DOI https://doi.org/10.36059/978-966-397-237-4-11

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

КІБЕРАТАКИ ТА МІЖНАРОДНЕ ПРАВО: ПРИРОДА Й АНАЛІЗ OPINIO JURIS ДЕРЖАВ ЩОДО ЗАСТОСОВУННЯ МІЖНАРОДНОГО ПРАВА В КІБЕРПРОСТОРІ

Анотація*. Кібернетичні атаки є серйозним викликом для міжнародної спільноти, з огляду на їх постійне збільшення, відсутність lex specialis та практики притягнення до відповідальності за такі атаки. Оскільки opinio juris може компенсувати недостатньо розвинуту або непослідовну практику держав щодо формування міжнародних звичаїв, метою дослідження є виявлення того, наскільки позиція держав, виражена в різних формах opinio juris, є узгодженою щодо застосування конкретних норм міжнародного права в кіберпросторі. Це дасть змогу встановити розуміння та очікування держав щодо інтерпретації та застосування наявних норм до кібератак, а також ідентифікацію юридичних підстав для притягнення держав до відповідальності за кібератаки, що їм атрибутуються.*

Здійснено аналіз офіційних заяв, декларацій, воєнних доктрин, національних стратегій та інших форм вираження opinio juris, в процесі якого встановлено різні підходи до норм міжнародного права, які, на думку держав, застосовуються чи не застосовуються до кібератак. Також встановлено, що наявне opinio juris нині не дозволяє зробити висновок про формування універсальних звичаєвих норм міжнародного кіберправа через різне розуміння того, які норми, за яких умов та як застосовуються в кіберпросторі.

Вступ

Стрімкий розвиток інформаційно-комунікаційних технологій (далі – ІКТ) створив низку можливостей для міжнародної спільноти загалом та для окремих держав загалом. Такий розвиток ІКТ сприяв тому, що паралельно до звичних для

людства просторів (суша, повітряний, морський та космічний простори) виникає ще один – кіберпростір, який фактично є віртуальним інформаційно-комунікаційним простором.

Станом на квітень 2021 року близько 4,72 мільярдів осіб постійно користуються можливостями Інтернету, що становить більш ніж 60% населення Землі [22]. З огляду на те, що використання кіберпростору значною частиною людей здійснюється із метою встановлення та реалізації політичних, економічних та соціальних зв'язків (участь у прийнятті політичних рішень, доступ до публічних послуг, комунікація тощо), можна з впевненістю стверджувати, що кіберпростір став невід'ємною та важливою частиною життя у XXI столітті. На думку низки вчених, кіберпростір охоплюється концепцією «спільна спадщина людства»; крім того, доступ до тих можливостей та переваг, які він надає, захищається на міжнародному та національному рівнях [15, с. 89–90].

Саме кіберпростору ми завдячуємо виникненням нетрадиційних для людства атак – кібератак, адже він є середовищем для їх реалізації та забезпечує їх необхідними засобами здійснення – технічними можливостями кіберпростору [10, с. 341]. На відміну від «фізичного» світу з його «кінетичними» атаками, кіберпростір та здійснювані в межах нього кібератаки характеризуються низкою особливостей. Згідно з Талліннським керівництвом 2.0, що представляє собою найбільш авторитетне доктринальне дослідження щодо застосування міжнародного права до кібероперацій, *кіберпростір* – це «середовище, утворене фізичними та нефізичними компонентами для зберігання, модифікації та обміну даними за допомогою комп'ютерних мереж» [48, с. 564]. Схоже розуміння цього поняття міститься в ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, де зазначається, що під кіберпростором варто розуміти «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [7, ст. 1].

Аналіз вищезгаданих понять дає змогу встановити, що кіберпростір – це не лише віртуальне середовище. Він складається з трьох різних рівнів (пластів) – фізичного, логічного

та соціального [48, с. 12], – *в межах яких або проти яких можна здійснювати кібератаки*. Важливо, що в будь-який момент «функціонально релевантні компоненти кожного пласту знаходяться десь на земній кулі, як правило, на суверенній території або підконтрольній принаймні одній державі» [16, с. 9].

Фізичний пласт кіберпростору складається з фізичних компонентів мережі, а також географічної складової частини. Фізичні компоненти мережі включають всі елементи – від оптоволоконних кабелів до стільникових вишок, комп'ютерів та серверів, що необхідні для зберігання, обробки та передачі інформації в кіберпросторі. Знаходження цих елементів у фізичному просторі є відправною точкою для встановлення географічного розташування, а отже, становить географічну складову частину фізичного пласту кіберпростору [48, с. 9].

Логічний пласт кіберпростору можна розглядати як центральну нервову систему кіберпростору. Цей пласт відповідає за маршрутизацію пакетів даних до їх кінцевих пунктів призначення [45, с. 41–42]. Отже, він є абстрактним та стосується систем доменних імен, Інтернет-протоколів, браузерів, програмного забезпечення, через які передаються дані, та покладається на згадані вище компоненти фізичного пласту.

Зрештою, соціальний пласт охоплює всіх акторів, що беруть участь у кіберактивності. Іноді його ще називають компонентом «кіберперсона», оскільки він охоплює процес ідентифікації особи або персони в мережі (електронна адреса, IP-адреса комп'ютера, номер мобільного телефону та інші) [30, с. 121–122]. При цьому індивід може мати кілька кіберперсон (зокрема, за рахунок наявності кількох облікових записів на різних комп'ютерах), а одна кіберперсона може використовуватися кількома користувачами (особами).

У Талліннському керівництві 2.0 підкреслюється, що «фізичний, логічний та соціальний пласти кіберпростору підпадають під сферу охоплення принципу суверенітету» [48, с. 12]. Разом із тим кіберпростір – це глобальний вимір, позбавлений фізичних кордонів, який *de facto* має транснаціональний характер. Він доступний для всіх і кожного, що робить його системи тісно взаємопов'язаними і часто призводить до кваліфікації таких систем як систем подвійного використання. Отже, для того щоб, наприклад, нападнику обірвати військовий зв'язок, швидше за все, доведеться зруйнувати всю мережу, яка

використовується не лише військовими, а й цивільними. Такий тісний взаємозв'язок вже нині змушує задуматись над тим, як гарантувати відповідальне використання кіберпростору в мирний та воєнний час, враховуючи високу залежність від об'єктів критичної інфраструктури, функціонування яких залежить від стійкості ІКТ.

З огляду на природу кібероперацій і можливість їх легко «замаскувати», кіберпростір також дає змогу зберегти анонімність і передбачає складний процес атрибуції для встановлення кола осіб, причетних до кібероперацій. А вторинні чи навіть третинні наслідки кібератак є більш значимими, ніж їх первинні наслідки, що значно виділяє кібератаки на фоні звичайних атак [46, с. 534]. Всі ці особливості створюють серйозний виклик для міжнародного права, якому потрібно швидко адаптуватись до розвитку технологій, що завжди на крок випереджає кодифікацію норм міжнародного права.

У доктрині є багато визначень того, що входить у поняття «кібератака». Більшість вчених сходяться на тому, що кібератака – це діяльність, яка спрямована на використання, спотворення, підміну або знищення інформації в комп'ютерній мережі або пов'язаній системі [5, с. 29]. З позиції міжнародно-правової доктрини, на особливу увагу заслуговує визначення, надане експертами Талліннського керівництва. Згідно з ним, *кібератака* – «це кібероперація, наступальна або оборонна, що цілком очікувано може призвести до завдання трав чи смерті осіб або шкоди чи знищення об'єктів» [48, с. 415]. Приклади включають маніпуляції та знищення даних або коду в комп'ютерній системі для управління або відключення електромережі, з метою обривання (чи іншого порушення) військового зв'язку або для деградації надійності банківських даних.

Необхідно також відмежовувати кібератаки від *кібер-експлуатації*, що за своєю природою також входить у поняття «кібероперація». Фундаментальна відмінність між двома категоріями полягає в тому, що вони призводять до різних юридичних, політичних та юрисдикційних наслідків. Випадки кіберексплуатації, хоч і мають вплив на міжнародні відносини між державами, але, як правило, підпадають під виключну сферу регулювання національного права. Кіберексплуатація є актом спостереження (моніторингу) та пов'язаного з ним шпигунства за комп'ютерними системами, а також копіювання (і, отже,

крадіжки) даних у цих системах. Приклади кіберексплуатації включають викрадення військових таємниць, об'єктів інтелектуальної власності, номерів кредитних карток тощо [44, с. 9–12, 32]. На відміну від кібератаки, кіберексплуатація не спрямована на порушення звичного функціонування комп'ютера або мережі.

