DOI: https://doi.org/10.18524/2411–2054.2021.43.241005
УДК 341.1/.8

О. О. Сурілова, докт. юрид. наук, професор
Національний університет «Одеська юридична академія»
Кафедра міжнародного та європейського права
Фонтанська дорога, 23, Одеса, 65009, Україна
e-mail: elenasurilova@ukr.net
ORCID: https://orcid.org/0000–0001–7071–6678

ПУБЛІЧНА АТРИБУЦІЯ КІБЕРАТАК ДЕРЖАВАМИ-ЧЛЕНАМИ ЄС ТА ЗАСТОСУВАННЯ КІБЕРСАНКЦІЙ СОЮЗОМ ЩОДО КІБЕРАТАК, ЯКІ СТАНОВЛЯТЬ ЗАГРОЗУ ЄС ТА ЙОГО ЧЛЕНАМ

В статті досліджується питання публічної атрибуції кібератак державами-членами ЄС та ефективність прийнятих «інструментів кібердипломатії» в рамках спільного дипломатичного реагування ЄС на шкідливу кібердіяльність. Особливий акцент робиться на оцінці ефективності кіберсанкцій, які мають вибірковий характер та запроваджуються на рівні Союзу щодо обмеженого кола кібератак, які становлять загрозу для ЄС чи його членів.

Також проаналізовано перспективи запровадження секторальних санкцій, стримуючий та попереджуючий ефект яких вищий, ніж вибіркових санкцій проти фізичних та юридичних осіб. Нарешті, в статті обгрунтовується можливість використання звітів про атрибуцію, підготованих приватним сектором, з ціллю включення осіб в санкційний список, якщо атрибуція держав-членів базується на даних розвідки, які вони не бажають оприлюднювати.

Ключові слова: кібератаки, атрибуція, публічна атрибуція кібератак, інструменти кібердипломатії, кіберсанкції.

Постановка проблеми. Кібернетичний простір (кіберпростір)[1], що є середовищем здійснення кібероперацій[2], відкрив для держав нові можливості досягнення своїх політичних та стратегічних цілей. Державні органи чи проксі, до послуг яких все частіше звертається держава, вдаються як до серйозних кібератак проти об'єктів критичної інфраструктури, так і не гребують промисловим кібершпигунством для підвищення конкурентоздатності вітчизняних компаній. Проте, попри намагання міжнародної спільноти підвищити рівень відповідальної поведінки в кіберпросторі і підтвердження того, що існуюче міжнародне право застосовується до кібероперацій, кількість зловмисних кібератак з кожним роком лише збільшується.

Безкарність в кіберпросторі підштовхнула Європейський Союз та його держав-членів до максимізації зусиль, що спрямовані на ідентифікацію і встановлення відповідальності тих, хто стоїть за кіберопераціями. В результаті Європейський Союз прийшов до прийняття Рамок для спільного дипломатичного реагування ЄС на шкідливу кібердіяльність, що наразі представляють унікальний підхід до реагування на кібератаки.

Мета статті. Встановити місце публічної атрибуції кібератак в діяльності держав-членів ЄС та ефективність ЄС в питаннях боротьби зі шкідливими кібератаками шляхом застосування кіберсанкцій.

---

[1] Кібероперація є збірним поняттям, що об'єднує кібератаки та кіберексплуатацію. Відмінність між ними полягає в тому, що кібератаки передбачають втручання в функціонування комп'ютерів та мереж. На відміну від кібератак, кіберексплуатація є своєрідним моніторингом (спостереженням) за комп'ютером чи мережею. На практиці кіберексплуатація часто переростає в кібератаку, оскільки успішна кібератака не можлива без належного спостереження та виявлення вразливостей комп'ютера чи мережі.

