DOI: https://doi.org/10.18524/2411–2054.2021.43.241002
УДК 341.1/.8

М. В. Грушко, канд. юрид. наук, доцент
Національний університет «Одеська юридична академія»
Кафедра міжнародного та європейського права
Фонтанська дорога, 23, Одеса, 65009, Україна
e-mail: malvina.grushko@gmail.com
ORCID: 0000–0002–5856–8147

АТРИБУЦІЯ КІБЕРАТАК ЯК ПЕРЕДУМОВА ЗАБЕЗПЕЧЕННЯ ВІДПОВІДАЛЬНОЇ ПОВЕДІНКИ В КІБЕРПРОСТОРІ

Статтю присвячено питанню атрибуції кібератак з ціллю забезпечення відповідальної поведінки держав в кіберпросторі. Проаналізовано наявну практику публічної атрибуції та особливості атрибуції кібероперацій в цілому, що, як правило, потребує здійснення технічної, публічної та юридичної атрибуції. В статті також досліджено звичаєві підстави атрибуції поведінки державі, що містяться в Статтях про відповідальність держав та Талліннському керівництві 2.0 щодо застосування міжнародного права до кібероперацій. Особлива увага приділяється тесту ефективного контролю, який використовується для атрибуції поведінки недержавних акторів державі, та його застосуванню до кібератак. Нарешті, робиться висновок про необхідність об'єднання глобальних зусиль задля забезпечення відповідальної поведінки в кіберпросторі, особливо в контексті міжнародної безпеки.

Ключові слова: кібероперації, кібератаки, атрибуція, публічна атрибуція кібератак, юридична атрибуція кібератак, Талліннське керівництво, відповідальна поведінка в кіберпросторі.

Постановка проблеми. Стрімкий розвиток технологій призвів до постійного зростання кількості кібератак. Кіберпростір став ще одним середовищем, де держави намагаються досягати своїх інтересів. Щоправда, їх діяльність в кіберпросторі суперечить основним постулатам міжнародного права та призводить до порушення ряду норм та принципів. Попередити значну кількість кібератак можливо шляхом притягнення держав до відповідальності, але наразі процес атрибуції ускладняється особливостями кіберпростору.

Мета статті. Проаналізувати наявний досвід атрибуції кібератак, а також встановити які норми та як саме будуть застосовуватися при здійсненні юридичної атрибуції для цілей притягнення держав до міжнародної відповідальності.

Виклад основного матеріалу. В своїй Доповіді від 24 червня 2013 року група урядових експертів з досягнень в сфері інформатизації і телекомунікацій встановила, що «міжнародне право, і зокрема Статут Організації Об'єднаних Націй, застосовується і має важливе значення для підтримки миру, стабільності, створення відкритого, безпечного, мирного і доступного інформаційного середовища… та поширюється на поведінку держав у межах діяльності, пов'язаної з використанням ІКТ» [12, пар. 19, 20]. Очікувалось, що такий висновок буде сприйнятий державами як застереження щодо утримання від неправомірної діяльності в кіберпросторі, адже застосування норм та принципів міжнародного права покладає на державу зобов'язання, у випадку порушень яких наступають несприятливі наслідки. Проте, на практиці держави часто вдаються до протиправної діяльності в кіберпросторі задля досягнення своїх геополітичних інтересів, цим самим ігноруючи свої зобов'язання за міжнародним правом. Це означає, що притягнення держав до відповідальності повинно стати тим важелем, який допоможе значно скоротити кількість кібератак і сприяти відповідальній поведінці в кіберпросторі.

Встановлення відповідальності держави не можна уявити без атрибуції. У випадку з кібероперaціями мова йде не тільки про юридичну атрибуцію, а й про здійснення технічної та публічної (політичної) атрибуції, які їй передують. Технічна атрибуція дозволяє пов'язати кібератаку з конкретним комп'ютером та/чи особою на підставі оцінки

технічних «відбитків». Публічна атрибуція полягає в реалізації суверенної волі держав присвоїти кібератаку конкретній державі, на яку вказують технічні та, в першу чергу, політичні індикатори [4]. Залежно від своїх цілей та інтересів держава може здійснити атрибуцію кібератаки або утриматися від таких дій. Нарешті, юридична атрибуція дозволяє атрибутувати поведінку осіб, що стояли за виконанням кібератаки, державі відповідно до звичаєвих норм відповідальності держави.

На сьогоднішній день сутнісні характеристики кібератак надають державам ряд переваг та ускладнюють процес атрибуції, який є необхідним для притягнення держави до відповідальності. Зокрема, кіберпростір дозволяє зберігати анонімність та маскуватись за допомогою спуфінг-атак під іншу державу. Окрім цього, за умови здійснення успішної кібератаки, держава-правопорушниця може завдати серйозних наслідків при використанні досить незначних ресурсів у порівнянні з тими, що необхідні на реалізацію кінетичної операції з аналогічними руйнівними наслідками.

Сучасні людські та технічні можливості, що знаходяться у розпорядженні держав, тривалий час були досить обмеженими, і унеможливлювали процес встановлення виконавців кібератак та держав, що за ними стоять. Наразі, навпаки, значна кількість держав демонструє свою здатність та бажання здійснювати атрибуцію кібератак. Так, наприклад, в 2015 році директор Національної розвідки США Джеймс Клеппер заявив: «Хоча кібероператори можуть проникати або порушувати цільові мережі ІКТ, більшість з них уже не може розраховувати на те, що їх діяльність залишиться непоміченою. Вони також не можуть розраховувати, що у разі виявлення вони матимуть змогу приховати свою особу. Професіонали уряду та приватного сектору досягли значних успіхів у виявленні та атрибуції кібератак» [1]. З позиції канцлера Великобританії Джорджа Осборна також випливає готовність Великобританії до атрибуції кібератак, що підтверджується багатою практикою публічної атрибуції кібератак державним та недержавним акторам [6].

Кібероперації змусили відійти від державоцентризму в процесі атрибуції, оскільки обмежені ресурси держави часто компенсуються за рахунок підвищеної співпраці з приватним сектором. Іноді це також зумовлено більшими можливостями та оперативністю приватного сектору. Серед яскравих прикладів вдалої атрибуції та аналізу кібероперацій варто згадати звіт приватної компанії CrowdStrike «Putter Panda» [2], в якому встановлено, що підрозділ 61486 Китайської Народно-визвольної армії відповідальний за злочинну крадіжку корпоративної комерційної таємниці, насамперед стосовно супутникової, аерокосмічної та комунікаційної галузей. А технічний звіт компанії Symantec щодо вірусу «Stuxnet», який був використаний проти іранської ядерної установки, вплинув на дипломатичні відносини між державами, розгляд питань про розповсюдження ядерної зброї та механізми глобального управління кібербезпекою [10].

Практика публічної атрибуції кібероперацій, яка за останнє десятиліття значно зросла, свідчить про бажання держав забезпечувати відповідальну поведінку в кіберпросторі. Водночас, як видається, публічних заяв щодо атрибуції не достатньо. Обмежувальні заходи ЄС щодо осіб, які стояли за серйозними кібератаками, є кроком вперед, але вони також не можуть значно підвищити відповідальну поведінку в кіберпросторі. Зокрема, у випадку з публічною атрибуцією кібератаки «NotPetya» рядом держав Російській Федерації та навіть після включення співробітників Головного управління Генерального штабу ЗСУ РФ до санкційного списку ЄС за цю кібератаку, Росія продовжує заперечувати свою причетність. Міністерство закордонних справ РФ постійно виражає позицію щодо бездоказовості, антиросійської сутності таких дій і їх «нелегітимності» за міжнародним правом [13]. Таким чином, існує необхідність здійснення юридичної атрибуції, яка може поставити точку у спорі щодо причетності держави та її державних органів до кібератаки.

