researches and publications. Cyberattacks attribution is an issue actively discussed by legal scholars and experts of cyber and IT firms due to its twofold nature. Among law scholars, there are number of those whose works are dedicated to the issue of attribution of cyberattacks – M. Schmitt, M. Roscini, J. Richmond, P. Stockburger, D. Hollis, K. Ziolkowski, D. Alperovitch etc. Additionally, reports of private sector that contain propositions concerning creation of an independent international entity responsible for attribution were analyzed.

The main **goal** of this article is to identify the difficulties of application of the rules on attribution to cyberattacks and to emphasize upon the need to create a special entity for attribution.

Main text. Increasing number of cyberattacks against objects of critical infrastructure requires identification of those who stands behind and establishing responsibility to decrease cyberattacks' permanent growth. Due to the extensive work of Tallinn Manual experts, international community has received authoritative findings on application of law of international responsibility to cyberspace. This article focuses primarily on attacks committed by *de facto* state organs or state's proxies. The rationale behind this is their potential to destabilize an injured state, especially if launched during an armed conflict.

For cyberattack attribution, there is a need to identify: (a) computers and servers used for launching a particular cyberattack, (b) people that launched it or otherwise engaged in its commission, and (c) to establish a link between these people and a state proving that they may be treated as state agents.⁴ Indeed, this is not an easy task, but far from impossible. Private individuals or *de facto* state organs can assimilate hosts located in different states into a botnet and then use it for targeting. Thus, by making it almost impossible to identify computers and servers, or they may physically destroy computers. Furthermore, it is not always possible for an injured state with limited human and technical resources to perform such attribution and invoke international responsibility of another state. This is the main reason why public (political) attribution of states or decentralized technical attribution of private sector became so widespread.

Starting from 2007, there have been more than twenty high profile cyberattacks and respective attribution claims by governments, private sector and civil society. None of them have led to legal responsibility. On one hand, states have limited themselves by public attribution because, most probably, did not want to share information from their intelligence services (based on which they performed attribution). On other hand, it deems they do not start legal actions due to the temporal character of disruption or limited kinetic effects of cyberattacks.⁵

In any case, such public attribution based on human and technical intelligence, political and technical indicators, means states' readiness to resort to self-help measures if an illegal cyber operation continues or repeats. Experts of the Tallinn Manual have confirmed the right of states to apply unilateral self-help measures against another state after *ex ante* determination.⁶ But what if a cyberattack had such effects that it is impossible to accumulate evidence and make *ex ante* determination? Here, decentralized attribution by private sector could be a solution; however, technical data may be falsified and not always private sector have all necessary tools and information for correct attribution.⁷ For example, while the Novetta company led a coalition of technology industry partners, it expressed its ability to support the process of attribution, but not to perform it by oneself.⁸ Furthermore, they are not always willing to go further state-sponsorship conclusions owing to the lack of all the necessary political indicators and state intelligence data.

Highly-authoritative Tallinn Manual on the International Law Applicable to Cyber Operations clearly defines the rules, which should be used for the purpose of attribution. It does not make a step 'left' or 'right', but merely confirms the general rules of attribution enshrined in ARSIWA⁹ by adding comments in the light of specific context. According to the rules enshrined therein, a cyberattack will be attributed to a state if it is committed by its *de facto* or *de jure* organs, or by private individuals acting under its effective control. It is also possible to establish state responsibility when a state did nothing to terminate a cyberattack from its territory. Responsibility thus can arise not only from culpability, but also from negligence and the lack of due diligence.¹⁰

Rule 15 of Tallinn Manual reads as follows, "[c]yber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State". Since not all states possesses necessary knowledge and skills related to cyberspace, they may empower private individuals or firms to conduct cyberattacks. In this case, they will be equated with state organs.

Being empowered "to exercise elements of governmental functions" is a key precondition for making a conclusion on *de facto* state organ status. A particular cyber activity must be proved to be among elements of governmental functions. As a matter of fact, it is not clear what constitute "specified functions which are akin to those normally exercised by organs of the State".¹¹ While applying this standard, international tribunals frequently make a distinction between sovereign and commercial acts that is normally used in cases regarding state immunity.¹² In con-

text of cyberattacks, this standard causes some difficulties because it is not always obvious whether a particular activity fall within this concept.