[2] Загально прийнятим серед держав є розуміння відсутності обов'язку розкривати інформацію, на підставі якої кібератака була публічно атрибутована конкретній державі. Така інформація потенційно може бути розкрита на вимогу суду, який розглядає спір між державами та здійснює юридичну атрибуцію. Водночас при здійсненні публічної атрибуції держави часто пояснюють в своїх звітах чи односторонніх деклараціях, які технічні «відбитки» та політичні індикатори свідчать про причетність певної держави.

Виклад основного матеріалу. За останнє десятиліття держави продемонстрували свою готовність публічно атрибутувати найбільш серйозні кібератаки конкретним державам, які за ними стояли. Публічну атрибуцію кібератак слід відрізняти від юридичної атрибуції, яка є елементом міжнародно-протиправного діяння. Така атрибуція є вираженням суверенної волі держав, що здійснюється шляхом прийняття односторонніх декларацій постраждалою державою чи групою держав і сигналізує про готовність протистояти шкідливій діяльності в кіберпросторі [6, с. 7]. Вона здійснюється, в першу чергу, на підставі аналізу політичних індикаторів та є важливою передумовою для здійснення юридичної атрибуції з ціллю притягнення держави до відповідальності за кібератаку.

Публічна атрибуція кібератак – це завжди реалізація суверенного права держави, тому держави (як постраждалі, так і треті), можуть публічно присвоїти кібератаку іншій державі або утриматись від таких дій. Така атрибуція здійснюється на підставі аналізу даних власної розвідки, оцінки політичних індикаторів, а також результатів роботи CERT-EU та INTCEN, які на рівні Союзу сприяють виробленню спільного розуміння[1]. Враховуючи політичне забарвлення цього виду атрибуції і нерівні людські та технічні можливості, державам-членам ЄС досить складно прийти до спільного рішення. Внаслідок цього їх підходи до публічної атрибуції досить різні: одні займають активну позицію та навіть здійснюють політичну атрибуцію разом з державами, які не є членами ЄС (Нідерланди, Німеччина, Великобританія до виходу з ЄС), інші – утримуються від політичного присвоєння кібератак державам (Франція). Водночас в новій Стратегії кібербезпеки ЄС зазначається необхідність для ЄС та держав-членів підвищити свою здатність здійснювати атрибуцію шкідливої кібердіяльності [12, п. 2.3], що є особливо актуальним для держав-членів ЄС з обмеженими людськими та технічними ресурсами.

Основні причини, що зумовили виникнення таких полярних підходів до атрибуції, можна прослідкувати в офіційних позиціях найбільш яскравих представників цих двох «блоків», а саме – Нідерландів та Франції, що містяться в національних кіберстратегіях, воєнних доктринах та односторонніх деклараціях. В Стратегії кіберзахисту Нідерландів, яка відводить центральне місце публічній атрибуції кібератак, зазначається наступне: «Активна політика публічної атрибуції сприяє стримуванню та робить Нідерланди менш привабливими як об'єкт кібератак. Державний актор, відповідальність якого була встановлена (публічно), дасть іншу оцінку, ніж нападник, який може діяти в повній анонімності. Таким чином, Нідерланди роблять свій внесок у боротьбу з безкарністю у цифровій сфері» [7, с. 2].

Франція, навпаки, тривалий час зберігає свій неповторний підхід в утримані від публічної атрибуції кібератак. Офіційна позиція Франції полягає в тому, що нездійснення публічної атрибуції переслідує процес «деескалації» та ведення діалогу із державою, яка стоїть за кібератакою. На думку французького уряду, атрибуція, про яку повідомляється у двосторонньому порядку через дипломатичні канали, є найбільш ефективною [5]. Разом з тим, заява керівника Французького агентства з кібербезпеки від 21 липня 2021 року щодо втручання в діяльність ряду французьких суб'єктів з боку групи APT31 [11], за якою, як вважається, стоїть Уряд Китаю, сприймається як досить близька до атрибуції [14][2]. Відтак, досить стримана позиція Франції щодо публічної атрибуції, яка є результатом прийнятої в 2008 році Кіберстратегії, зазнала трансформації після прийняття нової стратегії в 2018 році.

---

[1] Загально прийнятим серед держав є розуміння відсутності обов'язку розкривати інформацію, на підставі якої кібератака була публічно атрибутована конкретній державі. Така інформація потенційно може бути розкрита на вимогу суду, який розглядає спір між державами та здійснює юридичну атрибуцію. Водночас при здійсненні публічної атрибуції держави часто пояснюють в своїх звітах чи односторонніх деклараціях, які технічні «відбитки» та політичні індикатори свідчать про причетність певної держави.

[2] Заява керівника Французького агентства з кібербезпеки послідувала через два дні після того, як Великобританія публічно атрибутувала ряд кібератак APT31 та Китаю. Відтак, багатьма сприймається як публічна атрибуція кібератак Китаю.

Індивідуальне та колективне[1] здійснення публічної атрибуції сприяло тому, що у 2017 році ЄС прийняв Рамки для спільного дипломатичного реагування ЄС на шкідливу кібердіяльність, які досить часто називають «інструментами кібердипломатії». Цим ЄС продемонстрував свою готовність бути одним із ключових гравців в кіберпросторі. Інструменти кібердипломатії не передбачають здійснення спільної публічної атрибуції на рівні Союзу, але фактично процедура включення осіб в список тих, хто підпадає під санкції, є досить близькою до публічної атрибуції. Такий висновок зумовлений тим, що особи, які потрапили в санкційний список, мають пряме або опосередковане відношення до держави. Так, наприклад, під обмежувальні заходи потрапили співробітники Головного управління Генерального штабу Збройних сил Російської Федерації (ГУ/ГРУ) та Головне управління в цілому як юридична особа; фізичні та юридичні особи, що стоять за ATP10 та Lazaruz Group (останні пов'язують з урядами Китаю та Північної Кореї відповідно). Такий підхід є своєрідним повідомленням для держави, яке, хоч і замовчує її назву, сигналізує про можливості Європейського Союзу зі встановлення виконавців та готовність боротися з неправомірною поведінкою в кіберпросторі. Важливо також і те, що держави сприймають це повідомлення як таке, що адресовано особисто їм, а не особам, які потрапили під обмежувальні заходи. Так, наприклад, із Заяви Міністерства закордонних справ РФ «Про чергові нелегітимні обмежувальні заходи Європейського союзу проти Росії» від 21 лютого 2021 року, що була зроблена в силу підготовки «нових протиправних односторонніх обмежень щодо російських громадян» [15], випливає висновок про те, наскільки «особисто» Російська Федерація сприймає вибіркові санкції ЄС проти фізичних та юридичних осіб.

Всі кіберсанкції, або обмежувальні заходи[2], до яких може вдаватись Європейський Союз, мають автономний вибірковий характер. У Рішенні Ради 2019/797 та Регламенті Ради (ЄС) 2019/796 перелічено шість видів кібератак проти держав-членів ЄС, які можуть призвести до введення санкцій, ціллю яких є «стримування та реагування на кібератаки зі значним ефектом, що становлять зовнішню загрозу для Союзу або його держав-членів» [2; 3]. До них відносяться напади на критичну інфраструктуру; послуги, необхідні для підтримання основних соціальних та економічних заходів; важливі державні функції; зберігання або обробку секретної інформації; урядові групи реагування на надзвичайні ситуації; напади, здійснені проти установ, органів, офісів ЄС, агентств, делегацій в третіх країнах, а також місій та операції в рамках спільної політики безпеки та оборони. Введення та застосування санкцій, які мають «більше зубів», ніж декларації та дипломатичні заяви, є беззаперечним успіхом Європейського Союзу. Ваги таким санкціям додає і той факт, що вони можуть бути предметом судового перегляду з боку Суду ЄС.

