ТРИБУНА МОЛОДОГО ВЧЕНОГО

УДК 341.1/8
DOI https://doi.org/10.32837/yuv.v0i4.1985

В. Музика,
аспірантка кафедри міжнародного та європейського права
Національного університету «Одеська юридична академія»

ПРОБЛЕМА АТРИБУЦІЙ КІБЕРАТАК ПРОТИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ШЛЯХИ ЇЇ ВИРІШЕННЯ В МІЖНАРОДНОМУ ПРАВІ

Кількість кібератак проти об'єктів критичної інфраструктури держав постійно зростає, як і загроза фізичного знищення таких об'єктів. Ті ресурси, якими володіють хакери та складність кібероперацій свідчать про безпосередню або опосередковану участь держави в плануванні та здійсненні атак, а також використанні технічних та наукових ресурсів держави. Незважаючи на це, наразі практично не можливо притягнути державу до відповідальності, оскільки ця проблема виходить за межі юридичної площини та, окрім правової атрибуції, вимагає здійснення технічної атрибуції кібератак.

Мета статті – розглянути можливість створення допоміжного органу, який займався би питаннями атрибуції для подальшого притягнення держав до міжнародної відповідальності.

Притягнення держав до відповідальності вимагає встановлення двох елементів міжнародно-протиправного діяння – порушення зобов'язання та його присвоєння державі [10, ст. 2]. Що стосується першого елемента, то залежно від контексту та наслідків таких кібератак будуть діяти норми міжнародного гуманітарного права чи міжнародного права прав людини. Кібератаки проти об'єктів критичної інфраструктури держави також можуть призвести до порушення принципу заборони погрози або застосування сили і досягти рівня збройної агресії. Отже, проблем з юридичними підставами відповідальності на практиці не виникає, що не можна сказати щодо фактичних підстав.

Враховуючи делікатність та серйозність заяв щодо порушення державою міжнародних зобов'язань, Міжнародний Суд ООН встановив досить високий тест для притягнення держав до відповідальності. Відповідно до тесту ефективного контролю, який був розроблений у справі щодо військової та напіввійськової діяльності в Нікарагуа, для цілей відповідальності необхідна наявність ефективного контролю над приватними особами [6, п. 86]. У контексті кібератак це означає те, що встановлення відповідальності держав не можливе, коли держава здійснює загальний контроль над приватними особами (хакерами, групами хакерів, IT-компаніями тощо) шляхом планування, фінансування або підтримання кібератак. У такому випадку можна встановити лише порушення принципу невтручання у внутрішні справи держави, але ніяк не порушення заборони погрози чи використання сили, норм міжнародного гуманітарного права чи міжнародного права прав людини. Тому

виходить, що міжнародне право практично безсильне, якщо держава самостійно не визнає свою причетність до кібератаки, або якщо не буде доведена відсутність необхідної турботи з боку останньої.

Для атрибуції кібератак також потрібно спочатку встановити комп'ютери та сервери, які застосовувалися під час їх здійснення, ідентифікувати осіб, які мають безпосередній стосунок до цих атак, а потім довести, що ці особи діяли від імені конкретної держави, щоб атрибутувати їхні дії державі [8, с. 240; 9, с. 98–103]. Таке завдання очевидно виходить за межі юридичної площини та вимагає оцінки технічних індикаторів.

Пов'язані з правовою та технічною атрибуцією труднощі змусили юристів-міжнародників серйозно задуматись над ефективними шляхами їх подолання в міжнародному праві. З одного боку, були намагання сформувати новий підхід на підставі публічної атрибуції кібератак. Але така практика носить швидше політичний характер, ніж правовий [7, с. 47–48], що не дозволяє констатувати формування *lex specialis*. Відсутній елемент *opinion juris* [11], тому про формування норм звичаєвого права, відмінного між загальноприйнятих правил притягнення до відповідальності (на підставі тесту ефективного контролю), також неможливо говорити. З іншого боку, політичні індикатори, вироблені в межах публічної атрибуції кібератак, все ж потребують урахування для отримання достовірних висновків [7, с. 46–47].