У межах цього дослідження увага приділятиметься виключно кібератакам, що передбачають втручання та мають потенціал до завдання кінетичних наслідків. Проте на практиці кіберексплуатація передує здійсненню кібератаки, оскільки успішна кібератака залежить від ефективного спостереження за комп'ютерними системами та встановлення вразливостей таких систем. Як уже зазначалося, середовищем реалізації кібератак є кіберпростір, а засобами здійснення – технічні можливості кібернетичного простору, зокрема розробка або пошук вразливостей систем управління (активів) [10, с. 341]. Тому, на противагу кіберексплуатації, в процесі кібератак використовують можливості вірусів-шифрувальників та/чи ботнетів задля розгортання розподілених атак проти операційних систем (DDoS-атак), активації багатофункціонального шкідливого програмного забезпечення, хмарних ланцюгів тощо.

З першого погляду може здатися, що є загальне розуміння того, що собою представляють кібератаки задля колективного реагування на можливі наслідки та їх попередження в майбутньому. Проте в теорії і ще більше на практиці виникає ряд питань до атак у кіберпросторі, зокрема: що є об'єктом кібератаки; в який момент конкретна кібероперація може кваліфікуватися як кібератака; чи застосовується міжнародне право до кібератак і, якщо так, то в якому об'ємі. Усі ці питання є логічним наслідком того, що відсутнє спеціальне правове регулювання кібероперацій, яке б містило юридично обов'язкове поняття та норми, що застосовуються до них. Це зумовлює необхідність дослідження позиції держав та міжнародних установ щодо застосування міжнародного права в кіберпросторі.

1. Кібератаки та міжнародне право

Експерти Талліннського керівництва зробили значний внесок у розуміння того, як міжнародне право застосовується до кіберпростору, але, як зазначив професор Женевського університету Марко Сассолі, «воно [Талліннське керівництво]

не зуміло представити нові правила там, де це було потрібно, і часто критикується за те, що було розроблено в основному експертами НАТО» [46, с. 541]. Він також зазначив, що сучасна міжнародна атмосфера не сприяє і не буде сприяти розробці нових правил, допоки міжнародна спільнота не засвідчить кібератаку з катастрофічними наслідками [46, с. 542]. Але навіть якщо спеціальні норми будуть розроблені, існує високий ризик того, що через швидкий розвиток технологій вони застаріють до моменту вступу в силу [58, пар. 24].

Проте беззаперечним залишається те, що чинне міжнародне право застосовується до кібероперацій. У Доповіді групи урядових експертів щодо досягнень у сфері інформатизації та телекомунікацій і контексті міжнародної безпеки від 24 червня 2013 року зазначається: «*Міжнародне право, зокрема Статут Організації Об'єднаних Націй, застосовується* і має важливе значення для підтримки миру і стабільності і створення відкритого, безпечного, мирного і доступного інформаційного середовища… [М]іжнародні норми і принципи, що випливають із принципу державного суверенітету, поширюються на поведінку держав у межах діяльності, пов'язаної з використанням ІКТ, а також на юрисдикцію держав над ІКТ-інфраструктурою на їх території» [4, пар. 19–20; 3, пар. 24–26]. У Доповіді урядових експертів від 2015 року, яка підтверджує висновок про застосування Статуту та міжнародного права до ІКТ, вказується, що «найважливіше значення» мають такі зобов'язання, як «суверенна рівність держав; вирішення міжнародних суперечок мирними засобами таким чином, щоб не ставити під загрозу міжнародний мир і безпеку і справедливість; відмова в міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і будь-яким іншим чином несумісним із цілями Організації Об'єднаних Націй; повага прав людини і основних свобод; невтручання у внутрішні справи інших держав» [3, пар. 26].

У Консультативному висновку 1996 року про законність погрози ядерною зброєю або її застосування Міжнародний Суд ООН підкреслив, що міжнародне гуманітарне право «застосовується до всіх форм воєнних дій та всіх видів зброї минулого, сьогодення і майбутнього» [6, с. 36]. У межах роботи групи урядових експертів експерти від Російської Федерації та

Китаю заперечували можливість застосування МГП до кібератак, оскільки, на їх думку, це може призвести до виправдання ворожого застосування кіберпростору проти військових об'єктів [34]. Позиція Куби, яка є у відкритому доступі, також зводилась проти визначення того, як *jus ad bellum* та *jus in bello* застосовуються до використання ІКТ з огляду на побоювання щодо потенційної мілітаризації кіберпростору, яке може «легітимізувати <...> односторонні каральні силові дії, включаючи застосування санкцій і навіть збройної сили державами, які заявляють, що є жертвами незаконного використання ІКТ» [20]. Насправді такі побоювання не позбавлені раціонального зерна, але, незважаючи на таку риторику, застосування міжнародного гуманітарного права до кібероперацій, незалежно від того, розглядаються вони як засіб чи метод ведення військових дій, є беззаперечним [46, с. 534].

У своїй Декларації представник Куби також виразив позицію щодо неможливості розглядати зловмисне використанням ІКТ як «збройна атака», що згадується в ст. 51 Статуту ООН, та наділяє постраждалу державу *правом на самооборону* відповідно до *jus ad bellum.* Такий підхід він обґрунтував тим, що оновлена інтерпретація положень Статуту призведе до нав'язування «законів джунглів», де інтереси найсильніших держав матимуть перевагу над інтересами найбільш вразливих. Разом із тим у Декларації містився заклик до необхідності «прийняти міжнародний юридично обов'язковий інструмент, щоб на основі співпраці ефективно реагувати на значні існуючі правові прогалини в контексті кібербезпеки та зростаючі виклики та загрози, з якими ми стикаємось у цій галузі» в межах діяльності Організації Об'єднаних Націй [20].

Беручи до уваги той факт, що в роботі групи урядових експертів приймали представники лише 25 держав світу, можна допустити те, що ряд країн світу, зокрема латиноамериканських, схиляються до позиції, вираженої представником Куби. Пояснити це можна реальними побоювання щодо потенційних маніпуляцій і помилкової атрибуції, що є наслідком спуфінгу – маскування з ціллю фальсифікації даних щодо особи чи програми. В українському контексті також не варто виключати зловживання з боку Російської Федерації через активність Головного управління розвідки Збройних (далі – ГРУ) Сил РФ. Разом із тим цю проблему можна вирішити шляхом розробки

юридично обов'язкового інструменту, який передбачав би створення спеціального правового режиму для здійснення міжнародно-правової кваліфікації та атрибуції кібератак на міжнародному рівні. Інакше складно собі уявити, як Рада Безпеки ООН може надавати рекомендації чи приймати рішення щодо застосування заходів, які не передбачають чи передбачають використання збройних сил відповідно до ст. 40 та ст. 41 Статуту, «зацікавленим сторонам» чи щодо них, коли відсутнє розуміння того, хто ці сторони (як правило, складнощі існують щодо ідентифікації саме держави-правопорушниці). Ще один висновок, який випливає з цієї позиції, – відсутність загальної підтримки положень Талліннського керівництва з боку всіх держав, принаймні на цей момент.

Що стосується активації *jus in bello,* важливо, щоб кібератака кваліфікувалася як збройна атака. Оскільки юридично встановлене визначення того, що таке кібератака, відсутнє, звернемося до традиційного поняття «атака» (або «напад» відповідно до офіційного перекладу поняття «attack», що є синонімами у цьому випадку), яке міститься в ст. 49 (1) Додаткового Протоколу I до Женевських Конвенцій 1949 року. Згідно з ним, поняття «атака» охоплює «акти насильства щодо противника, незалежно від того, здійснюються вони під час наступу чи під час оборони» [2, ст. 49(1)], а також представляє собою військові дії «на суші, в повітрі або на морі» [2, ст. 49(3)]. При цьому «акти насилля» не обмежені кінетичними засобами [23, с. 84; 46, с. 5]. Як зазначає професор М. Сассолі, воно є проблематичним та надмірно інклюзивним [46, с. 535]. Отже, можна погодитись із підходом експертів Талліннського керівництва, які встановили, що вирішальним фактором для кваліфікації кібератаки є очікувані наслідки від такої атаки, незалежно від того, є вони вторинними чи третинними за своєю природою [48, с. 415]. Саме операції, які здійснюються проти осіб чи об'єктів, розглядаються як атака, якщо ціллю останніх було завдання шкоди або знищення. Аналогічний підхід, зокрема, застосовується до використання ядерної, хімічної та біологічної зброї, яке також не передбачає застосування фізичної сили [31, пар. 120, 124]. Крім того, потрібно розуміти, що завдання шкоди системам, які використовується для здійснення кібератаки, не є необхідною умовою. Так, наприклад, за допомогою маніпуляцій системи управління SCADA водних дамб,

можна спричинити викид вод, а отже, втрати серед цивільного населення і знищення цивільних об'єктів. При цьому в подальшому сама система може продовжити своє нормальне функціонування і не зазнати кінетичних наслідків (пошкодження або знищення) [48, с. 416].