У рішенні по справі Каді, яке стосувалося санкцій, накладених Організацією Об'єднаних Націй, Суд ЄС прийшов до ряду висновків, які є релевантними у випадку прийняття кіберсанкцій щодо конкретних фізичних чи юридичних осіб. Суд підкреслив, що включення до санкційного списку має ґрунтуватися на надійній фактичній основі, а наявна інформація та докази мають підтверджувати необхідність застосування до особи обмежувальних заходів [8, пар. 41]. Отже, всі фізичні та юридичні особи, які потрапили у список в силу того, що були ідентифіковані як виконавці кібератак, можуть звернутися до Суду ЄС за повним переглядом такого рішення. Така можливість ще більше переводить боротьбу з кібератаками в юридичне поле, що не можливо у випадку з односторонніми заявами про публічну атрибуцію – держава, якій публічно атрибутується кібератака, як правило, намагається спростувати її шляхом надання заяви у відповідь.

У випадку з кібератаками увагу заслуговує і можливість передачі конфіденційної інформації Суду при перегляді справи, оскільки саме він приймає рішення щодо того, чи існують виправданні підстави для нерозголошення. Звичайно Суд може попросити відповідні агентства ЄС чи конкретних держав-членів надати детальні комп'ютерно-

[1] На практиці колективна атрибуція здійснюється державами-партнерами та, як вважається, має більше ваги, оскільки ряд держав майже одночасно публічно атрибутує кібератаку відповідальній державі, що зводить до мінімуму сумніви щодо можливої помилковості їх висновків.

[2] В Європейському Союзі поняття «санкції» та «обмежувальні заходи» є взаємозамінними.

технічні звіти, що послужили підставою для застосування обмежувальних заходів до конкретної особи. Але включення особи до санкційного списку неможливо уявити без даних розвідки, які держави із зрозумілих причин не хочуть розголошувати. Крім того, у випадку загальної доступності інформації про кібератаку існує досить високий і виправданий ризик того, що інші кіберактори її використають для здійснення більш масштабних кібератак. Така практика уже мала місце після розголошення деталей про кібератаку «WannaCry», внаслідок якої у 2017 році постраждало чимало установ, а також приватних осіб. Того ж року зовсім інша група використала більш агресивну версію цієї зловмисної програми для атаки державних установ по всьому світі («NotPetya») [13].

Тому для держав-членів ЄС та Європейського Союзу в цілому важливою є співпраця з приватним сектором, який відіграє критично важливу роль в технічній та публічній атрибуції зловмисних кібератак. З урахуванням людських та технічних можливостей, які є у приватних компаній, держава має шанс вчасно отримати від них інформацію для прийняття стратегічно важливих рішень. Адже кібератаки – це не проблема держав, це спільна проблема, з якою стикаються як державні, так і недержавні кіберактори. Приватні компанії були одними з перших, хто публічно атрибутував ряд кібератак відповідальним урядам. Зокрема, компанія Symantec однією з перших оприлюднила інформацію про шкідливе програмне забезпечення Stuxnet, яке нанесло серйозної шкоди іранській ядерній установці у 2010 році, а Лабораторія Касперського ідентифікувала інструменти, методи та процедури властиві хакерській команді «Equation Group», яка, як вважається, пов'язана з федеральним агентством США [10, с. 71].

Більшість комп'ютерно-технічних звітів приватних компаній, що займаються питаннями кібербезпеки, є публічними та не містять конфіденційної інформації (або така інформація передається постраждалому уряду окремо), що може бути використана для повторних кібератак проти існуючих вразливостей. Вважаємо, що докази, які в них містяться та які пов'язують кібератаку з конкретною фізичною чи юридичною особою, можуть слугувати в якості підстави для включення таких осіб в список тих, хто потрапляє під кіберсанкції ЄС.

