Отже, у резолюції 74/274 міститься заклик для створення глобального доступу до ліків, вакцин і медичного обладнання, необхідного для боротьби з COVID-19, і зазначається необхідність створення Міжорганізаційної цільової групи, до складу якої увійде і ВООЗ.

Ключові слова: Генеральна Асамблея ООН, ВООЗ, резолюція, COVID-19, пандемія.
Ключевые слова: Генеральная Ассамблея ООН, ВОЗ, резолюция, COVID-19, пандемия.
Key words: UN General Assembly, WHO, resolution, COVID-19, pandemic.

MUZYKA VIKTORIIA VASYLIVNA

National University "Odesa Law Academy",
PhD student at the Department of International and European Law

PUBLIC ATTRIBUTION OF CYBER-ATTACKS: TOWARDS A NEW APPROACH IN INTERNATIONAL LAW

Widespread dependence and reliance upon technological advancements make governments, militaries and ordinary people more vulnerable in face of cyber-attacks. Such advancements bring a lot of benefits; however a coin has two sides and technologies are susceptible to cyber-attacks launched by non-state actors. The latter are not homogenous and may include individual hackers, groups, criminal organizations engaged in cyber crime, legal entities (commercial IT services, software companies), cyber terrorists and others [10, p. 95], whose interests may overlap with states' ones.

It is clear that actions of cyber armies or other state actors are easily attributable to respective states under the law of state responsibility [10, p. 87]. However, to avoid responsibility some states act through proxies by sponsoring and supporting the unlawful activity of non-state actors. In this way states can bolster own interests and hide their identity. That is the main reason why attribution of cyber-attacks committed by non-state actors merit a special consideration.

In the 2013 Report on Developments in the Field of Information and Telecommunications in the Context of International Security, the UN Group of Governmental Experts recognized the applicability of international law, mainly IHRL and IHL, to cyberspace, as well as the need to establish responsibility in case of its violation [1].However, international community has faced a new challenge because it cannot present hard evidence tracing a specific cyber-attack to a particular state. At the same time, many states show their ability and willingness to adapt to changing environment by publicly attributing cyber-attacks.

Under customary international law, conduct of non-state actors will be attributable to the State "only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation" [6, p. 47]. Thus, actions of non-state cyber actors are attributable to a state if the requirements of effective control test are satisfied. In its landmark

judgment in Nicaraguacase the International Court of Justice has elaborated on the issue whether a State "exercise [s] such a degree of control in all fields as to justify treating [private actors] as acting on its behalf" [8, para. 86]. In particular, the effective control test recognizes that specific instructions concerning the commission of a specific act have to be given by the State – the issuing of specific orders by the State, or its direction of each individual operation [8, para. 86].

In fact, the reality is such that it is hardly possible (if possible) for an injured state to attribute a cyber-attack by virtue of the effective control test. Nevertheless, many states have publicly attributed cyber attacks by relying upon the multitude of various factors, such as motivation or strategic interests, technical indicators, level of proximity between state and non-state actors and geographic location.

Since 2014, a number of cyber-attacks have been publicly attributed to particular states without discussing and applying the effective control test. In particular, a cyber-attack against Sony Pictures Entertainment was publicly attributed to North Korea due to the technical analysis of the data deletion malware that was previously used by North Korea. As a result, similarities in specific lines of code, encryption algorithms, data deletion methods and compromised networks have been revealed. FBI also observed "significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack". Furthermore, they found similarities between the tools used during cyber-attacks against the Sony and South Korean banks and media outlets, which was launched allegedly by North Korea [4].

Motivation of the "Guardians of Peace", hackers that took responsibility for the attack [4],should be taken into account. The attack allegedly was motivated by the release of "The Interview" movie about fictional assassination of Kim Jong-un. One can reasonably imply that motivation of hackers fully collude with the interests of North Korea – to prevent release of the film. This conclusion flows from messages received by the Sony and the letter of North Korea's ambassador to the UN, Ja Song-nam. In particular, Mr. Ja Song-nam called this film "the most blatant act of terrorism and war" that "will absolutely not be tolerated" by adding "If the US administration allows and defends the showing of the film, a merciless counter-measure will be taken". "It is their [DPRK's people] firm determination to mercilessly destroy anyone who dares hurt or attack the supreme leadership of the country even a bit", he said [7]. Meanwhile, the hackers sent a threatening message that "the world will be full of fear" and mentioned the repetition of 9/11 attack [13]. The Sony and all the cinemas thus cancelled the film screening [11].

Interestingly, on 22 December 2014, three days after publication of FBI's report, North Korea also became a victim of cyber-attack. It had experienced an Internet outage that lasted for more than 10 hours. And in a few days later, the U.S. President signed an order imposing increased sanctions on North

Korea [13]. Therefore, one can reasonable imply the involvement of both states in this cross-attacks.

Another example that merits a special consideration concerns NotPetya. The great change in public attribution has been achieved on 15 February 2018 when two states – the US and United Kingdom – officially attributed NotPetya malware, which encrypted the data without possibility to decrypt it, to Russia. It was for the first time more than one stated traced a cyber-attack to a particular state because of international consequences NotPetya had caused. Importantly, the United Kingdom was the very first state to declare that "the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017." [5]. On the same day, the United States of America published a statement on the White House website. The US also attribute NotPetya attack to the Russian military by adding that it was "the most destructive and costly cyber-attack in history. [...] It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences." [12]

Since NotPetya affected not only Ukraine but other countries in Europe, Asia, and the Americas, other states – Australia, Canada, New Zealand have joined the US and UK by publicly attributing NotPetya to Russia after own verification. In particular, the Australian Government came to a conclusion that "Russian state sponsored actors were responsible for the incident" due to investigation of the Australian intelligence agencies, and consultation with the USA and UK [9]. And finally, Canada publicly stated that "actors in Russia were responsible for developing NotPetya" and condemned indiscriminate attacks on "critical financial, energy, government, and infrastructure sectors around the world in June 2017" [2].

Importantly, in 2016 hackers showed their ability to interfere with politics. In the run-up to the 2016 election in the USA, the US Democratic National Committee received numerous phishing emails. As a result, hackers got an access to about 60,000 emails in John Podesta's private Gmail account, who was the chairman of Hillary Clinton's campaign. This cyber attack thus constitutes an interference with the election process and allegedly impacted the outcomes of the 2016 elections.

In its investigation report, a public cybersecurity company, CrowdStrike has discovered two adversaries on the network –"cozy bear" and "fancy bear". The company also found out that these two adversaries were linked to the Russian state. The rationale for such a conclusion was the "extensive political and economic espionage for the benefit of the government of the Russian Federation" and that adversaries "are believed to be closely linked to the Russian government's powerful and highly capable intelligence services [GRU, Main Intelligence Service]" [3].

Therefore, current practice of public attribution of cyber-attacks calls for new standards applicable to cyberspace. Otherwise, it would be impossible to apply effective control test and invoke state responsibility in cases where it is impossible to trace a particular cyber-attack with high level of confidence (probability). For this, such factors as strategic interests, technical indicators,

level of proximity between state and non-state actors and geographic location should be taken into consideration.

References:

1. 2013 report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.
2. CSE Statement on the NotPetya Malware [Electronic resource]: Mode of access: https://www.cse-cst.gc.ca/en/media/2018-02-15.
3. D.Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike Blog* (June 15, 2016) [Electronic resource] – Mode of access: https://www.crowdstrike.com/blog/bears-midst-intrusion-democraticnational-committee/.
4. FBI, "Update on Sony Investigation", Press Release (Dec. 19, 2014) [Electronic resource] – Mode of access: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
5. Foreign Office Minister condemns Russia for NotPetya attacks (15.02.2018) [Electronic resource] – Mode of access: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.
6. ILC, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, in UN Doc A/56/10 (2001).
7. 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 [Electronic resource] – Mode of access: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/934.
8. Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986.
9. Minister for Law Enforcement and Cyber Security Hon. Angus Taylor MP Australian Government attribution of the 'NotPetya' cyber incident to Russia (16.02.2018) [Electronic resource] – Mode of access: https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-attributes-notpetya-malware-to-russia.pdf
10. Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations.
11. Sony Pictures hackers invoke 9/11 while threatening theaters that show 'The Interview' [Electronic resource] – Mode of access: https://www.washingtonpost.com/news/the-switch/wp/2014/12/16/sony-pictures-hackers-invoke-911-while-threatening-theaters-that-show-the-interview/
12. Statement from the Press Secretary, February 15, 2018: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.
13. Timeline: North Korea and the Sony Pictures hack, available at: https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

Ключові слова: кібератаки, атрибуція, публічна атрибуція, відповідальність держав.

Ключевые слова: кибератаки, атрибуция, публичная атрибуция, ответственность государств.

Key words: cyber-attacks, attribution, public attribution, state responsibility.