Норми щодо атрибуції міжнародно-протиправних діянь державі містяться в Статтях про відповідальність держав 2001 року [3]. Хоча дані Статті представляють собою доктрину, немає сумнівів стосовно звичаєвого характеру статей, що містять положення про присвоєння поведінки державі. Звичаєвий характер даних статей фактично підтверджений групою міжнародних експертів, що розробили Талліннське керівництво 2.0 щодо

застосування міжнародного права до кібероперацій [8]. Правила 14, 15, 17 Талліннського керівництва дублюють положення Статей, адаптуючи їх зміст до кібероперацій. Зазначені статті є найбільш релевантними, але Талліннське керівництво містить і інші статті щодо атрибуції, зокрема Правила 16 та 18, які стосуються атрибуції кібероперацій здійснених органами однієї держави під тимчасовим розпорядженням іншої та у випадку сприяння чи надання допомоги у здійсненні кібератаки (відповідно).

Правило 14 передбачає загальну норму щодо відповідальності держави за кіберпов'язану поведінку, що атрибутується державі і представляє порушення міжнародного зобов'язання. Воно віддзеркалює ідею, яка була закладена в суть Статей про відповідальність держав – «кожне міжнародно-протиправне діяння тягне за собою міжнародну відповідальність цієї держави» [3, ст. 1]. Як видається, у випадку з найбільш серйозними та масштабними кібератаками, що загрожують нормальному функціонуванню держави та добробуту населення країни, атрибуція такої зловмисної кіберповедінки є більш, ніж очікуваною. При цьому, дане правило застосовується не лише до кібероперацій, а й до поведінки при якій держава зробила свою кіберінфраструктуру доступною для недержавних груп чи інших держав, не вживши необхідних заходів для припинення кібероперацій, що походить із її території або надала програмне забезпечення для виконання кібероперації [8, с. 84–85].

Правило 15 Талліннського керівництва інтегрує дві підстави для атрибуції поведінки державі за Статтями про відповідальність держав, а саме – поведінку державних органів та фізичних чи юридичних осіб, що здійснюють елементи урядових функцій [3, ст. 4, 5]. Відтак, експерти Талліннського керівництва об'єднали в одному правилі поведінку *de jure* та *de facto* органів держави, хоча і розмежували їх в силу різного статусу. Згідно з Правилом 15, «Кібероперації, що проводяться органами держави або особами чи організаціями, уповноваженими національним законодавством здійснювати елементи державних повноважень, атрибутуються державі». З одного боку, це означає те, що діяльність кіберармій, військових кіберпідрозділів та розвідувальних органів, що вдаються до кібероперацій чи іншої кіберпов'язаної діяльності буде присвоюватися державі, незалежно від того, чи має цей суб'єкт статус органу за національним законодавством. З іншого боку, мова йде про приватних осіб, що уповноважені на здійснення урядових функцій. Зокрема, дії приватних корпорацій, ІТ-компаній чи компаній, що займаються питаннями кібербезпеки, атрибутуються державі, коли вони уповноважені державою на здійснення кіберрозвідки або наступальних кібероперацій проти іншої держави [8, с. 89]. Водночас їх поведінка, яка не пов'язана із розвідкою чи здійсненням наступальних операцій, присвоюватися державі не може. Наприклад, злочинна діяльність, яка здійснюється паралельно з метою отримання прибутку, немає ніякого відношення до «елементів урядових повноважень». Така діяльність може атрибутуватися уряду, якщо здійснюється під його керівництвом чи контролем, але юридична підстава атрибуції буде іншою, тому що злочинна діяльність в кіберпросторі не може розглядатися в якості реалізації найважливіших урядових функцій.

Правило 17 Талліннського керівництва також об'єднує дві підстави для атрибуції поведінки державі та повторює формулювання статей 8 та 11 Статей про відповідальність держав [3, ст. 8, 11]. Відповідно до даного Правила, кібератаки недержавних акторів присвоюються державі, коли: «(a) здійснюється згідно з її інструкціями або під її керівництвом чи під контролем; або (b) держава визнає та приймає операції як власні» [8, с. 94]. Це правило підтверджує застосування тесту ефективного контролю, що був розроблений Міжнародним Судом ООН у справі про військову та напіввійськову діяльність в Нікарагуа («Нікарагуа проти США») [5]. І, як свідчить практика міжнародних судових установ, він встановлює досить високий поріг контролю в силу того, що стосується відповідальності держав. В кіберпросторі, як видається, його складно (якщо можливо) досягти, адже потрібно довести, що держава надавала конкретні вказівки щодо вчинення конкретної операції [5, пар. 86]. У випадку з кібератаками, це також передбачає те, що держава має бути в позиції визначати хід конкретної операції, а кібердіяльність

недержавного суб'єкта розглядається в якості «невід'ємної частини» операції держави [3, ст. 3, пар. 8].

Встановити ефективний контроль держави над недержавним актором майже неможливо, особливо для держав, які не мають достатніх фінансових та/або технічних ресурсів [9, с. 201]. В результаті даний тест часто сприймається як «ліцензія на безкарність в кіберпросторі», оскільки здійснення кібератаки недержавними акторами та правдоподібне заперечення з боку, як стверджується, держави-правопорушниці унеможливлюють задоволення вимог даного тесту. Так, наприклад, існують комп'ютерно-технічні та стратегічні докази того, що так звані «кіберпатріоти» Російської Федерації здійснювали кібератаки під керівництвом Уряду РФ в ході збройних конфліктів з Грузією у 2008 році. Але коли мова доходить до атрибуції, фактично неможливо представити докази ефективного контролю.

Занадто високий стандарт спричинив ряд дискусій щодо застосування тесту загального контролю замість тесту ефективного контролю. Тест загального контролю був вперше застосований Міжнародним кримінальним трибуналом по колишній Югославії у справі Душко Тадіча. Відповідно до нього, для відповідальності достатньо встановити роль держави в організації, координації або наданні підтримки недержавним акторам [7, пар. 104]. Тобто, цей тест полягає в тому, що загальний контроль повинен бути доведений поза розумним сумнівом, і вважається досяжним у випадку з атрибуцією кібератак задля притягнення держави до відповідальності [9, с. 198–201].

Щодо атрибуції кібератак пропонується розробка та застосування нових тестів в силу природи кібероперацій, такі як тест «контролю та можливостей», який, як стверджується, ґрунтується на останній практиці публічного присвоєння кібератак державі і має ще нижчий поріг, ніж тест загального контролю [11].

Справедливим буде зазначити, що незалежно від тесту, який буде застосовуватися для атрибуції кібератак, стандарт доказування в будь-якому разі залишиться досить високим. Крім того, тест ефективного контролю в силу встановленого високого порогу для атрибуції кібератак певною мірою захищає держави від можливих негативних наслідків з боку постраждалої держави. До прикладу, як застерігають експерти Талліннського керівництва 2.0, якщо висновок постраждалої держави щодо атрибуції виявиться хибним внаслідок застосованого тесту загального контролю, держава, що вдасться зокрема до контрзаходів, сама стане державою-правопорушницею по відношенню до тієї держави, щодо якої були застосовані контрзаходи.

Висновки і пропозиції. Наявна практика публічної атрибуції кібератак державам є значним кроком в забезпеченні відповідальної поведінки в кіберпросторі. Проте, лише юридична атрибуція зможе по-справжньому стримувати держави в кіберпросторі від поведінки, яка суперечить та порушує норми і принципи міжнародного права.