Приватні IT-компанії та компанії, що займаються питаннями кібербезпеки, показали можливість здійснення технічної атрибуції та встановлення відповідальних осіб, а іноді – і держав, що за ними стоять. Так, наприклад, у 2013 році компанія Мандіант опублікувала безпрецедентний звіт, що викривав діяльність китайської кібергрупи APT1 (*Advanced Persistent Threat 1*), яка займалась тривалим кібершпигунством. Звіт готувався протягом 7-ми років та враховував «активність» проти 141-ї організації, які були скомпрометовані APT1 та діяли в 20-ти основних галузях промисловості. Серед іншого, звіт 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 [5].

Цікаво, що до цього, у 2010 році, Мандіант опублікував свій перший звіт щодо APT. 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 й успішна, але не єдина). Тоді Мандіант виразив позицію щодо того, що діяльність цієї кібергрупи могла санкціонуватися Урядом Китаю, визнаючи, що на той момент не уявлялось за можливе встановити рівень причетності. Звіт 2013 року, навпаки, містить докази причетності та 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) у своїй місії, можливостях та ресурсах аналогічний APT1. Підрозділ 61398 PLA також розташований у точно тій самій зоні, з якої починається активність APT1» [5, с. 2].

Такий детальний звіт, що був представлений на оцінку широкому

загалу, породив так званий «ефект Мандіанту»: відтепер компанії, що займаються питаннями кібербезпеки, переконані в тому, що задля всезагального визнання здійсненого аналізу та підвищення репутації їхні 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 та наполягає на широкомасштабних кампаніях проти урядів та компаній, що базуються в різних країнах світу [2]. Цим самим CrowdStrike демонструє системність проблеми та існування низки небезпечних кібергруп.

Крім того, як видається з аналізу публічної та технічної атрибуції кібератак 2014–2018 років, 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 й не можуть контролювати в межах власного суверенітету, не хочуть визнавати за приватним сектором. Але тут також важливим є той факт, що децентралізована атрибуція з боку недержавних акторів та їхня готовність обмінюватися інформацією і спільно взаємодіяти з державою та її агентами зводить до мінімуму ризик помилкової атрибуції.

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

Сценарій, за яким і держави, і недержавні кіберактори проводять технічну атрибуцію окремо один від одного, має своє плюси, але більш ефективно об'єднати зусилля з урахуванням переваг, якими кожна зі сторін володіє. Перевага, яка є у держав у разі атрибуції, полягає в тому, що вона прекрасно обізнана з власним історичним, соціальним, політичним та економічним контекстом, в межах якого були здійснені кібератаки проти її критичної інфраструктури. Що ж до приватних компаній, то в їх розпорядженні часто містяться відомості ряду компаній, що стали жертвами кібератак у різних країнах. Фактично це і є тією причиною, яка дозволяє приватному сектору здійснити технічну атрибуцію в короткі строки. Але й ці строки можуть скоротитися, якщо буде проходити періодичний обмін інформацією з державою, що підтверджує доцільність об'єднання зусиль державних та недержавних акторів.

Співпраця може стати тим важелем, який запустить правову атрибуцію кібератак для цілей притягнення держав до міжнародної відповідальності. Експерти Microsoft пропонують досить оптимальний варіант міжнародного механізму, який би займався питаннями атрибуції. Зокрема, пропонується створити організацію, яка би включала не тільки державних, а й приватних технічних експертів, науковців, представників громадянського суспільства, що зможуть оцінити тактику та прийоми, які використовують державні кіберактори, та інші індикатори, що демонструють причетність держави до кібератаки [1, с. 11].

Така централізована атрибуція за участі всіх зацікавлених сторін сприяла б не тільки здійсненню атрибуції, а й досягненню стандарту доказування у випадку подання міждержавного спору. Завдяки атрибуції

з високим рівнем підтвердження державам-жертвам кібероперацій вдасться притягнути державу-правопорушницю до міжнародної відповідальності, якщо остання має безпосереднє відношення до кібератак. Разом із тим для міжнародної спільноти це шанс зменшити зростаючу кількість кібератак та почати реагувати на порушення норм міжнародного права, зокрема в ситуаціях, коли кібероперації проти об'єктів критичної інфраструктури досягають порогу використання сили.