Наразі санкції застосовуються до восьми фізичних осіб та чотирьох юридичних осіб і включають замороження активів та заборону на в'їзд [4]. Такі санкції мають нормативну перевагу в силу того, що не ставлять за ціль покарати все населення відповідальної держави за дії невеликої урядової меншини [10, с. 9]. Але їх вибірковий характер вірогідно також зменшує їх ефективність. Європейський Союз не є єдиним актором, що вдається до застосування вибіркових санкцій. До обмежувальних заходів вибіркового характеру також не раз вдавалась Організація Об'єднаних Націй, і дослідження їх ефективності свідчить про досить обмежені можливості вибіркових санкцій в плані примусу, стримування та сигналізування [1, с. 236]. Водночас вибіркові санкції в Європейському Союзі є компромісним та попереджувальним заходом, що дозволяє ЄС оперативно реагувати на політичні виклики та події, що суперечать його цілям та цінностям.

Вважається, що ефективність вибіркових санкцій можна підвищити за рахунок секторальних (галузевих) санкцій, які ЄС, до прикладу, застосував проти Білорусі після примусової посадки літака Ryanair у Мінську. В цьому випадку під обмежувальні заходи потрапили не лише фізичні та юридичні особи, що пов'язані з режимом президента, а й цілі сектори (нафта, калій, банківська справа, тютюн та технології спостереження) [16]. У випадку з кібератаками такий підхід був би виправданим в силу їх наслідків та попередження повторення.

Оцінка кібератак свідчить про їх високий деструктивний та руйнівний потенціал, особливо коли вони спрямовані проти об'єктів критичної інфраструктури. Так, наприклад, лише данська компанія Maersk, що є найбільшим оператором контейнерних перевезень у світі, втратила близько 300 млн. доларів в результаті кібератаки «NotPetya». Загалом дана кібероперація обійшлась організаціям 1,2 млрд. доларів сукупного квартального та річного доходу [9]. Операція «Cloud Hopper» проти інформаційних систем ТНК на шести континентах також призвела до значних економічних втрат [2]. Але кібератаки –

це не лише про економічні втрати, а й про можливі серйозні наслідки для нормального функціонування держави та добробуту суспільства. В ході кібератаки «Спалах на Сонці» в 2021 році, яка є наразі наймасштабнішою в історії США, серед іншого, постраждало Міністерство енергетики, яке відповідає за управління ядерною зброєю, Міністерства фінансів та торгівлі. Потенційні наслідки, які могли б мати місце при повній реалізації можливостей, могли мати серйозний негативний вплив на життя та здоров'я людей. Відтак, впровадження секторальних санкцій в рамках існуючого режиму було б виправданим та розумним, але Рамки для спільного дипломатичного реагування ЄС на шкідливу кібердіяльність передбачають виключно обмежувальні заходи проти фізичних та юридичних осіб.

По-перше, як видається, Європейський Союз на даний момент не готовий здійснювати публічну атрибуцію кібератак, без якої не можливо уявити застосування секторальних санкцій. Причини вірогідно криються у зовнішній політиці держав-членів ЄС та Союзу в цілому. Будучи одним із ключових акторів, ЄС намагається зберігати свою позицію та уникати напруги у відносинах з третіми державами, яка може перерости у відкрите протистояння.

По-друге, Європейський Союз досить обережний та скрупульозний в питаннях застосування секторальних санкцій, оскільки побічні, не цілеспрямовані наслідки таких санкцій матимуть вплив на цивільне населення. До прикладу, робоча група радників з міжнародних відносин (RELEX) Ради ЄС детально обговорювала застосування секторальних санкцій проти Російської Федерації, що було реакцією на анексію Криму в 2014 році. Група була стурбована реакцією Росії у випадку непропорційності санкцій ЄС, зокрема ескалації перебігу конфлікту в Україні та скорочення поставок нафти і газу до держав-членів ЄС [10, с. 88]. Беручи до уваги той факт, що більшість кібератак здійснюються угрупуваннями висококваліфікованих хакерів, що діють під контролем або є державними органами урядів Російської Федерації, Китаю, Північної Кореї, США, Туреччини тощо, Європейський Союз, принаймні наразі, не готовий йти на такий крок з ряду економічних та політичних причин.