The most important finding for the purpose of this article concerns a need to apply the effective control test elaborated by the ICJ in the Nicaragua case, which requires specific instructions concerning the commission of a particular act to be given by a State.¹³ Besides this test and equation with a state organ, there are also other possibilities for attribution; however, states are unwilling to acknowledge and adopt actions of private individuals or to recognize own wrongdoing.¹⁴

The impact of aforementioned Tallinn Manual is so high that it doubtfully will be ever changed. This may be justified by the possibility of misattribution and spoofing. Firstly, misattribution is possible when a cyberattack does not reach the threshold of the use of force and a state have to react immediately. For instance, to terminate an unlawful cyber intrusion states may apply retorsions or even countermeasures. Tallinn Manual states that “in the context of unilateral self-help measures [...] the State may be faced with a situation to which it may have to respond in an extremely short timeframe, without recourse to the full range of information that might be available in the non-cyber context”.¹⁵ In case when a state relies upon own capabilities, which are limited, and respond immediately, the risk of misattribution is substantial. It implies an important conclusion that cyberspace creates ‘cyber race’ and sometimes capabilities of non-governmental actors may match and even prevail upon clashing with cyber capabilities of states when they are sponsored or supported by another state. Therefore, for the purpose of cyber deterrence, legal attribution should be established, especially when human lives are the cost of such attacks.

Establishing a nexus between a particular state and its proxies is hardly achievable if an injured state does not have enough capabilities and resources. Thus, if we cannot change the rules for legal attribution, we can create a regime of attribution that would complement or substitute centralized governmental attribution. States should accept that state-centrism is no longer a key characteristic of a modern world order. Moreover, since governments are too reluctant, mostly unable to present sufficient evidence and afraid of politicization, the relevance of attribution has spurred a few proposals for creating an independent and centralized international entity. In particular, the Atlantic Council made a proposition to establish a Multilateral Cyber Attribution and Adjudication Council with the power to provide “a consensus attribution of illegal cyber campaigns by states and a formal process for adjudicating associated interstate disputes”.¹⁶ Microsoft suggested a special body “consist[ing] of technical experts from across governments, the private sector, academia, and civil society”, which would be created by virtue of Atomic Energy Agency example.¹⁷ Finally, RAND Corporation researchers made a quite radical proposition to create a Global Cyber Attribution Consortium, which fully excludes states membership. They believed it would be more appropriate to include technical experts, academia and cyberspace policy experts.¹⁸

Conclusion. When it comes to cyberattacks attribution, one should accept the need to change ‘old bottles’ for ‘new wine’. The importance of cybersecurity and IT companies has drastically increased since they are able to make technical attribution faster than governmental agencies and produce correct results that are extremely important to avoid misattribution and retaliation. But it does not mean states should be excluded from this process. In contrast, there is a clear need for well-balanced cooperation and data-sharing due to the need to assess and take into consideration both technical and political indicators. This will solve not only a problem of technical attribution, but a wide range of political problems. As a matter of fact, sometimes serious challenges emerge at the political level for states, while private actors are more independent and impartial. States thus should engage in cooperation with cyber-related companies to keep peace and prevent serious violations of human rights, otherwise all the world will be in danger and responsibility for cyberattacks against vulnerable infrastructure will be impossible.

¹ Charney S., English E., Kleiner A. From Articulation to Implementation: Enabling Progress on Cybersecurity Norms (June 2016). P. 10. URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVMc8>

² CrashOverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. By Joe Slowik, Dragos Inc. URL: <https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>; 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

³ Mačák K., Rodenhäuser T., Gisel L. Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections? In: *Humanitarian Law & Policy*. 2020. URL: <https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/>

⁴ Roscini M. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*. Volume 50. Symposium Issue 2. 2020. P. 240; Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge: Cambridge University Press*. 2017. P. 98-103.

⁵ Tsagourias N. Cyber attribution: technical and legal approaches and challenges. *University of Sheffield*. 2018. URL: <https://sites.tufts.edu/cilg/files/2018/09/attributiondraftsm.pdf>.

⁶ Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge: Cambridge University Press*. 2017. P. 81.

⁷ Stateless Attribution: Toward International Accountability in Cyberspace, C. 16.

⁸ This process of private-sector firms indicating an inability to perform an attribution investigation has happened in the past. (stateless attribution... p. 30)

⁹ Responsibility of States for internationally wrongful acts : resolution / adopted by the General Assembly, 8 January 2008, A/RES/62/61. URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

¹⁰ Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge: Cambridge University Press*. 2017. P. 86.