Суперечливим є момент щодо того, чи можуть *дані* бути об'єктом атаки. У Талліннському керівництві зазначається, що «операція проти даних, на яку покладається функціональність фізичних об'єктів, іноді може становити атаку». Разом із тим відкритим залишається питання: в яких саме випадках? Припустимо, що йдеться про *нейтралізацію* даних як об'єкта атаки, коли сторона отримує військову перевагу шляхом видалення даних, а не знищення систем. Ст. 52(2) Додаткового протоколу I до Женевських Конвенцій встановлює, що військовими є об'єкти «... повне або часткове руйнування, захоплення або *нейтралізація* яких при існуючих в даний момент обставинах надає очевидну військову перевагу» [2, ст. 52(2)]. Як випливає з поняття «нейтралізація», знищення об'єкта не є обов'язковою умовою [26, с. 4]. Тому, повертаючись до Талліннського керівництва, можна зробити висновок, що дані можуть стати об'єктом атаки. І хоча можна сперечатись щодо того, в яких ситуаціях військові операції проти даних становитимуть атаку, такі випадки, наприклад, як знищення даних, що забезпечують функціонування фінансового ринку країни, дозволяють маніпулювати системами управління повітряним рухом противника, системами потоків нафтопроводів або атомними станціями тощо, очевидно, розглядатимуться як кібератака.

Нарешті, кібератаки, які не досягли мінімального рівня застосування сили, призвели до порушень міжнародних зобов'язань. Вони розглядатимуться як порушення основних принципів міжнародного права – принципу суверенної рівності держав, заборони втручання у внутрішні справи держав тощо, або порушення договірних чи звичаєвих норм окремих галузей міжнародного права (міжнародного права прав людини, міжнародного повітряного права, міжнародного економічного права та ін.) залежно від конкретного контексту. У будь-якому разі, вважаємо, що держави мають максимально утриматися від реагування на кібератаки, що здійснюється на підставі односторонньої кваліфікації та атрибуції. Такий підхід є логічним

з огляду на обмежені технічні та людські ресурси більшості держав, оскільки в разі помилкової атрибуції вірогідним є настання серйозних наслідків (наприклад, невиправдане застосування права на самооборону фактично є актом застосування сили проти держави та становить міжнародно-протиправне діяння).

Таким чином, зважаючи на природу та наслідки кібератак, можна виділити три групи кібератак, які запускають різні правові режими та зобов'язання:

1) кібератаки, які досягають рівня збройного нападу (атаки) та наділяють державу правом на самооборону відповідно до *jus ad bellum;*

2) кібератаки, які можна кваліфікувати як збройну атаку, здійснені в процесі збройного конфлікту або такі, що активують *jus in bello*;

3) кібератаки, які не досягли мінімального рівня застосування сили, але призвели до порушень міжнародних зобов'язань (зокрема основних принципів міжнародного права).

2. Opinio juris держав щодо ключових питань застосування міжнародного права до кібератак

Пандемія COVID-19 – перше, що спадає на думку, коли мова йде про 2020 рік. Але пройдешній рік також увійшов в історію як рік кіберпандемії. Через те, що значна частина соціальних, економічних та політичних взаємодій відбувались у кіберпросторі, вдалось уникнути перебоїв у роботі основних секторів та серйозних наслідків для близько 80 відсотків економіки. Це спровокувало значний скачок у кібердіяльності. З одного боку, кіберпростір вирішив виклики, спричинені COVID-19, які не могли подолати, наприклад, під час пандемії у 1918 році, з іншого – прискорив зловмисну кібердіяльність різних акторів [35]. На фоні всіх акторів на особливу увагу заслуговують саме ті, чиї дії відповідно до міжнародного права можуть атрибутуватися державі для цілей притягнення держав до відповідальності.

Притягнення держави до відповідальності являє собою правовий режим, основні правила якого зав'язані на наявності двох елементів. Згідно зі ст. 2 Статей про відповідальність держав за міжнародно-протиправні діяння, міжнародна відповідальність держави настає у разі наявності протиправної поведінки, яка «(a) атрибутується державі відповідно до

міжнародного права; (б) представляє собою порушення державою свого міжнародного зобов'язання» [27, ст. 2]. Тобто відповідальність держав настає за наявності юридичних та фактичних підстав для такої відповідальності.

Під юридичними підставами відповідальності держав слід розуміти міжнародно-правові зобов'язання держави, незалежно від їх походження, що містять вимогу щодо поведінки держави, порушення якої дозволяє кваліфікувати діяння як міжнародне правопорушення [9, с. 153]. Як неодноразово вказував Міжнародний суд ООН, «зобов'язання можуть покладатись на державу в силу договору і в силу дії звичаєвої норми, або в силу договору і в силу одностороннього акта» [42, пар. 63].

У випадку з кіберпростором, щодо застосування якого відсутнє *lex specialis*, виникає необхідність встановити, як чинні міжнародні зобов'язання повинні тлумачитись та застосовуватись до конкретних кібероперацій. Вважається, що *opinio juris* може компенсувати недостатньо розвинуту або непослідовну практику держав щодо формування міжнародних звичаїв [14, с. 111–112]. Звісно заяви, декларації та воєнні доктрини мають орієнтуючий, а не визначальний характер, але на стадії формування норм (можливо, навіть і галуззі міжнародного кібернетичного права), що діють у кіберпросторі, аналіз *opinio juris* дає змогу встановити «межі» відповідальної поведінки в кіберпросторі, розуміння того, якими держави бачать наявні зобов'язання та що вкладають в їх зміст. Крім того, такі позиції демонструють переважаюче непогодження щодо таких аргументів, як необхідність нового правового інструменту, щоб заповнити «правовий вакуум» (із позиції Куби, вираженої в ході роботи групи урядових експертів) або «прогалину некерованих територій» (позиція Індонезії, яка виступала від імені Руху неприєднання) [11].

Вироблення і узгодження таких позицій у майбутньому сприятиме загальній практиці, а значить, формуванню звичаєвих норм міжнародного права. Цілком справедливо можна зауважити, що саме у сфері регулювання діяльності держав у кіберпросторі норми звичаєвого права переживуть своє відродження як основне джерело міжнародного права, оскільки розробка міжнародного інструменту швидше стане ще одним «проєктом статей» з огляду на інтенсивний розвиток інформаційних технологій, які завжди, принаймні на крок, випереджають позитивне міжнародне право.

З позицій держав, які опублікували офіційні заяви щодо того, як міжнародне право застосовується до кіберпростору, загальну підтримку має ідея того, що *воно застосовується*. Коли ж йдеться про конкретні зобов'язання, держави не завжди спроможні виробити чітку позицію. Так, наприклад, опублікована у 2021 році промова заступника генерального прокурора Ізраїлю, яка стосувалась поглядів Ізраїлю щодо ключових правових та практичних питань застосування міжнародного права до кібероперацій, містить більше питань, ніж відповідей [49, с. 395]. Включення її до бази НАТО [55] підтверджує юридичний характер такої заяви, а не виключно доктринальну природу. Своєю чергою позиція Ліхтенштейну від 10 лютого 2020 року зводиться до визнання того, що Статут ООН загалом та інші джерела міжнародного права, зокрема в галузі міжнародного гуманітарного права, права людини та міжнародного кримінального права застосовуються в кіберпросторі. Нині Ліхтенштейн єдина держава, яка безпосередньо згадала міжнародне кримінальне право у своїй заяві. Що ж стосується інших держав, то їх позиція зводиться до відповідальності держав, а згадка про можливу відповідальності індивідів відсутня (за винятком відповідальності за національним правом). Ліхтенштейн також закликав розглянути питання щодо встановлення того, як Римський Статут Міжнародного кримінального суду застосовується до кібервоєн [50].

Аналіз позицій різних держав демонструє зацікавленість у встановленні та конкретизації того, як певні норми застосовуються в кіберпросторі. В першу чергу, на увагу заслуговує інтерпретація *принципу суверенної рівності держав*. Одні держави ігнорують його або наголошують на його абстрактному характері, інші – розкривають його зміст у кіберконтексті.

Класичне визначення того, що представляє «суверенітет», було надано в арбітражному рішенні щодо острову Пальмас (США проти Нідерландів). Арбітр М. Губер вказав: «Суверенітет у відносинах між державами означає *незалежність*. Незалежність щодо частини земної кулі являє собою право здійснювати там, за винятком будь-якої іншої держави, функції держави. Розвиток національної організації держав протягом кількох останніх століть і, як наслідок, розвиток міжнародного права встановив цей принцип *виключної компетенції держави* щодо її власної території <…>» [56, с. 838].

У класичному варіанті нормативний зміст принципу суверенної рівності держав розкрито в Декларації про принципи міжнародного права 1970 р., а також Заключному акті НБСЄ від 1975 р. Відповідно до положень Декларації 1970 р., поняття «суверенна рівність» включає шість елементів:

1) держави є юридично рівними;

2) кожна держава користується правами, властивими повному суверенітету;

3) кожна держава зобов'язана поважати правосуб'єктність інших держав;

4) територіальна цілісність і політична незалежність держави є недоторканними;

5) кожна держава має право вільно вибирати й розвивати свої політичні, соціальні, економічні та культурні системи;

6) кожна держава зобов'язана виконувати добросовісно та в повному обсязі свої міжнародні зобов'язання, жити в мирі з іншими державами [1].