Висновки і пропозиції. Безкарність в кіберпросторі підштовхнула Європейський Союз до виведення глобальних та регіональних зусиль із забезпечення відповідальної поведінки в кіберпросторі на якісно новий рівень. Європейський Союз не здійснює публічну атрибуцію кібератак, але процедура включення фізичних та юридичних осіб до санкційного списку фактично є мовчазним жестом в сторону відповідальної держави.

ЄС має великий досвід у розробці та застосуванні санкцій і наразі налічує більше санкційних режимів, ніж США чи ООН. Прийняті в 2019 році кіберсанкції проти фізичних та юридичних осіб стали потенційно цінним інструментом, який можна використати для примусу, покарання або сигналізації виконавцям кібератак про можливі наслідки їхніх дій, але їх ефективність можна підвищити лише за рахунок застосування секторальних санкцій. Інакше, відповідальна держава майже не відчуває наслідки таких обмежувальних заходів.

Список використаних джерел:

1. Biersteker, T., Tourinho, M., & Eckert, S. (2016). The effectiveness of United Nations targeted sanctions. In T. Biersteker, S. Eckert, & M. Tourinho (Eds.), *Targeted Sanctions: The Impacts and Effectiveness of United Nations Action*, pp. 220–247.
2. Council of the European Union, «Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyberattacks threatening the Union or its Member States». *Official Journal of the European Union*. L 129I, May 17, 2019, p. 13–19.
3. Council of the European Union, «Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States». *Official Journal of the European Union*. L 129I, May 17, 2019. pp. 1–12.
4. Cyber-attacks: Council prolongs framework for sanctions for another year. *Council of the EU official website*. Press release dated on 17 May 2021. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/.

5. Desforges A., Géry A. France Doesn't Do Public Attribution of Cyberattacks. But It Gets Close. *Lawfare website*. September 3, 2021. URL: https://www.lawfareblog.com/france-doesnt-do-public-attribution-cyberattacks-it-gets-close#.
6. Florian J Egloff, Public attribution of cyber intrusions. *Journal of Cybersecurity*. Volume 6. Issue 1. 2020. pp. 1–12. URL: https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454#207409750.
7. Florian J. Egloff & Max Smeets (2021): Publicly attributing cyber attacks: a framework, *Journal of Strategic Studies*. pp. 1–32. URL: https://www.tandfonline.com/doi/pdf/10.1080/01402390.2021.1895117?needAccess=true.
8. Kadi II, *European Commission and others v Kadi*, Judgment, Case C-584/10 P, Case C-593/10 P, Case C-595/10 P, ILEC031 (CJEU2013), 18th July 2013, Court of Justice of the European Union (Grand Chamber). URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8416907.
9. O`Connor F. NotPetya still roils company's finances, costing organizations $1.2 billion in revenue. *Cybereason website*. November 9, 2017. URL: https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue.
10. Pawlak P., Biersteker T. Gurdian of the Galaxy: EU cyber sanctions and norms in cyberspace. Chaillot Paper / 155. 2019. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf.
11. Poupard G. (21 July, 2021). ANSSI is currently handling a large intrusion campaign impacting numerous French entities. Attacks are still ongoing and are led by an intrusion set publicly referred as APT31 [Post]. *LinkedIn*. URL: https://www.linkedin.com/feed/update/urn: li: activity:6823528088136105984/.
12. The EU's Cybersecurity Strategy for the Digital Decade, European Commission, Joint Communication to the European Parliament and the Council, dated 16.10.2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018.
13. Three ways the 'NotPetya' cyberattack is more complex than WannaCry. *The Conversation: Academic rigour, journalistic flair.* June 30, 2017. URL: https://theconversation.com/three-ways-the-notpetya-cyberattack-is-more-complex-than-wannacry-80266.
14. UK and allies hold Chinese state responsible for a pervasive pattern of hacking. *UK`s Government official website*. URL: https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking.
15. Заявление МИД России от 22.02.21 «Об очередных нелегитимных ограничительных мерах Европейского союза против России». Официальный сайт Министерства иностранных дел РФ. URL: https://www.mid.ru/web/guest/evropejskij-souz-es/-/asset_publisher/6OiYovt2s4Yc/content/id/4590496.
16. ЄС затвердив секторальні санкції проти Білорусі. *Європейська правда.* 24.06.2021. URL: https://www.eurointegration.com.ua/news/2021/06/24/7124790/.