Очевидно, держави повинні об'єднати свої зусилля на міжнародному рівні для сприяння відповідальній поведінці в кіберпросторі, важливим елементом якої має стати атрибуція кібератак державам, а, отже, відповідальність такої держави. При цьому, відсутня необхідність розробки юридичного інструменту, який містив би правила атрибуції кібератак. Правил, які містяться в Талліннському керівництві, яке є найбільш авторитетним в питаннях застосування міжнародного права до кібероперацій, та звичаєвих норм про атрибуцію поведінки державі наразі достатньо.

Список використаних джерел:

1. Clapper J. Worldwide Threat Assessment of the US Intelligence Community. *Testimony to the Senate Armed Services Committee*. February 26, 2015. URL: https://www.dni.gov/files/documents/Unclassified_2015_ATA _SFR_-_SASC_FINAL.pdf.
2. CrowdStrike`s Intelligence Report Putter Panda. 2014. URL: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
3. Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1. URL: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

4. Lin H. Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Columbia Journal of International Affairs.* 2016. 70 (1). URL: https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents.
5. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984, p. 392. URL: https://www.icj-cij.org/public/files/case-related/70/070–19841126-JUD-01–00-EN.pdf.
6. Osborne G. Chancellor`s Speech to GCHQ on Cyber Security. *UK`s Government official website*. November 17, 2015. URL: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.
7. Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94–1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.
8. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. 2017. 598 p.
9. Shackelford S. State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Conference on Cyber Conflict Proceedings 2010: C. Czosseck and K. Podins (Eds.). pp. 197–208.
10. Stevens C. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*. 2020. 41(1). pp. 129–152. URL: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1675258.
11. Stockburger P. Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents. *NATO CCD COE Publications.* 2017. URL: https://ccdcoe.org/uploads/2018/10/Art-10-Toward-a-New-Lex-Specialis-Governing-State-Responsibility-for-Third-Party-Cyber-Incidents.pdf.
12. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. ГА ООН. A/68/98*, 24 июня 2013. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R
13. Заявление МИД России «Об очередных нелегитимных ограничительных мерах Европейского Союза против России» от 22.02.2021. Официальный сайт Министерства иностранных дел Российской Федерации. URL: https://www.mid.ru/web/guest/evropejskij-souz-es//asset_publisher/6OiYovt2s4Yc/content/id/4590496.

References

1. Clapper J. Worldwide Threat Assessment of the US Intelligence Community. *Testimony to the Senate Armed Services Committee*. February 26, 2015. URL: https://www.dni.gov/files/documents/Unclassified_2015_ATA _SFR_-_SASC_FINAL.pdf.
2. CrowdStrike`s Intelligence Report Putter Panda. 2014. URL: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
3. Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1. URL: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
4. Lin H. Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Columbia Journal of International Affairs.* 2016. 70(1). URL: https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents.
5. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984, p. 392. URL: https://www.icj-cij.org/public/files/case-related/70/070–19841126-JUD-01–00-EN.pdf.
6. Osborne G. Chancellor`s Speech to GCHQ on Cyber Security. *UK`s Government official website*. November 17, 2015. URL: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.
7. Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94–1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.
8. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. 2017. 598 p.
9. Shackelford S. State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Conference on Cyber Conflict Proceedings 2010: C. Czosseck and K. Podins (Eds.). pp. 197–208.
10. Stevens C. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*. 2020. 41(1). pp. 129–152. URL: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1675258.
11. Stockburger P. Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents. *NATO CCD COE Publications.* 2017. URL: https://ccdcoe.org/uploads/2018/10/Art-10-Toward-a-New-Lex-Specialis-Governing-State-Responsibility-for-Third-Party-Cyber-Incidents.pdf.
12. Report of the Group of Governmental Experts on Advances in Informatization and Telecommunications in the Context of International Security. UN GA. A / 68/98 *, 24 June 2013. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R. [in Russian].
13. Statement of the Russian Foreign Ministry «On the next illegitimate restrictive measures of the European Union against Russia» dated 02.22.2021. *Official website of the Russian Ministry of Foreign Affairs.* URL: https://www.mid.ru/web/guest/evropejskij-souz-es/-/asset_publisher/6OiYovt2s4Yc/content/id/4590496. [in Russian]

Стаття надійшла 10.09.2021 р.

М. В. Грушко, канд. юрид. наук, доцент
Национальный университет «Одесская юридическая академия»
Кафедра международного и европейского права
Фонтанская дорога, 23, Одесса, 65009, Украина
e-mail: malvina.grushko@gmail.com
ORCID: 0000–0002–5856–8147

АТРИБУЦИЯ КИБЕРАТАК КАК ПРЕДПОСЫЛКА ОБЕСПЕЧЕНИЯ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ В КИБЕРПРОСТРАНСТВЕ

Резюме

Статья посвящена вопросу атрибуции кибератак с целью обеспечения ответственного поведения государств в киберпространстве. Проанализировано имеющуюся практику публичной атрибуции и особенности атрибуции кибероперацій в целом, что, как правило, требует осуществления технической, публичной и юридической атрибуции. В статье также исследованы обычные основания атрибуции кибератак государству, содержащиеся в Статьях об ответственности государств и Таллинском руководстве 2.0 по применению международного права к кибероперациям. Особое внимание уделяется тесту эффективного контроля, который используется для атрибуции международно-противоправных деяний государству совершенных негосударственными актерами под его контролем. Наконец, делается вывод о необходимости объединения глобальных усилий для обеспечения ответственного поведения в киберпространстве, особенно в контексте международной безопасности.

Ключевые слова: кибероперации, кибератаки, атрибуция, публичная атрибуция кибератак, юридическая атрибуция кибератак, Таллинское руководство, ответственное поведение в киберпространстве.

M. V. Hrushko, Candidate of Juridical Sciences, Associate Professor
National University «Odessa Law Academy»
the Department of International and European Law
Fontanska Doroga, 23, Odessa, 65009, Ukraine
e-mail: malvina.grushko@gmail.com
ORCID: 0000–0002–5856–8147

ATTRIBUTION OF CYBERATTACKS AS A PREREQUISITE FOR ENSURING RESPONSIBLE BEHAVIOR IN CYBERSPACE

Summary

Growing impunity in cyberspace is cause by the lack of responsibility for the most serious cyberoperations that present a threat to both state and non-state actors. The only possible solution is to trace such cyberoperations to those who stand behind them. Since the seriousness of consequences increases in case of state-committed cyberattacks, the article deals with the issue of attribution of cyberattacks to states with the aim of ensuring responsible behavior of all states in cyberspace.

The existing practice of public attribution and features of cyberoperations, as a rule, requires not only performing legal attribution, but also technical and public (political) attribution. Author thus starts with analyzing the current state of affairs – public attribution of cyberattack, its effectiveness and the role of private sector in attribution (decentralized attribution to support or deny government`s finding). The article also examines the customary basis for attributing state-related cyberattacks contained in the Articles on State Responsibility for Internationally Wrongful Acts and Tallinn Manual 2.0 on the Application of International Law to Cyberoperations. Although public attribution is, indeed, a step towards responsible behavior in cyberspace, legal attribution may contribute even more.

In this article increased attention is paid to the test of effective control, which is used to attribute internationally wrongful acts to states committed by non-state actors acting under its control or direction. Finally, it concludes that global efforts are needed to ensure responsible behavior in cyberspace, especially in the context of international security. For this, states should get into partnership with private sector in performing attribution of cyberoperations and apply to international bodies, which have jurisdiction over state claims and are able to perform legal attribution for the purpose of establishing state responsibility. Only in this way it will be possible to guarantee responsible behavior of states in cyberspace, and create a common understanding and approach against cyberoperations committed by non-state cyber actors.

Keywords: cyberoperations, cyberattacks, attribution, public attribution of cyberattacks, legal attribution of cyberattacks, Tallinn Manual, responsible behavior in cyberspace.