Найбільш послідовно та виважено, як видається, до інтерпретації принципу суверенітету підійшла Німеччина у своїй позиції щодо застосування міжнародного права в кіберпросторі від 5 березня 2021 року [43]. Пояснюється те, як Німеччина бачить порушення політичної незалежності (втручання в хід виборів), а також територіальної цілісності. Щодо останнього зазначається, що «кіберпростір не є детериторізованим простором» [43, с. 3]. У кіберпросторі відсутні традиційні кордони між державами, але, як зазначив Уряд Німеччини, «не існує незалежних «кіберкордонів», які не узгоджуються з фізичними кордонами держави, обмежуючи або нехтуючи територіальною сферою охоплення суверенітету». Тобто в межах своїх фізичних кордонів держави, з одного боку, мають право в повній мірі здійснювати свої повноваження щодо захисту кібернетичної діяльності осіб, які в ній беруть участь, а також кіберінфраструктури від втручання (включаючи кібер-втручання) з боку іноземних держав, з іншого – зобов'язані не дозволяти використовувати свою територію для дій, що суперечать правам інших держав [43, с. 3].

Німеччина також висловила підтримку правилу 4, запропонованому в Талліннському керівництві 2.0, яке говорить, що кібероперації, які атрибутуються державі та призвели до фізичних наслідків і шкоди на території іншої держави, є порушенням територіального суверенітету цієї держави [43, с. 4]. У контексті

цього дослідження важливим є і той факт, що, на думку Німеччини, кібероперарації в прцесі яких постраждали об'єкти критичної інфраструктури, можуть розглядатися як порушення територіальної цілісності. Поряд із критичною інфраструктурою згадуються і «компанії, що становлять особливий суспільний інтерес» [43, с. 4]. Логічно допустити, що таке формулювання викликане відсутністю загальноприйнятого поняття «критична інфраструктура». Це випливає з того, що позиція щодо цього принципу завершується твердженням про те, що кібероперації, спрямовані проти інших об'єктів чи компаній, що не кваліфікуються як «критична інфраструктура» або «компаній, що становлять особливий суспільний інтерес», також можуть призвести до порушення принципу територіальної цілісності як одного з конститутивних елементів принципу суверенної рівності [43, с. 4].

Досить схожою є позиція Франції, виражена в 2019 році. Згідно з нею, Франція наголошує, що здійснює свій суверенітет над інформаційними системами, розташованими на її території, а також вимагає слідування принципу *due diligence*, який випливає із суверенітету. Як зазнає французька сторона, держави мають: (1) використовувати кіберпростір відповідно до міжнародного права, зокрема, не використовувати третіх осіб (проксі) для вчинення дій, які за допомогою ІКТ порушують права інших держав, та (2) гарантувати, що їх територія не використовується для таких цілей, у тому числі недержавними суб'єктами [33, с. 6].

Що ж стосується принципу суверенітету, то зазначається, що він може бути порушений виключно державою, яка діє через офіційні органи, *de facto* органи, які виконують елементи урядових повноважень, або через приватних осіб, що діють за вказівками або під керівництвом чи контролем держави. Отже, виключається можливість розглядати спорадичні кібератаки автономних хакерів як порушення суверенітету держави. Призвести до порушення суверенітету можуть будь-які кібератаки, спрямовані проти цифрових систем Франції, або наслідки, що є результатом використання цифрових систем у межах території Франції [33, с. 7]. З цього робимо висновок, що підхід держави полягає в тому, що будь-яке несанкціоноване проникнення в інформаційно-комунікаційні системи Франції є порушенням цього принципу.

В офіційній позиції Чеської Республіки прослідковується досить чітка конкретизація того, що, на думку держави, є порушенням принципу суверенної рівності держав за умови, що

здійснені проти Чехії кібероперації атрибутуються іноземній державі. Справедливим буде зазначити, що Чехія відходить від підходу щодо необхідності «проникнення». Уже в першому пункті («A») виділяються кібероперації, що призводять до смерті або поранення людей або завдають значну фізичну шкоду. Нині Чехія – єдина держава, що пов'язує такі ситуації з принципом суверенної рівності держав. Як видається, таким чином держава хоче посилити свою позицію щодо того, що принцип суверенітету є «самостійним правам», повага до якого становить «самостійне зобов'язання» [19, с. 3]. Загалом кібероперації, що спричиняють смерть (чи поранення) людей або значний фізичний збиток кваліфікуються як застосування сили, якщо на це вказуватиме тест на «масштаб та наслідки» («*scale and effects*»), що є досить популярним серед держав та використовується задля порівняння кібератак із використанням сили у «фізичному» світі. Прикрим упущенням цієї заяви є те, що в позиції Чехії відсутні висновки щодо того, коли кібератаки кваліфікуються як застосування сили. Проте відсутність таких положень може розглядатись як свідчення загальної підтримки положень та висновків, до яких дійшли експерти урядової групи ООН та НАТО.

У другому пункті («B») згадуються кібероперації, що спричиняють пошкодження або порушують функціонування кіберінфраструктури чи іншої інфраструктури, що суттєво впливає на національну безпеку, економіку, охорону здоров'я чи навколишнє середовище. Кібероперації, що передбачають втручання в дані або надання послуг, необхідні для здійснення невід'ємних функцій уряду («C»), також розглядаються як порушення принципу суверенної рівності держав. У заяві наводиться приклад останніх кібероперацій: поширення програм-шантажистів, що шифрують комп'ютери, які використовуються урядом, коли воно призводить до затримки виплати пенсій [19, с. 3].

У розріз із позицією більшості держав та експертів Талліннського керівництва йде останній пункт («D»), який, на жаль, не супроводжується поясненням із боку Уряду Чехії. Так, кібероперації проти держави, державних органів чи агентів, що знаходяться в межах її території, включаючи міжнародні організації, є порушенням принципу суверенітету, якщо здійснюються органами іншої держави, що фізично присутні на території Чехії. Незрозуміло, чому акцент робиться на фізичній присутності агентів іноземної держави, а не на наслідках

кібероперації. Виходить, що кібероперації, які здійснюються з території держави-порушниці, незалежно від наслідків, не розглядаються як порушення суверенітету Чехів, в той час, як такі ж операції здійснювані з території останньої є порушенням суверенітету. Як видається, наслідки в обох випадках можуть бути ідентичними, але їх юридична кваліфікація – різна.

Цей пункт також змушує задуматись над кібероперaціями, здійснюваними недержавними акторами. У пункті «D» чітко зазначається «органами іншої держави» («*organ of another State*»), і під це формулювання однозначно не можуть підпадати проксі, які діють відповідно до вказівок або під контролем чи керівництвом держави. Враховуючи те, що цей пункт використовує формулювання з Талліннського керівництва щодо реалізації елементів внутрішнього суверенітету в кіберконтексті, можна зробити висновок, що виключення частини «та інших, чия поведінка атрибутується державі» [48, с. 19] із заяви Чехії було свідомим вибором.

У липні 2020 року свою офіційну позицію щодо застосування міжнародного права в кіберпросторі опублікував Генеральний штаб Збройних Сил Ісламської Республіки Іран [21]. Декларація складається лише з преамбули і чотирьох статей, які в досить стислому вигляді висвітлюють позицію Ірану з ключових питань: принципу суверенітету, заборони інтервенції та заборони використання сили. Відповідно до статті II(4) неправомірне проникнення в публічну чи приватну кіберструктуру може розглядатися як порушення суверенітету держави, що стала жертвою такого проникнення [21, ст. II(4)]. Цікаво, що в параграфі 5 цієї ж статі зазначається, що принцип суверенітету підпорядковується принципу рівності, і «суверенітет будь-якої держави не вище суверенітету інших держав. Отже, будь-які обмежувальні та заморожувальні заходи, включаючи санкції, є порушенням суверенітету незалежних держав через недотримання суверенітету держав-мішеней» [21, ст. II(5)]. Беззаперечним є те, що держави мають поважати суверенітет одна одної, але санкції не є порушенням суверенітету. Це лише форма дозволеного примусу, що є реакцією на міжнародно-протиправне діяння. Тому допускаємо, що така позиція держави є наслідком того, що Іран тривалий час знаходився під односторонніми та багатосторонніми санкціями.

Позицію Сполучених Штатів Америки щодо принципу суверенної рівності держав конкретизував Головний Радник

Департаменту оборони Пол Ней: «Щодо кібероперацій, які не є забороненим втручанням чи застосуванням сили, Департамент вважає, що відсутня загальна і послідовна практика держав, яка б випливала з усвідомлення юридичного обов'язку, що міжнародне звичаєве право загалом забороняє такі несанкціоновані кібероперації на території іншої держави» [25]. На думку Департаменту оборони США, публічне мовчання багатьох держав щодо низки публічно відомих кіберпроникнень в іноземні мережі виключає висновок про те, що держави об'єдналися навколо спільної думки про те, що існує міжнародна заборона на всі подібні операції (хоча й такі операції, як правило, забороняються національним правом та передбачають відповідне покарання). Також було зазначено, що, незважаючи на те, що США не розглядає «всі порушення суверенітету в кіберпросторі» як порушення міжнародного права, Департамент продовжить вивчення цього питання [25]. Отже, США відкидає підхід щодо того, що будь-яке несанкціоноване втручання (проникнення) є порушенням суверенітету, але залишає за собою змогу визначити «поріг» втручання для констатації порушення суверенітету.