References:

1. Biersteker, T., Tourinho, M., & Eckert, S. (2016). The effectiveness of United Nations targeted sanctions. In T. Biersteker, S. Eckert, & M. Tourinho (Eds.), *Targeted Sanctions: The Impacts and Effectiveness of United Nations Action*, pp. 220–247.
2. Council of the European Union, «Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyberattacks threatening the Union or its Member States». *Official Journal of the European Union*. L 129I, May 17, 2019, p. 13–19.
3. Council of the European Union, «Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States». *Official Journal of the European Union*. L 129I, May 17, 2019. pp. 1–12.
4. Cyber-attacks: Council prolongs framework for sanctions for another year. *Council of the EU official website*. Press release dated on 17 May 2021. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/.
5. Desforges A., Géry A. France Doesn't Do Public Attribution of Cyberattacks. But It Gets Close. *Lawfare website*. September 3, 2021. URL: https://www.lawfareblog.com/france-doesnt-do-public-attribution-cyberattacks-it-gets-close#.
6. Florian J Egloff, Public attribution of cyber intrusions. *Journal of Cybersecurity*. Volume 6. Issue 1. 2020. pp. 1–12. URL: https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454#207409750.
7. Florian J. Egloff & Max Smeets (2021): Publicly attributing cyber attacks: a framework, *Journal of Strategic Studies*. pp. 1–32. URL: https://www.tandfonline.com/doi/pdf/10.1080/01402390.2021.1895117?needAccess=true.
8. Kadi II, *European Commission and others v Kadi*, Judgment, Case C-584/10 P, Case C-593/10 P, Case C-595/10 P, ILEC031 (CJEU2013), 18th July 2013, Court of Justice of the European Union (Grand Chamber). URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8416907.
9. O`Connor F. NotPetya still roils company's finances, costing organizations $1.2 billion in revenue. *Cybereason website*. November 9, 2017. URL: https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue.

10. Pawlak P., Biersteker T. Gurdian of the Galaxy: EU cyber sanctions and norms in cyberspace. Chaillot Paper / 155. 2019. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf.
11. Poupard G. (21 July, 2021). ANSSI is currently handling a large intrusion campaign impacting numerous French entities. Attacks are still ongoing and are led by an intrusion set publicly referred as APT31 [Post]. *LinkedIn*. URL: https://www.linkedin.com/feed/update/urn: li: activity:6823528088136105984/.
12. The EU's Cybersecurity Strategy for the Digital Decade, European Commission, Joint Communication to the European Parliament and the Council, dated 16.10.2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018.
13. Three ways the 'NotPetya' cyberattack is more complex than WannaCry. *The Conversation: Academic rigour, journalistic flair.* June 30, 2017. URL: https://theconversation.com/three-ways-the-notpetya-cyberattack-is-more-complex-than-wannacry-80266.
14. UK and allies hold Chinese state responsible for a pervasive pattern of hacking. *UK`s Government official website*. URL: https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking.
15. Statement of the Russian Foreign Ministry dated 22.02.21 "On the next illegitimate restrictive measures of the European Union against Russia." Official site of the Ministry of Foreign Affairs of the Russian Federation. URL: https://www.mid.ru/web/guest/evropejskij-souz-es/-/asset_publisher/6OiYovt2s4Yc/content/id/4590496 [in Russian].
16. The EU has approved sectoral sanctions against Belarus. European truth. 06.24.2021. URL: https://www.eurointegration.com.ua/news/2021/06/24/7124790/ [in Russian].

Стаття надійшла 11.09.2021 р.

Е. А. Сурилова, докт. юрид. наук, профессор
Национальный университет «Одесская юридическая академия»
Кафедра международного и европейского права
Фонтанская дорога, 23, Одесса, 65009, Украина
e-mail: elenasurilova@ukr.net
ORCID: https://orcid.org/0000–0001–7071–6678

ПУБЛИЧНАЯ АТРИБУЦИЯ КИБЕРАТАК ГОСУДАРСТВАМИ-ЧЛЕНАМИ ЕС И ПРИМЕНЕНИЕ КИБЕРСАНКЦИЙ СОЮЗОМ В ОТНОШЕНИИ КИБЕРАТАК, КОТОРЫЕ ПРЕДСТАВЛЯЮТ УГРОЗУ ДЛЯ ЕС И ЕГО ЧЛЕНОВ

Резюме

В статье исследуется вопрос публичной атрибуции кибератак в пределах ЕС и эффективность принятых «инструментов кибердипломатии» в рамках совместного дипломатического реагирования ЕС на вредную кибердеятельность. Особый акцент делается на оценке эффективности киберсанкций, которые имеют избирательный характер и вводятся на уровне Союза в отношении ограниченного круга кибератак, которые представляют угрозу для ЕС или его членов.

Также проанализированы перспективы внедрения секторальных санкций, сдерживающий и предупреждающий эффект которых выше, чем выборочных санкций против физических и юридических лиц. Наконец, в статье обосновывается возможность использования отчетов об атрибуции, подготовленных частным сектором, с целью включения лиц в санкционный список, если атрибуция государств-членов базируется на данных разведки, которые они не желают обнародовать.

Ключевые слова: кибератаки, атрибуция, публичная атрибуция кибератак, инструменты кибердипломатии, киберсанкции.

O. O. Surilova, Doctor of Law, Professor
National University «Odesa Law Academy»
the Department of International and European Law
Fontanska Doroga, 23, Odesa, 65009, Ukraine
e-mail: elenasurilova@ukr.net
ORCID: https://orcid.org/0000–0001–7071–6678

PUBLIC ATTRIBUTION OF CYBERATACS BY EU MEMBER STATES AND THE APPLICATION OF CYBERSANCTIONS BY THE UNION TO CYBERATTACKS THREATENING THE UNION OR ITS MEMBER STATES

Summary

The article examines the issue of public attribution of cyberattacks threatening the European Union or its Member States, and effectiveness of the adopted «cyber diplomacy toolbox» within the Framework for a joint EU diplomatic response to malicious cyber activities. Since public attribution of cyberattacks is a sovereign political decision, which differs from legal attribution for the purpose of invoking state responsibility under Articles on State Responsibility for Internationally Wrongful Acts, author defines the rationale behind decisions to attribute or not to attribute cyberattacks to a particular state by examples of the Netherlands and France. While the Netherlands insist on deterrent effect of public attribution, France believes in the effectiveness of attribution provided to the allege wrongdoer by diplomatic channels.

In the article, the effectiveness of cybersanctions implemented at Union level against a limited range of cyberattacks threatening the Union or its Member States was also under assessment. Article concludes that imposition of targeted sanctions in conjunction with sectoral sanctions will increase sanctions` purposes to coerce, constrain, and to signal. However, nowadays only targeted sanctions against individuals and legal entities are foreseen by the EU`s decision. At the same time, this fact does not exclude the possible application of sectoral sanctions against the most serious cyberattacks against EU` or its member states` infrastructure.

Finally, the article justifies the possibility of using attribution reports prepared by the private sector to include individuals in the sanctions list if the attribution of Member States is based on intelligence that they do not wish to disclose. Moreover, malicious cyberoperations affect not only states`, but also private sector`s, interests. Private IT and cybersecurity companies thus have a chance to prove their ability to produce detailed and reliable reports on attribution of cyberoperations. Author is convinced both centralized (governmental) and decentralized (private) attribution of cyberattacks is necessary for correctness of findings.

Keywords: cyberattacks, attribution, public attribution of cyberattacks, tools of cyber diplomacy, cyber sanctions.