Важливо, що, пропонуючи такий міжнародний механізм, експерти Microsoft надихнулися прикладом Міжнародної агенції з атомної енергії (МАГАТЕ). І тут складно не погодитися, оскільки цей механізм добре відомий своєю технічною експертизою. До Ради керуючих МАГАТЕ входять 35 країн-членів, які змінюються на ротаційній основі. Процес прийняття Радою рішень, як правило, визначається консенсусом, що також є бажаним для майбутнього механізму з питань атрибуції кібероперацій. До основних напрямів діяльності МАГАТЕ відноситься здійснення ядерних перевірок (зокрема, верифікаційної та моніторингової діяльності в Ірані з ціллю виконання резолюції РБ ООН 2231 від 2015 року), виробництво медичних радіоізотопів та радіаційних технологій у межах ядерного застосування, технології ядерного паливного циклу і матеріалів тощо. Отже, діяльність організації неможлива без залучення технічних експертів, які проводять інспекції та розробки. МАГАТЕ – це саме той приклад, який може бути використаний як модель для створення механізму, що здійснюватиме технічну атрибуцію кібератак. Однозначно позитивним буде створення виключно технічного механізму, який не прийматиме політичних рішень, а лише встановлюватиме факти.

Створення такого механізму необхідне і з тієї причини, що між приватними фірмами існує розрив у тих методах та інструментах, які вони використовують для здійснення технічної атрибуції. Так, наприклад, Лабораторія Касперського (Kaspersky Lab) зазначила, що аналіз, проведений BAE та Anomali щодо зв'язку між «групою Лазарус» (Lazarus Group) і Північною Кореєю та їх причетністю до пограбування Центрального банку республіки Бангладеш, 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 [4; 3, с. 20].

На увагу заслуговує пропозиція, що виключає участь агентів держави. При цьому складно повірити в можливість створення такого механізму, який виключав би роль держави в процесі здійснення технічної атрибуції. По-перше, із 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 із тим пропозиції створення «бездержавного» міжнародного механізму для здійснення технічної атрибуції все ж існують.

Зокрема, Корпорація РЕНД (RAND) запропонувала створення Глобального консорціуму з кібератрибуції [3]. 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 питань кіберпростору, юристів-науковців та експертів з міжнародних відносин різних наукових та дослідницьких організацій. У консорціум повинно входити від 20-ти до 40-ка 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 технічної атрибуції в межах створеного міжнародного механізму. По-перше, держави здійснюють технічну атрибуцію на підставі доказів та матеріалів розвідки, які вони не готові публічно оприлюднити. Тому виникають обґрунтовані запитання щодо достовірності та повноти доказів, які неможливо перевірити. По-друге, держави переслідують свої політичні інтереси. Представники РЕНД припускають можливий тиск із боку державних акторів задля отримання бажаного висновку від Консорціуму [3, с. 19]. І це дійсно можливо, якщо враховуватимуться не лише технічні індикатори, а й політичні індикатори та інформація із різних джерел. Спиратись виключно на технічні індикатори стратегічно невірно, оскільки технічні індикатори можуть бути підроблені [3, с. 16]. По-третє, у випадку членства в Консорціумі держави зможуть впливати на вибір справ для розслідування. Тобто можливий варіант, коли кібероперації за участю конкретних держав будуть відсіюватися.

Незважаючи на відмову від постійної участі держав у діяльності Консорціуму, РЕНД не виключає можливість співпраці з державами. Останні зможуть надавати інформацію, яка може допомогти в розслідуванні та встановленні відповідальних. Разом із тим на Консорціум не покладатиметься обов'язок щодо використання цієї інформації, особливо в ситуаціях, коли виникають сумніви щодо достовірності переданої інформації.