Проте не можна погодитись із такою позицією США. Те, що багато держав мовчать щодо того, що стали жертвами несанкціонованого проникнення, не означає, що вони таким чином виражають позицію щодо відсутності юридичних зобов'язань, які випливають із принципу суверенної рівності держав. Як зазначала Комісія з міжнародного права, мовчання має значення в процесі формування звичаєвого права, коли воно має місце з боку постраждалої держави і за умови, що така держава могла відреагувати [28, с. 142–143]. Реальність кіберпростору полягає в складнощах здійснення фактичної атрибуції кібератак, тому більшість держав, не маючи необхідних технічних та людських ресурсів, просто не знаходять себе «в позиції для реагування». Що ж до тих, хто має необхідні можливості, то їх практика демонструє зворотне. Так, наприклад, у вербальній ноті до Генерального Секретаря ООН Постійне представництво Венесуели при ООН від імені держав МЕРКОСУР засудило акти шпигунства з боку США, підкресливши, що такі дії «є неприйнятною поведінкою, яка порушує наш *суверенітет* і шкодить нормальним відносинам між народами» [29]. Таким чином, Грузія, яка зазнала широкомасштабної кібератаки з боку Головного управління розвідки Російської Федерації у жовтні

2019 року, засудила таку атаку як таку, що «йде в розріз із міжнародними нормами і принципам, ще раз порушивши *суверенітет* Грузії» [54]. Вірогідність того, що кібератаки були здійснені ГРУ, відповідно до позиції Національного Центру Кібербезпеки Великобританії, який допомагав у питаннях атрибуції, становила більш ніж 95 відсотків [57]. Отже, коли постраждалі держави знаходяться «в позиції для реагування», тобто мають відповідні знання щодо того, хто стоїть за конкретною кібератакою, вони впевнено вдаються до політичної атрибуції поведінки іноземній державі та наголошують на порушенні принципу суверенної рівності, коли це дійсно доцільно.

Доволі однозначною і не узгодженою з власною практикою є позиція Великобританії, озвучена 23 травня 2018 року. Генеральний прокурор Джеремі Райт зазначив, що, попри фундаментальне значення суверенітету для міжнародно-правової системи, нині неможливо екстраполювати із цього загального принципу конкретне правило або додаткову заборону для кібердіяльності, окрім заборони втручання. Отже, «<…> позиція уряду Великобританії полягає в тому, що не існує такої норми в межах сучасного міжнародного права» [18, с. 402]. Нині лише Великобританія зайняла таку позицію публічно, в той час як інші держави, що висловились із цього приводу, характеризують суверенітет як принцип і норму міжнародного права (наприклад, Німеччина, Франція, Чехія, Фінляндія, Іран, Нідерланди, Болівія, Китай, Гватемала, Гайана, Нова Зеландія, Республіка Корея та Швейцарія, а також НАТО – за винятком Великобританії). Інтерес привертає Кіберстратегія Великобританії на 2016–2021, де наголошується, що кіберпростір є сферою, в якій «… ми мають захищати свої інтереси та суверенітет» [38, с. 47]. Таке твердження порушує досить важливе і частково схоластичне питання: чи дійсно треба захищати те, що, згідно з офіційною позицією уряду, не може бути порушеним?

Існує ще один «табір» держав, позиція яких не містить визначеності. Так, наприклад, у позиції Ізраїлю відсутнє роз'яснення того, чи принцип суверенної рівності розглядається як норма міжнародного права, що застосовується в кіберпросторі та передбачає відповідальність у разі її порушення. З одного боку, Ізраїль визнає те, що принцип суверенітету є «наріжним каменем міжнародного права та міжнародних відносин». З іншого боку, проводиться розмежування між «суверенітетом

як загальним поняття» (незалежність) та «територіальним суверенітетом, який є міжнародно-правовою нормою». Виходить, що позиція Ізраїлю зводиться до того, що, посилаючись на захист своєї політичної волі та автономії, держави «не обов'язково» посилаються на норму права. Свою позицію щодо принципу суверенітету представник Ізраїлю завершує твердження про злиття двох розумінь суверенітету та застереження про те, що «нам слід бути дуже обережними, роблячи юридичні висновки» [49, с. 402]. Таким чином, не зрозуміло, чи з ремарки щодо злиття можна зробити висновок про те, що Ізраїль не розглядатиме втручання чи узурпацію невід'ємних урядових функцій як порушення суверенітету постраждалої держави, як це роблять експерти Талліннського керівництва відповідно до правила 4.

Фінляндія у своїй позиції застерігає: «Погодитись із тим, що ворожа кібероперація, яка не досягає порогу забороненої інтервенції, не становить міжнародно-протиправне діяння, означає залишити такі операції поза рамками правового регулювання та позбавити постраждалу державу важливої можливості захищати свої права». Відповідно, фіни розгадають принцип суверенної рівності як основну норму міжнародного права, порушення якої є міжнародно-протиправним актом та тригером для притягнення держави до відповідальності, а також підтверджують свою переконаність у тому, що ця норма повністю застосовується в кіберпросторі [32, с. 3]. *B opinio juris* Фінляндії підкреслюється, що вирішення питання щодо того, чи несанкціоноване кіберпроникнення призведе до порушення суверенітету держави, яка стала об'єктом кібератаки, залежить від характеру такої атаки та її наслідків і підлягає оцінці в кожному конкретному випадку [32, с. 3].

Поряд із принципом суверенної рівності держав згадується заборона інтервенції. Згідно з правилом 66 Талліннського керівництва, «[д]ержава не може здійснювати інтервенцію (прим. – *анг*. «intervene»), в тому числі за допомогою кіберзасобів, у внутрішні або зовнішні справи іншої держави» [48, с. 312]. Враховуючи непослідовність у використанні таких термінів, як «інтервенція» та «втручання», підкреслимо, що йдеться саме про інтервенцію в розумінні інструментів, прийнятих у рамках ООН (зокрема, Декларації про заборону інтервенції та втручання у внутрішні справи держав) та Міжнародного Суду ООН. Держави

досить часто використовують поняття «втручання» замість поняття «інтервенція», але вони мають різне юридичне наповнення.

Під «втручанням» варто розуміти дії держав, позбавлені примусової сили, які вдираються у справи, що належать до суверенної прерогативи іншої держави. Натомість поняття «інтервенція» обмежується таким втручанням у справи іноземної держави, що має примусовий ефект [48, с. 313]. Як зазначає Міжнародний Суд ООН «інтервенція є неправомірною, коли вона передбачає використання методів примусу щодо такого вибору, який має залишатися вільним» [36, пар. 205]. Тобто обов'язковою характеристикою інтервенції є *примус*.

Що стосується принципу заборони інтервенції, то всі держави, які висловили свою офіційну позицію щодо застосування міжнародного права в кіберпросторі, зійшлись на тому, що цей звичаєвий принцип безсумнівно застосовується. Серед основних прикладів інтервенції, більшість держав згадували інтервенцію у виборчий процес, яка є втручанням у внутрішні справи держави та характеризується наявністю примусу (маніпулювання результатами голосування), втручання у фундаментальну діяльність парламенту або стабільність фінансових систем держав (Франція, США, Німеччина, Ізраїль, Австралія) [12, с. 5].

Як і у випадку з принципом суверенної рівності держав, принцип заборони інтервенції застосовується виключно у відносинах між державами. Отже, порушення цього принципу матиме місце, якщо за міжнародно-протиправними діями стояли агенти держави або приватні особи, дії яких атрибутуються державі відповідно до норм міжнародного права [48, с. 313–314].

У Декларації Ісламської Республіки Іран від липня 2020 року підтверджується звичаєвий характер принципу заборони інтервенції [21]. Під порушенням цього принципу в кіберпросторі держава розглядатиме ситуації політичного силового втручання (маніпулювання результатами виборів або формування громадської думки перед виборами як приклади *грубої інтервенції*), призупинення роботи вебсайтів із метою спровокувати внутрішню напруженість і конфлікти або масове надсилання повідомлень виборцям із ціллю впливу на результати [21, ст. III(1)]. У ст.. III окрема увага приділяється військовій інтервенції.