- ¹¹ Report of the ILC, 26th Session, ILC Yearbook 1974, Vol. II(1). P. 281. URL: https://legal.un.org/ilc/publications/yearbooks/english/ilc_1974_v2_p1.pdf
- ¹² Emilio Agustín Maffezini v. The Kingdom of Spain, ICSID Case No. ARB/97/7. URL: <https://www.italaw.com/cases/641> ; Fleming DutyFree Shop Private Limited v. Poland, UNCITRAL, Award of 12 Aug. 2016. URL: <https://www.italaw.com/cases/4471>
- ¹³ Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14. Para. 86.
- ¹⁴ Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. 2017. P. 282.
- ¹⁵ Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. 2017. P. 81.
- ¹⁶ Hearley J., Mallery J., Jordan K. Confidence-Building Measures: a multistakeholder approach for stability and peace. *Atlantic Council*. 2014. P. 10. URL: https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyber_space.pdf
- ¹⁷ Charney S., English E., Kleiner A. From Articulation to Implementation: Enabling Progress on Cybersecurity Norms (June 2016). P. 11. URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVMc8>
- ¹⁸ Davis J., Boudreaux D., Welburn J. Stateless Attribution: Toward International Accountability in Cyberspace. 2017. P. 29. URL: https://www.rand.org/pubs/research_reports/RR2081.html

Резюме

Музыка В.В. Застосування правил атрибуції щодо кібератак проти об'єктів критичної інфраструктури.

У статті аналізується застосування норм щодо атрибуції державі поведінки *de facto* органів, а також дій приватних індивідів на підставі тесту ефективного контролю. Акцентується увага на постійному збільшенні кількості кібератак проти об'єктів критичної інфраструктури та відсутності необхідного реагування – атрибуції та, як наслідок, притягнення держав до відповідальності, коли їх роль в здійсненні таких атак встановлена шляхом централізованого та децентралізованого аналізу кібератаки.

В статті також робиться висновок про необхідність створення незалежного міжнародного органу, який би займався питаннями встановлення атрибуції, беручи на себе всі ризики пов'язані з помилковою атрибуцією.

Ключові слова: атрибуція кібератак; відповідальність держав; правила атрибуції; присвоєння поведінки державі; критична інфраструктура.

Резюме

Музыка В.В. Применение правил атрибуции к кибератакам против объектов критической инфраструктуры.

В статье анализируется применение правил касательно присвоения поведения *de facto* органов государству, а также действий частных индивидов на основании теста эффективного контроля. Акцентируется внимание на постоянном увеличении количества кибератак против объектов критической инфраструктуры и отсутствии необходимого реагирования – атрибуции и, как следствие, привлечения государств к ответственности, когда их роль в осуществлении таких атак установлена путем централизованного и децентрализованного анализа.

В статье также делается вывод о необходимости создания независимого международного органа, который бы занимался вопросами атрибуции, принимая на себя риски, связанные с ошибочной атрибуцией.

Ключевые слова: атрибуция кибератак; ответственность государств; правила атрибуции; присвоение поведения государству; критическая инфраструктура.

Summary

Viktoriia Muzyka. New wine in old bottles: applicability of the rules on attribution to cyberattacks committed against objects of critical infrastructure.

Growing number of cyberattacks committed by states or with their support testifies to the need of legal attribution for the purpose of international responsibility. Tallin Manual that comprises authoritative findings on how the attribution rules should be applied raises a serious concern about the practical possibility to establish attribution. The main reason for this concern may be found in the nature of cyberspace that is characterized by anonymity, spoofing and targeting from the territory of other states etc.

The rules of Tallinn Manual reiterated the provisions of ARSIWA and do not evidence about the existence of *lex specialis* for cyberattacks attribution. Pursuant to them, states are responsible for actions of their *de facto* and *de jure* organs empowered to exercise the elements of governmental functions, private actors within their effective control or for the violation of due diligence obligations.

This article argues that there is no necessity to change the rules on attribution, but, due to limited human and technical resources of most states, a special body for technical attribution should be created. The author analyses the different proposals that foresees a membership of states or fully excludes it. Notwithstanding a model, which may be chosen, there should be a variety of technical expertise and limitations of states ability to impact a decision concerning the choice of a case and its outcomes.

Key words: cyberattack attribution; responsibility of states; attribution rules; critical infrastructure.