Щодо можливого впливу на організації-учасниці, які, попри свою незалежність від держав, створені відповідно до національного законодавства та діють на території держави, то наявність значної кількості технічних експертиз і процедур розслідування дозволить мінімізувати можливий вплив [3, 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 технічної атрибуції. Історія знає приклади, коли приватні організації були змушені призупинити процес атрибуції через потребу в даних урядової розвідки. Так, наприклад, компанія Novetta під час підготовки звіту щодо операції «Блокбастер» виразила бажання підтримати роботу інших акторів, зазначивши відсутність ресурсів для самостійної технічної атрибуції. Це пояснюється тим, що відомі хакерські групи, які підтримуються державами, зазвичай не одразу попадають у поле зору приватних компаній. Крім того, нападники не є ізольованою та єдиною групою, а масштаб їхньої діяльності досить значний і може охоплювати значну кількість країн та сфер.

У своїх звітах приватний сектор визнає необхідність оцінки політичних індикаторів, і це зумовлено не лише можливістю фальсифікації технічних даних. З одного боку, встановлення ряду держав, які мають політичні, економічні чи інші мотиви в здійсненні кібератаки, може пришвидшити процес технічної атрибуції. Адже зазвичай ціль атаки та знання, які необхідні для її здійснення, свідчать про участь держав, а не випадкові атаки хакерів заради розваги [3, с. 12]. Наприклад, розробникам вірусу Stuxnet потрібне було не лише глибоке розуміння мережевої архітектури чутливого ядерного об'єкта, але і знання щодо досить складного процесу збагачення урану. Отже, йдеться не лише про

збір розвідувальних даних, а також про залучення фахівців із глибоко спеціалізованими знаннями в конкретній галузі [1, 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, вибрана ціль та використані знання можна розглядати як додаткові підтвердження причетності російських державних акторів.

Звичайно, поодинці технічні та політичні індикатори не завжди спроможні надати відповідь на питання, хто стоїть за конкретною кібероперацією. Технічних індикаторів не завжди достатньо, а політичні іноді досить розмиті (наприклад, у ситуації коли потенційні мотиви є у декількох, ніяк не пов'язаних держав або коли мотиви взагалі не зрозумілі). Отже, співпраця між державами та приватним сектором, а також участь держави в діяльності механізму, який займатиметься питаннями атрибуції, є необхідною умовою отримання достовірних результатів атрибуції.

У статті досліджено проблему атрибуції кібератак у міжнародному праві. Встановлено, що неможливість присвоєння державі поведінки приватних осіб зумовлена високим порогом тесту ефективного контролю. Отже, аналізується пропозиція щодо створення міжнародного механізму за прикладом МАГАТЕ, який би займався питаннями технічної атрибуції для подальшого встановлення правової атрибуції і відповідальності в межах міжнародного права. Лише такі висновки незалежного міжнародного механізму зможуть задовольнити вимоги ефективного контролю та поводження з приватними особами як з агентами держави. Це зумовлено тим, що в більшості звітів щодо технічної атрибуції наявні докази використання державної інфраструктури, а також взаємодії хакерів та хакерських груп з державними органами.

У статті також розглянуті запропоновані моделі цього міжнародного механізму. З одного боку, пропонується такий міжнародний механізм, який би здійснював технічну атрибуцію на підставі взаємодії державних та недержавних акторів, з іншого боку, приватний сектор пропонує створити механізм, який би передбачав виключно консультації та отримання інформації від держав. Тому виключається членство держав, а інформація, яка надана ними, не буде обов'язковою для врахування у випадку сумнівів щодо достовірності даних. Ця пропозиція зумовлена тим, що, на думку приватного сектору, держави спробують втрутитися в процес технічної атрибуції через свої політичні мотиви або намагатимуться досягти рішення щодо відсіювання розслідування кібератаки, до якої вони або їхні союзники причетні.