Під інтервенцією збройні сили також розглядатимуть всі ситуації, що передбачають застосування явних та «вишуканих» форм і прийомів примусу, повалення чи вираження обурення

(образ) задля «інтриг у політичному, соціальному чи економічному порядку» чи «дестабілізації урядів, що прагнуть лібералізації власних економічних, політичних та культурних систем» (форм контролю, що існують у таких системах). Втручання іноземців є незаконним відповідно до цієї статті щодо заборони інтервенції [21, ст. III(3)]. Така згадка про втручання іноземців без посилання на атрибуцію викликає низку питань, зокрема, чи це випадковість, а якщо ні, то яким чином поведінка приватних осіб може призвести до порушення одного з основних принципів міжнародного права, що застосовується у відносинах виключно між державами. У будь-якому разі відсутні офіційні пояснення з приводу вираженої позиції щодо втручання іноземців.

Доволі деталізованою є позиція Німеччини щодо принципу заборони інтервенції. Німеччина резервує за собою можливість розглядати поширення дезінформації через Інтернет як порушення, якщо воно здійснюється з ціллю підбурення до насильницьких політичних переворотів, заворушень та/або громадянських міжусобиць у чужій країні, тим самим суттєво перешкоджаючи нормальному проведенню виборів та підрахунку бюлетенів. На думку Уряду Німеччини, за своїми масштабами та наслідками така діяльність близька до підтримки повстанців, тому містить елемент примусу. У виборчому контексті інтервенцією у внутрішні справи держави також є виведення з ладу виборчої інфраструктури та технологій (зокрема електронних бюлетенів), «якщо це компрометує або навіть перешкоджає проведенню виборів, або якщо результати виборів тим самим суттєво модифіковані [43, с. 5].

Як уже зазначалося, офіційне висловлення позиції щодо застосування міжнародного права в кіберпросторі відіграє вагому роль у процесі формування практики держав та для подальшого притягнення до відповідальності. З одного боку, *opinio juris* у всіх своїх формах сприяє формуванню звичаєвих норм, оскільки є одним із двох елементів такої норми, а з іншого – у подальшому э важливим для практичної реалізації норм про відповідальність держав. Наприклад, 3 жовтня 2018 року Національний центр кібербезпеки (далі – НЦКБ) Великобританії на своєму офіційному сайті розмістив заяву про «невибіркові та безвідповідальні» кібератаки Головного розвідувального управління РФ. У заяві цитується позиція міністра закордонних

справ, в якій наголошується, що дії ГРУ «є безвідповідальними та невибірковими: вони намагаються зірвати та втрутитися у вибори в інших країнах; вони навіть готові завдати шкоди російським компаніям та громадянам Росії. Така модель поведінки демонструє їх бажання діяти, ігноруючи міжнародне право чи встановлені норми, діяти з почуттям безкарності та без наслідків». Наголошується на тому, що Великобританія разом із своїми союзниками готова реагувати на таку поведінку.

У заяві Національного центру кібербезпеки міститься перелік кібератак із відповідною оцінкою. Щодо чотирьох нових кібератак, які атрибутуються в цій заяві, зазначається наступне: «НЦКБ із високим ступенем впевненості (*high confidence*) встановив, що ГРУ майже напевно (*almost certainly*) відповідальне» [37]. Така атрибуція, очевидно, є значною перемогою в боротьбі за правомірне використання кіберпростору. Проте відсутність конкретизації того, які норми міжнародного права були «грубо» порушені з боку ГРУ, дещо нівелюють отримані результати.

Що стосується першої категорії атрибутованих кібератак, то саме з нею пов'язана найбільша складність щодо встановлення того, які норми міжнародного права були порушенні. Національний центр кібербезпеки випустив з уваги наявність збройного конфлікту в Україні, оскільки він ніде не згадується і відсутнє розмежування з іншими країнами, які не знаходяться в стані збройного конфлікту. Отже, робимо висновок про те, що йдеться не про порушення норм міжнародного гуманітарного права.

Шифрування жорстких дисків, що призвело до неоперабельності систем київського метро, одеського аеропорту, Російського центрального банку та ряду російських ЗМІ [37], які перераховуються в першій категорії, становить перманентну втрату функціональності. Відповідно до позиції деяких експертів Талліннського керівництва, серйозні наслідки (які не призвели до людських втрат чи знищення) можуть кваліфікуватися як порушення заборони незастосування сили. Проте, беручи до уваги позицію Великобританії, де було зазначено, що кваліфікуватися як порушення цього принципу будуть кібератаки проти ядерних реакторів та систем управляння повітряним рухом, що мали *летальний ефект*, можна з впевненістю відкинути імовірність того, що, на думку Великобританії, мало місце порушення цього принципу.

Що стосується принципу заборони інтервенції, досить складно (якщо можливо) встановити та довести намір Російської Федерації змінити прийняте Україною рішення, що входить у коло суверенних прерогатив щодо «свободи вибору власної політичної, соціальної, економічної та культурної системи». І ось тут починається найцікавіше, оскільки найбільш очікуваним є твердження про порушення принципу суверенної рівності держав. На противагу принципу незастосування сили чи заборони інтервенції, він не містить важко досяжних вимог (щодо наслідків та примусу відповідно), а також є очевидно порушеним. Виникає логічне запитання: чи може держава, яка не визнає, що з принципу суверенної рівності витікають юридичні зобов'язання, наполягати на його порушенні? Подібним чином, менше ніж через два тижні після публікації заяви на сайті Національного центру кібербезпеки міністр закордонних справ із питань кібербезпеки наголошує на відповідальності ГРУ за кібератаку NotPetya, підкреслюючи, що така кібератака «свідчить про тривалу зневагу *суверенітету* України», що проявляється в кібератаках проти уряду, енергетичного та фінансового секторів [51].

Зі свого боку, Україна нині не представила свою офіційну позицію щодо застосування міжнародного права в кіберпросторі. Проте із Стратегії кібербезпеки на 2021–2025 роки, затвердженої 14 травня 2021 року, випливає, що Україна підтримує тезу про повне застосування міжнародного права в кібердомені. Зокрема, в Стратегії зазначається, що «Україна продовжить активну участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також добровільних необов'язкових норм, правил та принципів відповідальної поведінки держави», а також «Україна буде сприяти подальшому дотриманню міжнародного права та стандартів у галузі прав людини» [8, с. 24–25].

Крім того, в Законі України «Про основні засади забезпечення кібербезпеки України» згадується реалізація «невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі» [7, ст. 7(5)]. Таким чином, виводячи приватне із загального, позиція України проявляється у повному застосуванні норм міжнародного права до кібератак. Це могло б означати те, що Україна вправі притягнути Російську Федерацію до відповідальності

за порушення суверенітету, але, з огляду на наявний збройний конфлікт, виникає питання, яке виходить за межі цього дослідження, – життєздатність заборони застосування сили та інтервенції у внутрішні справи, а також обов'язку поважати суверенітет між протиборчими воюючими сторонами.

У другій категорії кібератак, присвоєних Головному розвідувальному управлінню РФ, міститься кібератака проти Всесвітнього антидопінгового агентства (*далі* – ВАДА), в результаті якої були оприлюднені конфіденційні медичні справи ряду міжнародних спортсменів. ВАДА публічно заявила, що поширені дані було отримано шляхом зламу її антидопінгової системи адміністрування та управління. За прикладом своїх партнерів у Сполученому королівстві, міністерство закордонних справ Канади опублікувало заяву щодо відповідальності ГРУ [53]. Але, на відміну від заяви Великобританії, заява Канади, на території якої знаходиться штаб-квартира ВАДА, звучить досить узгоджено із внутрішньою позицією держави щодо застосування міжнародного права в кіберпросторі, оскільки Уряд Канади визнає принцип суверенної рівності держав нормою, що покладає на державу конкретні зобов'язання.

Аналогічним чином міністр оборони Нідерландів атрибутував кібероперацію ГРУ, спрямовану проти Організації із заборони хімічної зброї, яка базується в Нідерландах, зауваживши, що ця кібероперація ГРУ підриває міжнародне верховенство права [39]. На своєму офіційному вебсайті міністерство оборони досить детально описало те, як їм вдалося зірвати кібероперацію, яка могла б скомпрометувати висновки щодо Солсберівської атаки – отруєння Сергія Скрипаля речовинами нервово-паралітичної дії сімейства «Новичок». Служба розвідки та безпеки Нідерландів не тільки зірвала операцію ГРУ, але й випроводила їх із країни. Наявна інформація щодо їх переміщення напередодні та спорядження, яке активно використовувалося проти Бразилії, Швейцарії та Малайзії, дозволили з впевненістю встановити, що агенти ГРУ перебували в Нідерландах із ціллю виконати вказівки Уряду Російської Федерації, а не провести в Нідерландах вікенд.

Зауважимо, що в офіційному листі міністерства безпеки, міністерства іноземних справ та міністерства юстиції до Палати представників Нідерландів відсутнє посилання на те, що Російська Федерація порушила суверенітет Нідерландів [24]. Разом із тим, відповідно до Талліннського керівництва,

здійснення кібероперацій органами держави або особами, поведінка яких може атрибутуватися державі, що перебувають на території іншої держави, проти держави або утворених там осіб є порушення суверенітету цієї держави [48, с. 19]. У керівництві надається приклад, коли агент однієї держави використовує флеш-накопичувач USB для введення шкідливого програмного забезпечення в кіберінфраструктуру, розташовану в іншій державі. На думку експертів, такі дії порушують суверенітет держави [48, с. 19]. Оскільки агенти ГРУ намагалися зламати мережу Wi-Fi задля проникнення в мережу Організації із заборони хімічної зброї, така поведінка може розглядатися як проникнення в кіберструктуру Нідерландів, а отже, становить порушення суверенітету. Такий висновок випливає із спільної статті професора Університету Редінга Майкла Шмітта, що є основним розробником та автором Талліннського керівництва, та підполковника Джеффрі Біллера з Центру вивчення міжнародного права Військово-морського коледжу США [13].

Попри це, офіційна позиція Нідерландів полягає в тому, що поведінка ГРУ розцінюється як «підрив цілісності міжнародної організації». Також зазначається, що «як приймаюча країна, Нідерланди несуть особливу відповідальність за те, щоб міжнародні організації могли виконувати свої обов'язки як вільно, так і безпечно» [24]. Так, йдеться швидше про порушення норм дипломатичного права міжнародних організацій, ніж суверенітету. Хоча, зважаючи на те, що ВАДА не має власної кібернетичної інфраструктури, а використовує інфраструктуру держави, на території якої перебуває, вважаємо, що Нідерланди мали право кваліфікувати такі дії як порушення власного суверенітету.

Чимало можуть сказати кібератаки проти приватних осіб. Зокрема, підходи свідчить про те, що такі атаки не розглядаються як порушення норм міжнародного права. Так, наприклад, Великобританія та США не згадували про порушення норм міжнародного права щодо кампанії цільового фішингу, спрямованої проти приватних університетів, приватних компаній та неурядових організацій, яку ці держави атрибутували Ірану в березні 2018 року [52]. Фактично обидва уряди розглядали кіберпроникнення як злочинну діяльність відповідно до свого внутрішнього законодавства, тому США висунули звинувачення проти дев'яти іранців, які діяли в ім'я Корпусу вартових ісламської революції [41].

Такі заяви проводять чітку межу між діяльністю, яка впливає на здатність держави забезпечувати нормальне функціонування своїх «систем» (наприклад, функціонування парламенту; фінансового сектору; енергетики; транспорту), та діяльністю, спрямованою на забезпечення інтересів приватних осіб або приватних компаній. Принципу розмежування такої діяльності також слідує Європейський Союз, що випливає із прийнятого рішення про застосування обмежувальних заходів у випадку кібератак, що загрожують ЄС або його країнам-членам. У ст. 4, де міститься перелік кібератак, які розглядаються як загрози та підпадають під сферу дії рішення Ради ЄС, згадуються кібератаки. спрямовані проти: 1) критичної інфраструктури; 2) сфер, що забезпечують соціальну та/або економічну діяльність; 3) критичних функцій держави; 4) зберігання або обробки секретної інформації; 5) урядових груп реагування на надзвичайні ситуації [17, ст. 4]. Отже, кібератаки, що спрямовані проти приватних індивідів та компаній, виключаються – акцент робиться на цілих секторах.

У своїх заявах держави також згадують різні варіанти реагування на поведінку іншої держави в кіберпросторі, які міжнародне право їм надає. Варіанти, доступні в конкретному випадку, залежать від конкретних обставин. Різні форми *opinio juris* свідчать про те, що держави в разі потреби можуть вдаватися до реторсій, контрзаходів, самооборони та застосування принципу необхідності (як для підстави, що виправдовує загалом неправомірні дії).

Ст. 51 Статуту ООН гарантує невід'ємне право держав на самооборону. У своїх документах, що містять правову позицію, держави беззаперечно підтримують застосовність цього права в кіберконтексті. Щоправда, думки розходяться щодо того, коли його можна застосувати, та чи існує в кібердомені право на превентивну самооборону (*preventive self-defence*) чи самооборону на випередження *(pre-emptive self-defence*). Так, наприклад, у процесі аналізу позиції Великобританії стає очевидним, що держава не виключає використання права на самооборону на випередження, зазначаючи, що «кібероперації, що призводять до або *становлять безпосередню загрозу* смерті та знищення в масштабі, еквівалентному збройному нападу, породжуватимуть невід'ємне право вживати заходів для самооборони, як це визнано у статті 51 Статуту ООН» [18, с. 402]. Тобто така позиція, *inter alia*, є посиланням на тест, розроблений у справі про судно

«Caroline» (Великобританія проти США), де серед критеріїв на самозахист вказувались *необхідність, пропорційність і невідкладність.* Зазначимо, що підхід Міжнародного Суду ООН до вирішення цієї справи і нині знаходить критику серед противників концепції превентивної самооборони чи самооборони на випередження, які стверджують, що ці концепції суперечать ст. 51 Статуту ООН.

Що ж до інших держав, то їх позиція також не виключає можливість застосування концепції превентивної самооборони або самооборони на випередження. Так, наприклад, Франція висловлює рішучу позицію щодо застосування концепцій самооборони на випередження та/або колективного реагування (відповіді), що передбачається інструментами кібердипломатії ЄС, але не визнає превентивну самооборону [33, с. 9].

На увагу заслуговує позиція Нідерландів, яка містить чи не найжорсткіші умови, що мають бути виконані до того, як держава вдасться до реалізації свого права на самооборону. Так, Нідерланди встановили досить високий поріг для характеристики кібератаки як збройної атаки. Лише *серйозна, організована* кібератака *проти основних функцій* держави може кваліфікуватися як «збройна атака» у значенні ст. 51 Статуту ООН, якщо така операція могла привести або призвела до серйозних порушень функціонування держави або серйозних і довготривалих наслідків для стабільності держави [40, с. 23]. Для прикладу, кібератака, спрямована проти всієї фінансової системи, або така, що перешкоджає уряду виконувати важливі завдання (охорона навколишнього середовища, оподаткування), буде розцінюватися як збройний напад і, отже, наділяти державу правом на самооборону [40, с. 23].

З метою припинення міжнародно-протиправного діяння держави можуть вдаватися до реторсій. Загалом аналіз *opinio juris* свідчить про відсутність модифікації основних правил щодо їх застосування (Німеччина, Нідерланди, Австралія, Фінляндія). Держави мають право на власний розсуд вибирати вид реторсій, який, хоч і є недружнім, не становить порушення міжнародних зобов'язань. Окрім визнання дипломата персоною *non grata*, застосування економічних чи інших заходів впливу, держави також можуть обмежити чи закрити доступ до своєї цифрової інфраструктури (за умови відсутності договірних зобов'язань щодо надання спільного доступу на території двох країн).

На відміну від реторсій, певні процедурні правила щодо застосування контрзаходів, швидше за все, потребуватимуть коригування, як влучно підкреслив Уряд Фінляндії. Так, наприклад, атрибуція зловмисної кібероперації можлива лише після того, як вона завершена (адже на практиці потрібен час для розслідування кіберінциденту та ідентифікації відповідальних осіб), тоді як контрзаходи, як правило, слід вживати, поки триває міжнародно-протиправне діяння [32, с. 5]. Виділяється і позиція Німеччини щодо контрзаходів, яка нині єдина виразила публічну підтримку правилу 20 Талліннського керівництва у своїй офіційній позиції від березня 2021 року, зазначивши, що у разі порушень, які пов'язанні чи не пов'язані з кіберпростором, держави можуть вдаватися як до звичайних контрзаходів, так і до кіберконтрзаходів [43, с. 13].

Висновки

Аналіз наявних форм *opinio juris* (заяв, декларацій, воєнних стратегій, доктрин тощо), з одного боку, свідчить про загальний консенсус щодо застосування міжнародного права в кіберпросторі, а з іншого – про не завжди узгоджене розуміння того, *які* норми міжнародного права застосовуються до кібератак, *як* та *за яких умов*.

Зважаючи на постійне збільшення кібератак, зокрема проти об'єктів критичної інфраструктури, що забезпечують нормальне функціонування держави та суспільства, виникає гостра необхідність в узгодженні позицій із ключових питань. Лише нормативна чіткість офіційних позицій здатна посилити стійкість та мінімізувати ескалацію кібернетичних атак шляхом формування відповідної практики, а, отже, звичаєвих норм міжнародного права. Нині ж позиції держав іноді свідчать про формування певних політичних блоків держав, які намагаються пріоритезувати власні інтереси в питаннях, пов'язаних із кіберпростором. Тому на практиці виходить, що позиція держави щодо застосування конкретних принципів та норм міжнародного права в кіберпросторі визначається політичними інтересами держави (наприклад, позиція Росії та Китаю щодо неможливості застосування норм міжнародного гуманітарного права в кіберпросторі). Встановлено також, що практика в деяких випадках не узгоджена з офіційною позицією держави (офіційна позиція Великобританії щодо абстрактного характеру принципу суверенної рівності держав та

заяви про серйозні порушення міжнародного права в силу порушення суверенітету іноземних держав).

Попри те, що існують норми, застосування яких у кіберпросторі викликає низку дискусій серед держав (принцип суверенної рівності, заборони інтервенції та погрози чи застосування сили), уже нині можна говорити про формування певного консенсусу. Держави реагують на доктринальні розробки та обговорення експертів (ООН, НАТО тощо) та розробляють власні позиції, що надалі визначають їх практику. Це дає змогу не лише визначити очікування держав від поведінки в кіберпросторі, а й конкретизувати зміст нинішніх норм міжнародного права з метою їх застосування до кібератак та компенсувати відсутність договірних норм.

Список використаних джерел:

1. Декларація про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй : Декларація ООН від 24.10.1970., прийнята резолюцією ГА ООН 2625 (XXV). URL: https://zakon.rada.gov.ua/laws/show/995_569#Text.

2. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів : Протокол ООН від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text.

3. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности» A/70/174. 22 липня 2015. URL: https://undocs.org/pdf?symbol=en/A/70/174.

4. 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.

5. Климчук О. Кіберпростір як нова арена воєнних дій. *Актуальні проблеми управління інформаційною безпекою держави* : збірник мат-лів наук.-практ. конф., 22 берез. 2011 р.: [у 2 ч.]. Ч. 2. К. : Наук.-вид. відділ НА СБ України. 2011. С. 29–33.

6. Консультативное заключение Международного Суда ООН относительно законности угрозы ядерным оружием или его применения. 8 июля 1996 г. URL: https://www.icj-cij.org/public/files/advisory-opinions/advisory-opinions-1996-ru.pdf.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. 2163-VIII. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

8. Стратегія кібербезпеки України на 2021-2025 роки, затверджена Радою Національної безпеки та оборони України 14 травня 2021 року. *Безпечний кіберпростір – запорука успішного розвитку країни*. 27 с. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

9. Циверенко Г. Фактичні підстави для виникнення міжнародно-правової відповідальності. *Актуальні проблеми держави і права*. 2014. С. 152–157.

10. Шеломенцев В. Поняття та сутність кібернетичної атаки. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25. С. 337–344.

11. 1st Meeting of the first substantive session of the Open-Ended Working Group (OEWG). *DIGWATCH website*. URL: https://dig.watch/resources/1st-meeting-first-substantive-session-open-ended-working-group-oewg.

12. 2019 International Law Supplement. Annex B: Australia`s position on how international law applies to State conduct in cyberspace. 2019. URL: https://www.internationalcybertech.gov.au/our-work/annexes/annex-b.

13. Biller J., Schmitt M. Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences. *EJIL: Talk!* URL: https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/.

14. Brian L.D. Customary international law: a new theory with practical applications. Cambridge University Press. 2010. 795 p.

15. Buttigieg J. The common heritage of mankind: from the law of the sea to the human genome and cyberspace*. Symposia Melitensia*. 2012, Vol. 8, p. 81–92.

16. Corn G. Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace. *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare.* 2018. 71 p. URL: https://ssrn.com/abstract=3089071.

17. Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States. 14 May 2019. URL: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf.

18. Cyber and International Law in the 21st Century, From Attorney General`s Office and The Rt Hon Jeremy Wright QC MP. Published 23 May 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

19. Czech Republic, Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace Director of Cybersecurity Department, dated 11 February 2020. 4 p.

20. Declaration by Miguel Rodriguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York, June 23, 2017. URL: https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.

21. Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace. Armed Forces Cyberspace Center. July, 2020. URL: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

22. Digital Around the World. *Datareportal website*. 7 July 2021. URL: https://datareportal.com/global-digital-overview.

23. Dinstein Y. The Conduct of Hostilities under the Law of International Armed Conflict. Cambridge University Press. 2004. 341 p.

24. Disruption of a GRU cyber operation in The Hague. Letter of 4 October 2018 from the Minister of Defence Ank Bijleveld-Schouten, Minister of Foreign Affairs Stef Blok and Minister of Justice and Security Ferdinand Grapperhaus, to the House of Representatives, regarding the disruption of a GRU cyber operation in The Hague. URL: https://english.defensie.nl/downloads/parliamentary-documents/2018/10/04/disruption-of-a-gru-cyber-operation-in-the-hague.

25. DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, March 2, 2020, remarks By Hon. Paul C. Ney, Jr. URL: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

26. Dörmann K. Applicability of the Additional Protocols to Computer Network Attacks. *ICRC website*. 2004. URL: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

27. 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.

28. Draft conclusions on identification of customary international law, with commentaries. 2018. https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf.

29. General Assembly, Note verbale dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations addressed to the Secretary-General. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/411/07/PDF/N1341107.pdf?OpenElement.

30. Gioe D., Goodman M., Wanless A. Rebalancing cybersecurity imperatives: patching the social layer. *Journal of Cyber Policy*. 2019. № 4(1). P. 117–137.

31. ICTY, *Prosecutor v. Dusko Tadic´*, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995.

32. International law and cyberspace, *Finland's national positions*, 2020. 8 p. URL: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.

33. International Law applied to cyber operations. French official position. 2019. URL: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

34. Korzak E. UN GGE on Cybersecurity: The End of an Era? *The Diplomat*. 31 July 2017. URL: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

35. Lohrmann D., Lohrmann D. 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic. *Government technology website*. URL: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

36. 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.

37. National Cyber Security Centre, *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Exposed*. 3 October 2018. URL: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

38. National Cyber Security Strategy 2016-2021. *HM Government website*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

39. Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW. *Government of the Netherlands website.* 4 October 2018. URL: https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.

40. Netherlands` Cyber Warfare. No 77, AIV/ No 22, CAVV. Dec. 2011. 46 p. URL: https://www.advisorycouncilinternationalaffairs.nl/binaries/advisorycouncilinternationalaffairs/documents/publications/2011/12/16/cyber-warfare/Cyber_Warfare_AIV-Advisory-report-77_CAVV-Advisory-report-22_ENG_201112.pdf.

41. Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps. *US Department of Justice website*. 2018. URL: https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic.

42. North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3. URL: http://www.icj-cij.org/files/case-related/51/051-19690220-JUD-01-00-EN.pdf.

43. On the Application of International Law in Cyberspace Position Paper. March 2021. The Federal Government of German Federation. 17 p. URL: https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf.

44. Owes W.O., Kenneth W.D., Herbert S.L. Committee on Offensive Information Warfare, National Research Council; The Basic Technology of Cyberattack. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. 2009. 390 p.

45. Russell A. The Logic Layer. In Strategic A2/AD in Cyberspace (pp. 40-52). Cambridge: Cambridge University Press. 2017. 108 p.

46. Sassoli M. International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare. Edward Elgar Publishing. 720 p.

47. Schmitt M. Cyber operations and the jus in bello: key issues. *Naval War College International Law Studies*. Vol. 87. 2011. P. 89–110.

48. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. 2017. 598 p.

49. Schöndorf R. Practical Issues Concerning the Application of International Law to Cyber Operations. International Law Studies. *International Law Studies Series*. № 97. 2021. 395–406. URL:

https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2957&context=ils.

50. Statement by Georg Sparser, Deputy Permanent Representative Permanent Mission of the Principality of Liechtenstein to the UN. 2020. URL: https://ccdcoe.org/uploads/2020/04/Statement-on-International-Law-by-Liechtenstein-at-2nd-session-of-OEWG.pdf.

51. Statement of Foreign Office Minister, Lord Ahmad. *Foreign Office Minister condemns Russia for NotPetya attacks*. 15 October 2018. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

52. Statement of Foreign Office Minister, Lord Ahmad. F*oreign Office Minister condemns criminal actors based in Iran for cyber-attacks against UK universities*. 2018. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-criminal-actors-based-in-iran-for-cyber-attacks-against-ukuniversities.

53. Statement of Global Affairs Canada*. Canada identifies malicious cyber-activity by Russia*. 2018. URL: https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html.

54. Statement of the Ministry of Foreign Affairs of Georgia. 2019. URL: https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5.

55. Strategy and governance. *NATO Cooperative Cyber Defence Centre of Excellence website*. URL: https://ccdcoe.org/library/strategy-and-governance/?category=intl-law-statements.

56. The Island of Palmas Case (or Miangas). USA v. The Netherlands. Award of The Tribunal. Permenent Court of Arbitration. Reports of International Arbitral Awards. Volume. II pp. 829–871. 4 April 1928. URL: https://legal.un.org/riaa/cases/vol_II/829-871.pdf.

57. UK condemns Russia`s GRU over Georgia cyber-attacks, Press release Foreign & Commonwealth Office, National Cyber Security Centre, and The Rt Hon Dominic Raab MP, published on 20 February 2020. *UK Government website*. URL: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

58. Woltag J.C. Cyber Warfare. 2015. *Max Planck Encyclopedias of Public International Law*. URL: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e280?rskey=eCCfoY&result=7&prd=EPIL&print.