Автор доходить висновку про доцільність створення міжнародного механізму, який не передбачає повне виключення представників держави. Це пояснюється тим, що не лише технічні, а й політичні індикатори повинні бути враховані. Такий підхід знаходить підтримку серед усіх зацікавлених сторін через те, що технічні дані можуть бути скомпрометовані. Крім того, в розпорядженні державних агентів зазвичай знаходиться важлива інформація щодо конкретної кібератаки та контексту, в якому вона була здійснена. Не менш важливо й те, що міжнародна спільнота навряд чи погодиться на створення міжнародного механізму з представників приватного сектору, висновки якого потенційно

можуть стати доказами у встановленні відповідальності держав. Як наслідок, вирішення проблеми зі встановленням атрибуції буде відкладено на невизначений час.

Ключові слова: атрибуція кібератак, відповідальність держав, правова атрибуція, технічна атрибуція, міжнародний механізм, що відповідальний за технічну атрибуцію.

Muzyka V. The problem of attribution of cyberattacks against objects of critical infrastructure and ways of its solving

The article examines the problem of legal attribution of cyberattacks in international law. The main challenge associated with this problem is a high threshold for invocation of state responsibility that is based on the effective control test. Therefore, the author supports the idea to create an independent international mechanism responsible for technical attribution of cyberattacks. For this purpose, International Atomic Energy Agency, which deals with technical issues and expertise, may be used as a model. Technical outcomes thus could solve the existing problem of impunity for cyberattacks against objects of critical infrastructure that plays indispensable functions. It is argued that technical attribution and its outcomes are essential prerequisite for legal attribution and the possibility to treat private actors as de facto agents of state. This is due to the fact that most reports on technical attribution contain evidence of the use of state infrastructure, as well as evidence about the nexus between hackers or hacker groups and governmental agencies.

The article also contains the analysis of proposed models of this international mechanism. First, there is a proposition to create a mechanism able to carry out technical attribution based on the cooperation of state and non-state actors. Second, the private sector proposes to create a mechanism that would foresee only consultations with states and information-sharing. Therefore, the membership of the states is excluded, and the information provided by states will not be necessary considered in case doubts exists concerning the reliability of data. This proposal is made due to the fact that, according to the private sector, states will try to interfere in the process of technical attribution in light of their political motives or reach a decision to exclude a particular situation in which they or their allies are involved.

The author concludes that a new mechanism should not exclude the membership of state representatives. The rationale behind this conclusion is that not only technical but also political indicators must merit considerations. And this approach is supported by both states and private sector, otherwise – there is a high risk of technical indicators to be falsified. Furthermore, governments are usually in possession of important information about the specific cyberattack committed against its critical infrastructure and the context in which it was carried out. There is also a low probability that international community will agree to create an international mechanism consisting of representatives of private sector, whose conclusions could potentially be used in the process of establishing state responsibility. Therefore, most probably, resolving the attribution issue will be delayed.

Key words: attribution of cyberattacks, state responsibility, legal attribution, technical attribution, international mechanism responsible for technical attribution.

Література

1. Charney S., English E., Kleiner A. From Articulation to Implementation: Enabling Progress on Cybersecurity Norms. 2016. URL: https://query.prod.cms.

rt.microsoft.com/cms/api/am/binary/REVmc8

2. CrowdStrike Intelligence Report «Putter Panda». URL: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

3. Stateless Attribution: Toward International Accountability in Cyberspace / J. Davis et al. Santa Monica, CA: RAND Corporation, 2017. URL: https://www.rand.org/pubs/research_reports/RR2081.html.

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

5. Mandiant`s Report «APT1 Exposing One of China's Cyber Espionage Units». URL: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

6. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14 (June 27). URL: https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

7. Muzyka 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.

8. Roscini M. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. Texas International Law Journal. Volume 50. Symposium Issue 2. P. 234–273.

9. Schmitt M. Tallinn Manual on the International Law applicable to cyber warfare. 2013. 283 p.

10. UN General Assembly, 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

11. Vðljataga A. Tracing opinio juris in National Cyber Security Strategy Documents. NATO CCD COE. URL: https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf