

Міністерство освіти і науки України
Національний університет «Києво-Могилянська Академія»
Факультет правничих наук
Кафедра міжнародного та європейського права

МАГІСТЕРСЬКА РОБОТА

освітній ступінь – магістр

на тему: «**Відповідальність держав за здійснення кібератак: механізми
міжнародного права та сучасні виклики**»

«State responsibility for cyber attacks: international law framework and contemporary
challenges»

Виконала:

Студентка 2 року навчання
магістерської програми спеціальності 081
«Право»
Карпенко Анастасія Олегівна

Керівник магістерської роботи:

Коваль Дмитро Олександрович, кандидат
юридичних наук, доцент

Рецензент _____

Магістерська робота захищена з оцінкою

«_____» Секретар ЕК

_____ «____»

_____ 2021 рік

A. Koz

Київ – 2021

Декларація академічної доброчесності

Я, Карпенко Анастасія Олександрівна, студентка
2 року навчання факультету правничих наук
спеціальність „Право“
адреса електронної пошти: anastasiia12.karpenko@gmail.com
• підтверджую, що написана мною магістерська робота
на тему „Відповідальність держав за здійснення
кібератак: механізми міжнародного права та сучасні
виклики“ відповідає вимогам академічної доброче-
сності та не містить порушень, передбачених при-
писами 3.1.1 – 3.1.6. Положення про академічну до-
бросовісність здобувачів НаУКіП № від 07.03.2018 року,
зі змістом якої ознайомена;
• підтверджую, що надана мною електронна версія
роботи є остаточною і готовою до перевірки;
• згодна на перевірку моєї роботи на відповідність
критеріям академічної доброчесності, у тому-ж числі
спосіб, у тому числі порівняння змісту роботи
та формулювання звіту подібності за допомогою
електронної системи Plagiat;,
• даю згоду на архівування моєї роботи в репози-
таріях та баз даних університету для порівняння
з майбутніми роботами.

12 травня 2021 р. А. Карп Карпенко А.О.

ЗМІСТ

| | |
|---|-----------|
| ВСТУП..... | 4 |
| РОЗДІЛ 1..... | 9 |
| ПОНЯТТЯ І СУТНІСТЬ КІБЕРАТАК У МІЖНАРОДНО-ПРАВОВОМУ АСПЕКТІ | 9 |
| 1.1. Підходи до визначення поняття та суті кібератак | 9 |
| 1.1.1. Наукові підходи до визначення поняття «кібератака» | 9 |
| 1.1.2. Підходи до визначення поняття «кібератака» міжнародними організаціями | 12 |
| 1.1.3. Підходи держав до визначення поняття «кібер-атака»..... | 13 |
| 1.2. Основні цілі здійснення кібератак..... | 17 |
| 1.2.1. Здійснення кібератак з метою втручання у політичні питання держави | 25 |
| 1.3. Діяльність міжнародних організацій з протидії кібератак..... | 27 |
| 1.3.1. НАТО | 27 |
| 1.3.2. Рада Європи..... | 29 |
| 1.3.3. Організація Американських держав..... | 31 |
| 1.4. Висновки до Розділу 1..... | 31 |
| РОЗДІЛ 2..... | 34 |
| МЕХАНІЗМИ МІЖНАРОДНОГО ПРАВА ДЛЯ ПРИТЯГНЕННЯ ДЕРЖАВ ДО ВІДПОВІДАЛЬНОСТІ | 34 |
| 2.1. Належність поведінки держави..... | 34 |
| 2.1.1. Належність поведінки представників органів держави | 34 |
| 2.1.2. Здійснення контролю над поведінкою приватних суб'єктів..... | 37 |
| 2.1.3. Визнання державою поведінки приватних осіб як власної..... | 40 |
| 2.2. Кібератака у якості винного діяння держави..... | 41 |
| 2.2.1. Незаконне втручання у внутрішні справи держави | 41 |
| 2.2.2. Кібератака як застосування сили | 46 |
| 2.2.3. Кібератаки як результат порушення принципу належної обачності | 52 |
| 2.3. Висновки до Розділу 2..... | 56 |
| РОЗДІЛ 3..... | 58 |

| | |
|--|-----------|
| СУЧАСНІ ВИКЛИКИ | 58 |
| 3.1. Можливі відповіді уражених держав на кібератаки | 58 |
| 3.1.1. Застосування права на самооборону | 58 |
| 3.1.2. Застосування санкцій ураженими державами | 62 |
| 3.2. Розроблення єдиного міжнародного акту, що регулює поведінку держав у кіберпросторі | 64 |
| 3.3. Вплив пандемії Covid-19 на кібербезпеку держав | 70 |
| 3.4. Висновки до Розділу 3 | 71 |
| ВИСНОВКИ | 74 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ | 77 |

ВСТУП

Актуальність дослідження. На сьогодні майже усі сфери життя людини перейшли у площину кіберпростору. Функціонування як комерційних, так і державних установ тією чи іншою мірою залежить від комп'ютерних систем та мережі Інтернет. Окрім цього, пандемія Covid-19 призвела до посилення дистанційної комунікації за допомогою Інтернет мережі. З одного боку, використання нових технологій дозволило державам підвищити ефективність та доступність роботи підприємств та установ. З іншого боку, така залежність від функціонування Інтернет-мережі активно використовується іншими недобросовісними державами, що мають на меті завдати шкоди діяльності об'єктів критичної інфраструктури іншої держави. Один з таких випадків мав місце в Україні, коли внаслідок кібератак було пошкоджено функціонування електричних мереж на території Західної України та місті Києві. Окрім України, кібератаки були спрямовані на пошкодження функціонування об'єктів критичної інфраструктури Сполучених Штатів Америки, Естонії, Грузії, Ірану.

Дискусійність теми полягає у тому, що на сьогодні не було розроблено єдиного підходу до кваліфікації кібератак з точки зору міжнародного права. Наразі єдиного акту, який би встановлював права і обов'язки держав у кіберпросторі не було розроблено. У зв'язку з цим, науковці та уряди різних країн пропонують власні підходи щодо застосування існуючих норм та принципів міжнародного права до кібератак. Проте, сформовані концепції міжнародного права не враховують всіх тих особливостей, що притаманні протиправним діям, здійсненими за допомогою інформаційно-телекомунікаційних систем. Зокрема, центральним питанням кібератак є їх здійснення не безпосередньо представниками держав, а за допомогою недержавних суб'єктів. Проте, Міжнародний суд справедливості ООН встановлює досить високі стандарти доведення належності поведінки приватних суб'єктів державі.

Виходячи з реальних випадків здійснення кібератак, починаючи з 2008 року в Естонії і до сьогодні, жодну державу не було визнано відповідальною за здійснення кібератак.

У зв'язку з цим, існує необхідність вироблення уніфікованого підходу до кваліфікації діянь держав у кіберпросторі, який базувався б на вже існуючих усталених нормах та принципах міжнародного права. Такий підхід має дозволити ефективно реагувати на кібератаки у міжнародному просторі та притягувати до відповідальності винні держави.

Мета і завдання роботи. Метою даної роботи є здійснення системного аналізу норм та принципів міжнародного права, які дозволяють визначити кібератаки у якості протиправної поведінки, що призводить до відповідальності держав, а також визначення існуючих проблем та викликів, які виникають під час притягнення держав до відповідальності.

Для реалізації поставленої мети необхідно вирішити наступні завдання:

- 1) проаналізувати наукові підходи до визначення поняття «кібератака»;
- 2) проаналізувати підходи держав до визначення поняття «кібератака»;
- 3) проаналізувати підходи міжнародних організацій до визначення поняття «кібератака»;
- 4) здійснити аналіз основних цілей здійснення кібератак на прикладах Естонії, Грузії, США, Ірані та України;
- 5) дослідити діяльність міжнародних організацій, пов'язану з протидією кібератак;
- 6) проаналізувати принцип заборони втручання з точки зору його застосування до кібератак;
- 7) проаналізувати принцип заборони застосування сили з точки зору його застосування до кібератак;
- 8) проаналізувати принцип належної обачності з точки зору його застосування до кібератак;
- 9) здійснити аналіз підстав для визнання належності поведінки приватних суб'єктів державі;

- 10) визначити можливість застосування концепції де факто органу для визнання належності поведінки приватних суб'єктів державі під час здійснення кібератак;
- 11) порівняти концепції ефективного контролю та загального контролю для визнання належності поведінки приватних суб'єктів державі під час здійснення кібератак;
- 12) дослідити правову природу визнання державою поведінки приватних суб'єктів як своєї власної;
- 13) дослідити правову природу суверенітету держави у кіберпросторі;
- 14) проаналізувати можливість застосування державою контрзаходів у кіберпросторі; та
- 15) визначити вплив пандемії Covid-19 на кібербезпеку держав.

Об'єктом дослідження є інститут міжнародної відповідальності держав за здійснення кібератак, спрямованих проти інших держав.

Предметом дослідження є норми та принципи міжнародного права, що застосовуються при визначенні відповідальності держав за здійснення кібератак.

Методи дослідження. Для досягнення зазначеної мети та реалізації поставлених завдань було використано наступні методи:

порівняльно-правовий метод надав можливість зробити порівняльний аналіз регулювання кібератак у різних країнах та міжнародних організаціях;

метод аналізу допоміг визначити окремі норми міжнародного права, що можуть застосовуватись до регулювання поведінки держав, а також приватних суб'єктів у кіберпросторі. Разом з методом синтезу він дозволив визначити зв'язок між відповідними правовими нормами, зокрема взаємозв'язок норм, що визначають підстави належності поведінки приватних суб'єктів державі та норм, що визначають кібератаки протиправним діянням;

аксіологічний метод дозволив дослідити питання поведінки приватних осіб, а також посадових осіб держави. Зокрема, при вирішенні питання належності дій приватних суб'єктів державі, застосування механізму здійснення державою

контролю та втручання у кібератаку, ступінь визнання дій приватних осіб як власних;

системно-структурний метод дозволив визначити ієрархію існуючих правових інструментів та їх юридичну силу. Цей метод дав змогу виявити наявність норм та правил, що мають обов'язкову юридичну силу (наприклад, Статут ООН) і, так зване, м'яке право, що має рекомендаційний характер і не може бути самим по собі підставою для притягнення до відповідальності, проте є гнучким правовим інструментом, який більш детально розкриває сутність тих чи інших приписів і оперативно реагує на сучасні виклики міжнародному праву;

функціональний метод дозволив проаналізувати правові норми, правила і стандарти у їх сукупності, що функціонують узгоджено і взаємопов'язано. Це, зокрема, дозволить на практиці виробити єдину позицію для доведення відповідальності держави;

порівняльно-історичний метод дозволив проаналізувати рівень правового регулювання заборони кібератак і відповідальності за них у різні часові періоди, починаючи з кінця XX ст. і до сьогодні;

біхевіористський метод дав змогу визначити мотив, мету, намір держави брати участь у кібератаках, що є підставою для визнання такої поведінки як протиправної, зважаючи на наявність суб'єктивного чинника.

Теоретичну основу роботи склали наукові праці таких дослідників, як: М.А. Шаап, У. Хетеуей, К. Веглінські, Д. Сілвер, П. Шакарян, М. Шмітт, Д. Сілвер, Н. Попеску, М. Чен, М. Ваксман, Ф. Пул, М. Шмітт, Л. Табанський, Дж. Вігген, Т. МакКензі, С. Герцог, Л. Чіркоп.

Практичне значення дослідження полягає в тому, що теоретичні напрацювання та рекомендації, надані в цій магістерській роботі, можуть бути використані в:

науковій сфері - сформульовані висновки у дослідженні можуть бути використані у подальших дослідженнях, привідповідальності держав за здійснення кібератак;

правозастосовній сфері - висновки і рекомендації можуть бути використані для розроблення міжнародних актів, що регулюють поведінку держав у кіберпросторі.

Структура роботи. Магістерська робота складається зі вступу, трьох розділів, одинадцяти підрозділів, дев'ятнадцяти частин підрозділів, висновків за кожним розділом, загальних висновків та списку використаних джерел. Загальний обсяг дослідження - 97 сторінок, у тому числі список використаних джерел (145 найменувань) складає 20 сторінок.

РОЗДІЛ 1.

ПОНЯТТЯ І СУТНІСТЬ КІБЕРАТАК У МІЖНАРОДНО-ПРАВОВОМУ АСПЕКТІ

Кібератаки стали цілком закономірним наслідком світового поширення комп'ютерних технологій та мережі Інтернет. Як зазначає науковець Конрад Веглінські, піднімати це питання на міжнародний рівень почали ще у 90-х роках минулого століття, [1, с. 79]¹. Проте лише після здійснення державами кібератак у ХХІ столітті міжнародна спільнота усвідомила усю серйозність проблеми. Кібератака постала перед рядом країн у якості нової загрози їх національній безпеці. Тому вважаємо за необхідне дослідити правову природу кібератак. Оскільки наразі не розроблено єдиного міжнародного акту, який би регулював права і обов'язки держав у кіберпросторі, вважаємо за доцільне дослідити поняття і сутність кібератак, розроблені науковою доктриною, державами та організаціями. Також окрему увагу у цьому розділі буде приділено цілям, що переслідуються державами при здійсненні кібератак. Насамкінець, вважаємо за необхідне проаналізувати діяльність міжнародних організацій, пов'язану з протидією кібератакам.

1.1. Підходи до визначення поняття та суті кібератак

1.1.1. Наукові підходи до визначення поняття «кібератака»

На сьогодні не було розроблено єдиного підходу до визначення поняття кібератака, а також суміжних із ним - «кіберпростір» та «кібервійна» [2, с. 125-126]. Відповідно до статті 38 Статуту Міжнародного Суду справедливості ООН, доктрина є одним із джерел міжнародного права [3]. У зв'язку з цим, варто звернути

¹ Тут і далі переклад зроблено мною, Карпенко А.О.

увагу на доктрину, яка наразі пропонує власні підходи до визначення суті кібератак з точки зору міжнародного права.

Зокрема, Ліор Табанський приділяє велику увагу поняттю кіберпростір і саме через нього аналізує природу кібератак. Вчений виділяє три шари кіберпростору: фізичний – сюди входять об'єкти, що мають певні фізичні виміри (процесори, кабелі, накопичувальні пристрої тощо); програмне забезпечення – запрограмовані людиною системи команд щодо вчинення певних дій; інформація, що зберігається на пристроях [4, с. 77]. У своїй роботі автор зазначає, що кібератака спрямована не завдати не кінетичну шкоду фізичним об'єктам кіберпростору, а вплинути на програмне забезпечення [4, с. 81].

Тімосі М. МакКензі аналізує у своїй роботі підхід до визначення «кібератака», наведений у Таллінській книзі і зазначає, що «деякі дії, які відносяться до «руйнації» або «агресивного інциденту» можуть також досягти рівня кібератаки, залежно від економічного впливу руйнації» [5, с. 4]. Тімосі М. МакКензі наводить також своє визначення кібератаки: «навмисне пошкодження, руйнування або псування критичних особистих систем або критичних/некритичних урядових систем або будь-яка кібердіяльність, що заподіює значні фінансові втрати приватної компанії США або урядового органу/агенції США або заподіює смерть, руйнування або серйозне ушкодження» [5, с. 4-5].

Деякі науковці, як, наприклад, Уна Хетеуей у співавторстві з іншими науковцями, критикують широке визначення поняття «кібератака» і вважають за необхідне розмежовувати його з іншими суміжними категоріями. Так, у спільній праці Уни Хетеуей з іншими авторами, основною характеристикою кібератак є пошкодження функціонування комп'ютерних мереж в політичних цілях [6, с. 881]. У своїй роботі автори обґрунтовують власне запропоноване визначення. Так, вони зазначають, що кібератака може включати лише активну поведінку, наприклад, хакерство, або «зараження», її головною метою є порушення функціонування комп'ютерної мережі [6, с. 826-828]. Стосовно порушення функціонування комп'ютерної мережі автори зазначають, що кібератака відрізняється від

кібершпіонажу, чи кіберексплуатації тим, що суб'єкт впливає на функціонування системи або шляхом завдання шкоди або ж шляхом додавання шкідливої інформації, або ж копіюванням даних [6, с. 830]. Також автори зазначають, що критерієм для розрізнення кібератак та кіберзлочину є саме політична спрямованість перших [6, с. 830]. Так, кібератака, вчинена державним суб'єктом обов'язково стосується національної безпеки, а ось кіберзлочин, вчинений недержавним суб'єктом, буде вважатись лише тоді кібератакою, якщо спрямований на порушення політичної або національної безпеки [6, с. 830]. Загалом, автори розрізняють категорії «кібератака», «кіберзлочин» та «кібервійна». Так, кібератака передбачає можливість залучення як державних, так і недержавних суб'єктів, її метою є порушення функціонування комп'ютерної мережі для порушення політичної або національної безпеки держави [6, с. 833]. Обов'язковими ознаками кіберзлочину є порушення кримінального законодавства, а також можливість його здійснення лише недержавними суб'єктами [6, с. 833]. Кібервійна дещо перетинається з поняттям кібератака, оскільки її метою також є порушення функціонування комп'ютерної мережі для порушення політичної або національної безпеки держави, проте ще однією її характерною ознакою є ступінь спричиненої шкоди, який має дорівнювати ступеню шкоди внаслідок збройної атаки або ж це може бути діянням, що було здійснене в ході воєнного конфлікту [6, с. 833].

Як зазначають Метью Кохен та Чарльз Фрайліх:

політично зумовлені кібератаки мають на меті надати стратегічну, дипломатичну, економічну чи військову перевагу над протилежною стороною і включають спроби знищення критичної військової, урядової, або ж цивільної мережі, шпіонаж, а також спроби вплинути на системи за допомогою шкідливого програмного забезпечення для подальшого використання [7, с. 3].

Шаап у своїй праці аналізує підходи державних органів США, зокрема, Директиву Міністерства оборони щодо політики повітряних сил, до визначення поняття кібероперація [2, с. 126-127]. Зазначаючи, що військові операції у кіберпросторі можуть розглядатись у якості війни, вчений визначає поняття кібервійськові операції як: «використання мережевих засобів держави з метою порушення, відмови, погіршення, маніпулювання, чи знищення інформації, що

міститься на комп'ютерах та безпосередньо мережах іншої держави» [2, с. 127]. Також вчений виокремлює окремі типи кібератак: відмова у доступі до сервісу, розподілена атака на відмову в обслуговуванні, шкідливе програмне забезпечення; логічна бомба; IP спуфінг; цифрова маніпуляція [2, с. 134-137].

Крістіан Пейн та Лорейн Фінлей визначають кібератаку як діяння, під час яких «держави використовують комп'ютери та інформаційні технології як основні механізми руйнівного впливу на інтереси іншої держави». [8, с. 537]

Таким чином, на сьогодні науковці мають відносно схожі підходи до визначення поняття «кібератака». На основі наведених підходів можна навести таке визначення кібератак: це втручання у об'єкти комп'ютерної мережі, здійснене державами або приватними особами з політичними мотивами із використанням шкідливих інформаційно-телекомунікаційних засобів, спрямовані на ураження або втручання у функціонування таких комп'ютерних мереж.

1.1.2. Підходи до визначення поняття «кібератака» міжнародними організаціями

На сьогодні невелика кількість міжнародних та регіональних організацій здійснила спроби охарактеризувати поняття «кібератака». Не зважаючи на це, варто наголосити на основному наразі керівництві з відносин у кіберпросторі, а саме, Таллінській книзі з міжнародного права, що застосовується до кібервійни, розробленою Міжнародною групою експертів на запрошення Кооперативного Центру передового досвіду з кіберзахисту НАТО. У Таллінській книзі міжнародна група експертів викладає власні підходи до кваліфікації тих чи інших діянь держав у кіберпросторі. Окрім цього, Таллінська книга наводить наступне визначення кібератак: «це кібероперація, як наступальна, так і оборонна, яка, як обґрунтовано очікується, може спричинити поранення або смерть людей або пошкодження або знищення предметів» [9, с. 106]. Також група експертів зазначає, що здійснення кібератак може причинити шкоду не лише кіберсистемам, а також людині, фізичним об'єктам і навіть інформації [9, с. 107-108]. Глосарій термінів НАТО

визначає комп'ютерну мережеву атаку як: «діяння, спрямоване на перешкоджання, відмову, руйнування або знищення інформації резидента на комп'ютері та/або комп'ютерній мережі, або самих комп'ютера та/або комп'ютерної мережі» [10].

Окрім цього. у Європейському Союзі було прийнято Регламент (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з кібербезпеки та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та про скасування Регламенту (ЄС) № 526/2013 (так званий «Акт з кібербезпеки») [11]. Акт з кібербезпеки прямо не визначає поняття «кібератака», проте наводить дефініцію «кіберзагрози». Відповідно до статті 2(6) Акту з кібербезпеки ЄС, кіберзагроза означає «будь-який можливий наслідок, подію, чи діяння, що може зашкодити, перешкоджати чи будь-яким чином мати вплив на мережу та інформаційні системи, користувачів таких систем чи інших осіб» [11].

Також варто зауважити про Конвенцію про кіберзлочинність, розроблену Радою Європи та прийнятою у 2001 році [12]. Конвенція зосереджується не на самій суті кібератак, а на окремих видах злочинів, вчинених приватними суб'єктами. Оскільки Конвенція з кіберзлочинності, не наводить визначення «кібератака», то вважаємо за доцільне не зупинятись детально на її аналізі у цьому підрозділі.

1.1.3. Підходи держав до визначення поняття «кібер-атака»

Ряд кібер-атак, здійснених, зокрема, проти Естонії, США, Грузії, України та Ірану, змусив інші країни переглянути законодавче врегулювання відповідальності за здійснення протиправних діянь у кіберпросторі. Окрім цього, Генеральна Асамблея ООН у своїх Резолюціях неодноразово закликала країни до співпраці у сфері кібербезпеки [13; 14]. У зв'язку з цим, держави почали активно приймати стратегії з кібербезпеки, в яких, зокрема надається характеристика кібератак і визначаються її характерні ознаки. Тому вважаємо за необхідне проаналізувати стратегії з кібербезпеки, розроблені окремими країнами.

У Національній стратегії з кібербезпеки Іспанії зазначається, що кіберзлочин визначається найбільш важливим питанням безпеки громадян, оскільки внаслідок його здійснення спричиняється значна шкода тисячам інституцій та громадянам [15, с. 25]. При цьому, кіберзлочин визначається як «незаконні діяння у кіберпросторі, що націлені на окремі елементи, комп'ютерні системи або будь-яку іншу законну власність, не зважаючи на те, коли вони сплановані, їх розвиток і здійснення визначаються використанням технологічних інструментів...» [15, с. 25-26].

У Національній стратегії кібербезпеки Німеччини не міститься поняття кібератака. Проте робиться акцент на шкоді, спричиненій кібератаками і характеристиці суб'єктів атак. Так, у Стратегії зазначено, що кібератаки можуть впливати не лише на сам кіберпростір, а й спричиняти економічну, політичну, адміністративну, військову, фінансову складові функціонування держави [16, с. 5]. Самі ж суб'єкти зазвичай мають кримінальний, екстремістський/терористичний досвід і можуть знаходитись як вдома, так і за кордоном [16, с. 5].

Стратегія з кібербезпеки Великобританії розрізняє два види порушень у кіберпросторі – кіберзалежні злочини та кіберспоряджені злочини. До першого виду належать злочини, які як використовують інформаційно-телекомунікаційні технології, так і спрямовані на їх пошкодження; до другого виду належать традиційні злочини, під час здійснення яких використовуються комп'ютери або комп'ютерні мережі [17, с. 17].

У Стратегії з кібербезпеки Австрії під кібератакою розуміється атака, що спрямована на системи інформаційних технологій і спрямована на порушення конфіденційності, цілісності та доступності інформаційно-комунікаційних систем [18, с. 20].

У стратегії з кібербезпеки Хорватії альтернативно до поняття «кіберзлочин» використовується поняття «комп'ютерний злочин» [19, с. 16]. Так, під ним розуміється «злочин, який залучає комп'ютерні системи, програми та дані, здійснені у віртуальному просторі за допомогою комунікаційних та інформаційних

технологій, і створює загрозу для створення більш безпечного інформаційного суспільства» [19, с. 16].

Національна Стратегія з кібербезпеки Швеції приділяє окремо увагу кібератакам, проведеним державами або спонсорованими державами [20, с. 6]. Такі атаки розглядаються як з точки зору окремої погрози, так і як один із компонентів політичних або воєнних засобів сили [20, с. 6]. Такі кібератаки зазвичай спрямовані на отримання інформації, що стосується економіки, компаній, захисних можливостей, політики безпеки, критичної інфраструктури [20, с. 6].

Національна Стратегія Фінляндії досить поверхнево зупиняється на питанні кібератак, віддаючи перевагу аналізу управління кібербезпекою. В контексті кібератак зазначено, вони становлять загрози у кіберпросторі, які стосуються приватних осіб, бізнес середовища і суспільства в цілому [21, с. 1]. Кібератаки можуть застосовуватись як засоби політичного або економічного впливу і за ступенем тиску можуть порівнятись з воєнною силою [21, с. 1].

Національна Стратегія Нідерландів також прямо не наводить визначення кібератак, проте зазначає про їх спрямованість державних суб'єктів на економічному і політичному шпівонажі, що є прямою загрозою інтересам і безпеці країни [22, с. 7].

У Стратегії з кібербезпеки Словенії безпосередньо не наведено поняття «кібератака». Але наведені її характерні ознаки. По-перше, Стратегія наводить перелік кіберзлочинів, до яких, зокрема, належать: втручання в приватне життя, отримання інформації з метою вимагання, шахрайство в мережі Інтернет, цифрове піратство, економічне шпівунство [23, с. 7]. У той же час, Стратегія розрізняє групи злочинів на такі, що спрямовані на перешкоджання функціонування мережі Інтернет та кібертероризм, що може становити загрозу життю людини [23, с. 7].

Національна стратегія Польщі опосередковано визначає кібератаки як суттєве глобальне або локальне втручання у функціонування кіберпростору, що має вплив на відчуття особами захищеності, ефективність функціонування органів та національну безпеку загалом [24, с. 4].

В Україні поняття кібератака досить широко розкривається у Законі України «Про кібербезпеку». Так, відповідно до зазначеного закону, «кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [25].

Окремо варто також зупинитись на підходах до визначення кібератак державних органів Сполучених Штатів Америки. Зокрема, Міністерство Охорони США у Словнику воєнних символів наводить таке визначення кібератак у кіберпросторі: «дії, здійснені в кіберпросторі, що створюють помітні наслідки відмови (тобто деградацію, підриг або руйнування) в кіберпросторі, або маніпуляції, що призводять до відмови, що виникає у фізичному вимірі, і вважається формою стрілянини» [26, с. 55]. Директива військово-повітряних сил США 10-7 операції у кіберпросторі визначає як «застосування можливостей кіберпростору, де основною метою є досягнення цілей у кіберпросторі або за його допомогою» [27]. У 2006 році Клей Вілсон, спеціаліст відділу технологій та національної безпеки, закордонних справ, оборони та торгівлі підготував звіт для Конгресу під назвою «Інформаційні операції та кібервійна: можливості та пов'язані з цим політичні питання» [28]. У цьому звіті Клей Вілсон надає наступне визначення комп'ютерних атак в мережі: «операції, спрямовані на порушення або знищення інформації, що знаходиться в комп'ютерах та комп'ютерних мережах» [28]. До визначальних рис комп'ютерних атак в мережі Клей Вілсон відносить їх пов'язаність з потоком даних, що можуть використовуватись у якості зброї [28]. До

видів зброї, що використовуються під час кібератак належать віруси, троянські вірусні програми, інструменти для відмови в обслуговуванні [28].

Таким чином, не зважаючи на те, що держави при характеристиці кібератак оперують різними поняттями, їх спільними характерними ознаками є: здійснення кібератак відбувається через комп'ютерні мережі; основною метою є перешкоджання нормальному функціонуванню держави або завдання шкоди; внаслідок кібератак зазнають шкоди важливі об'єкти інфраструктури держави, компанії, державні інституції чи громадяни. На наше переконання, за зазначеними характеристиками кібератак можна дійти висновку, що вони є подібними до традиційних збройних атак, оскільки можуть завдати значної шкоди.

1.2. Основні цілі здійснення кібератак

Оскільки на сьогодні не існує міжнародного акта, що має обов'язкову юридичну силу для держав, варто звернути увагу на м'яке право, яке надає рекомендації щодо належної поведінки держав у кіберпросторі. Зокрема, у 2013, 2015 роках Група урядових експертів у галузі інформації та телекомунікацій в контексті міжнародної безпеки та у 2021 році Робоча група відкритого типу з питань розвитку інформації та телекомунікацій у контексті міжнародної безпеки підготувала звіти, що наводять, зокрема, перелік існуючих та потенційних загроз кібербезпеці держав [29; 30; 31]. На підставі аналізу цих звітів нами було виокремлено основні цілі, відповідно до яких можуть здійснюватись кібератаки.

1.2.1. Завдання шкоди об'єктам критичної інфраструктури держав

Завдання шкоди об'єктам критичної інфраструктури є однією з найбільш поширених цілей здійснення кібератак. Робоча група відкритого типу з питань розвитку інформації та телекомунікацій у контексті міжнародної безпеки неодноразово наголошувала на важливості охорони об'єктів критичної інфраструктури [30]. У Звіті за 2015 рік Робоча група вказала, що кібератаки на

об'єкти критичної інфраструктури є найбільш руйнівними [31]. При цьому, до критичної інфраструктури також варто відносити також критичну інформаційну інфраструктуру, що підтримує можливість надання важливих послуг [30].

У Резолюції Генеральної Асамблеї ООН № 58/199 визначено, в яких випадках інфраструктуру можна вважати критично важливою. Так, об'єктами критичної інфраструктури є ті, що «застосовуються, зокрема, для генерації, передачі та розподілу енергії, повітряного та морського транспорту, банківських і фінансових послуг, електронної комерції, водопостачання, постачання продукції та суспільного здоров'я – а також критичні об'єкти інфраструктури, що більшою мірою пов'язують та мають вплив на ці операції» [32].

У Директиві Президента Сполучених Штатів Америки NSC-63 об'єкти критичної інфраструктури визначаються як «фізичні або кібер системи, що є важливими для мінімальних операцій економіки та уряду» [33]. У згаданій Директиві, подібно з Резолюцією ООН 58/199, до таких об'єктів відносять, зокрема, телекомунікації, енергію, водопостачання, банківські і фінансові послуги [33].

Європейська Комісія визначає об'єкти критичної інфраструктури, як такі, що складаються з «фізичного та інформаційного технологічного обладнання, мереж, послуг та активів, які, у випадку їх пошкодження або знищення, матимуть серйозний вплив на здоров'я, безпеку або економічний доброту громадян чи ефективне функціонування урядів Держав-учасниць» [34, с. 3]. Європейська Комісія також наводить перелік об'єктів критичної інфраструктури, до яких, зокрема, належить, електричні установки, комунікації та інформаційні технології, фінанси, охорона здоров'я, водопостачання, транспорт, урядові послуги тощо [34, с. 4]. Для визначення того, чи належать об'єкти до критично важливих, Європейська Комісія вважає за необхідне враховувати обсяг поширення таких об'єктів, їх важливість, зокрема, загальносуспільну, економічну, екологічну, політичну [34, с. 5].

На сьогодні можна навести не один приклад кібератак, які мали за мету завдати шкоди об'єктам критичної інфраструктури держав.

Одним із перших таких випадків мав місце в Естонії. У квітні 2007 року Естонія зазнала численних кібератак, проведених, як вважається, Російською Федерацією [1, с. 80]. Причинами таких кібератак стали напружені відносини між країнами на ґрунті культурних питань [1, с. 80; 35, с. 50]. Естонія досить тривалий час входила до складу Радянського Союзу і станом на 2007 рік частину її населення становили російські меншини [35, с. 50]. У рамках політики квітні 2007 року естонський уряд прийняв рішення про перенесення меморіалу Бронзового Солдата, що символізував визволення Естонії радянськими військами від нацистів, з центральної частини міста до військового кладовища [36]. У якості протесту на вулицях Талліна виникли протести російських меншин [36]. Звичайно, що таке рішення влади Естонії викликало невдоволення і у Російській Федерації, уряд якої звинуватив естонський уряд у переписуванні історії [37, с. 54]. Тому, усвідомлюючи, що Естонія надавала більшість послуг онлайн і дуже сильно залежала від інтернет мережі, на критичні об'єкти її інфраструктури були здійсненні численні кібератаки, об'єктами яких стали веб-сайти державних органів, інтернет-провайдери, електронні банківські системи [38, с. 5]. Спочатку було здійснено атаку для відмови у доступі в обслуговуванні, а також розподілену атаку на відмову в обслуговуванні, розсилання спаму та дефейс сайтів [37, с. 55]. Наступним етапом було ураження об'єктів критичної інфраструктури - телекомунікаційних компаній, державних органів, а також найбільших банків країни - Hansapank та SEB Eesti Ühispank [37, с. 55-56]. Атаки призвели до припинення роботи онлайн банківських систем, комунікації за допомогою мобільного зв'язку, міжнародного інтернет трафіку, роботи урядових сайтів через спам [37, с. 56]. Як наслідок, уряд країни був позбавлений можливості ефективно комунікувати з населенням, люди не мали змоги скористатись численними урядовими та банківськими онлайн послугами [37, с. 56]. Хоча кібератаки призвели до порушення інформаційно-телекомунікаційних систем Естонії лише на декілька годин, матеріальний розмір збитків становив близько 415 тисяч євро [37, с. 56].

Уряд Естонії ініціював розслідування, у ході якого було встановлено, що для проведення кібератаки Росія залучила хакерів не лише з Росії, але і з Єгипту та

США. [35, с. 52] Не зважаючи на те, що уряд Естонії підозрював у здійсненні кібератак Російську Федерацію, прямих доказів для її причетності до цього інциденту не було встановлено [1, с. 80].

Не дивлячись на те, що атаки не спричинили суттєвої шкоди самим інформаційно-телекомунікаційним системам Естонії, цей інцидент привернув до себе увагу НАТО у якості потенційно нової загрози для безпеки інших держав [39]. Як слушно вирізняє Стефан Герцог: «це питання національного суверенітету, оскільки цифрові мережі і критично важлива інфраструктура, що є об'єктами ураження хакерів, є власністю держав або знаходиться на їх територіях» [35, с. 52].

Іншим випадком заподіяння шкоди об'єктам критичної інфраструктури є кібератака в Ірані. У якості інструменту кібератаки було використане шкідливе програмне забезпечення під назвою Стакснет [40, с. 70]. Ці кібер-атаки, були здійснені на тлі напружених стосунків між США та Іраном, що виникли з приводу наміру Ірану розробити ядерну зброю [41]. У 2002 році було оприлюднено інформацією, згідно якої іранський уряд здійснював збагачення урану на спеціальному обладнанні у Натанзі [42, с. 6]. І хоча сам уряд Ірану запевняв у тому, що така розробка здійснювалась виключно в мирних цілях, Організація Об'єднаних Націй та Міжнародне агентство з атомної енергії все ж схилились до думки, що Іран розробляв ядерну зброю [43]. Такі дії Ірану різко засуджувалось США та Європейським Союзом [41].

Міжнародне агентство з атомної енергії на початку 2000-х років висловлювало занепокоєння з приводу активної ядерної програми Ірану [43]. У 2006 році Іран заявив, що він здійснює виробництво урану, достатнього для живлення атомних електростанцій [43]. У відповідь, Рада Безпеки ООН видала Резолюцію 1737, якою заборонила Ірану здійснювати діяльність, пов'язану з ядерною енергією, а також закликала держави утримуватись від постачання будь-якого обладнання, матеріалів чи технологій, що можуть сприяти розробці ядерної зброї [44]. Окрім цього, Рада Безпеки закликала держави обачливо ставитись до транзиту через їх територію тих осіб, які були визначені Радою Безпеки як такі, що пов'язані з підтримкою ядерної діяльності Ірану [44]. У 2009 році Іран здійснив

тестовий запуск ракет дальнього спрямування, що викликало у держав неабияке занепокоєння [43].

У 2010 році білоруська компанія ВірусБлокАда першою виявила кібер-атаку, спрямовану на ураження газових центрифуг на установці зі збагачення урану в Натанзі [45]. Вірус під назвою Стакснет відрізнявся тим, що він зміг уразити мережу, не під'єднану до Інтернету [41]. На переконання Еміліо Іасієлло, функціональна складність, намір застосування та прихована поява Стакснету у мережі без Інтернет як з'єднання прямо вказує на причетність до цього держави [41]. Проте, хто саме здійснив атаку, так і не було встановлено. За найбільш поширеною версією, Стакснет було розроблено США за підтримки Ізраїлю [42, с. 4]. Однак, альтернативно, висувались припущення щодо здійснення таких атак Російською Федерацією [46].

В результаті дії Стакснету, Іран зазнав численних негативних наслідків різного характеру: соціально-політичних (суспільство відчуло незахищеність через неефективність іранських захисних механізмів проти кібер-атак); економічних (Іран опинився під рядом економічних ембарго, що завадило йому придбати обладнання для подальших ядерних розробок); технологічних (було уражено близько 1000 центрифуг зі збагачення урану) [42, с. 9-10]. З іншого боку, виникає питання, чи дійсно Стакснет завдав серйозних негативних наслідків Ірану. Не зважаючи на те, що завдяки кібер-атаці вдалось уповільнити темп розвитку ядерної програми Ірану, повністю зупинити його все ж не вдалось [41].

Таким чином, виходячи з характеристик кібератак, вони здатні заподіяти шкоду на рівні з зі збройною атакою із застосуванням зброї. Ураження критичної інфраструктури може повністю або частково завадити функціонуванню стратегічно важливих об'єктів.

1.2.2. Кібератаки як спосіб завдання шкоди під час збройного конфлікту

Якщо попередні приклади кібератак, здійснені проти Ірану та Естонії, виникли на тлі напружених відносин між країнами, то іншою метою кібератак,

може бути завдання шкоди державі під час збройного конфлікту для послаблення позицій протилежної сторони.

У Звіті за 2015 рік Робоча група відкритого типу з питань розвитку інформації та телекомунікацій зауважила про розвиток інформаційно-телекомунікаційних можливостей з метою їх застосування у воєнних цілях [31]. Робоча група також наголосила, що дуже ймовірно подальше застосування інформаційно-телекомунікаційних можливостей під час збройних конфліктів [31]. Аналогічна позиція була висловлена Робочою групою і у Звіті за 2021 рік [30].

У якості прикладів кібератак, що були здійснені на фоні збройного конфлікту, можна навести випадки в Грузії та Україні.

Зокрема, у 2008 році кібератаки були спрямовані проти Грузії. Вони були здійснені на фоні Російсько-Грузинської війни [47]. Загалом було вражено 54 веб-сайти, більшість із яких були державними [37, с. 59]. На відміну від кібератак в Естонії, наслідком яких була лише відсутність доступу до сервісу, влада Грузії у 2011 році виявила, що в ході кібератаки було також зібрано інформацію, яка торкалась питань національної безпеки [37, с. 59].

Павло Шакарян виділяє дві стадії цієї кібератаки: перша стадія була спрямована саме на відсутність доступу до сервісу, що було досягнуто шляхом використання шкідливого програмного забезпечення [48, с. 63-64]. На цій стадії постраждали урядові веб-сайти та сайти медіа; на другій стадії поряд з атаками на веб-сайти уряду та медіа, додалися сайти фінансових, навчальних та бізнес установ, та західних засобів масової інформації [48, с. 63-64]. При цьому, окрім відсутності доступу до серверу, було здійснено дефейс сайтів, а також масове розсилання спаму на електронні адреси політиків [48, с. 63-64].

Згідно Спеціального звіту Підрозділу США з кібернаслідків, аналогічно з випадком в Естонії, кібератаки були проведені різними людьми з різних місць [49, с. 2-3]. Було залучено цивільних громадян не лише з Росії, а і з України та Латвії [49, с. 3].

Виділяють такі найбільш поширені точки зору, що оцінюють ступінь зв'язку кібератак з урядом Російської Федерації: 1) кібератаки були здійснені спонтанно

так званими патріотичними «хактивістами» у відповідь на атаки на веб-сайти Південної Осетії; 2) атаки були здійснені лише російськими організованими кримінальними групами; та 3) кібератаки були здійснені російськими кримінальними групами на запит Кремля [48, с. 66-67]. Павло Шакарян не погоджується з першою точкою зору, зазначаючи, що кібератаки в Грузії були здійснені раніше, ніж у Південній Осетії, а також були використані ботнети, що вказує на причетність уряду Російської Федерації [48, с. с. 66-67]. Науковець частково поділяє другу та третю точки зору, зазначаючи, що з одного боку, багато хактивістських сайтів були пов'язані з кримінальними групами, а також наявний зв'язок кібератак з воєнними операціями Росії, а з іншого боку, що прямих доказів залучення уряду Російської Федерації до проведення таких кібер атак немає [48, с. 67].

Внаслідок кібератаки в період війни уряд Грузії був позбавлений можливості прокомунікувати як зі своїм населенням, так і сповістити міжнародну спільноту про кібератаки з боку Росії [50]. Окрім цього, сильно постраждала економіка країни, оскільки Національний банк Грузії не міг функціонувати протягом 10 днів [49, с. 6].

Досить велика кількість дослідників та публічних осіб переконана, що основна мета цієї кібератаки полягала у тому, щоб ізолювати, примусити грузинів мовчати і не дати їм можливості описати конфлікт з Росією зі своєї точки зору [48, с. 65-66; 51].

Щодо України, то вона декілька разів потерпала від кібератак на критичні об'єкти її інфраструктури. Подібно до попереднього випадку в Грузії, кібератаки проводились на фоні конфлікту з Російською Федерацією [52, с. 3].

Перша хвиля кібератак відрізнялась відносно незначним ступенем завданої шкоди [37, с. 61]. Такі кібератаки проводились у період Євромайдану та окупації і, в подальшому, анексії Кримського півострову [52, с. 10]. У цей період атаки були спрямовані на відмову у доступі до серверів [52, с. 10].

Ситуація змінилась у 2015 році, коли розпочався воєнний конфлікт між Україною та Російською Федерацією на території Донбасу. Однією з найбільш

деструктивних кібератак була спрямована на електростанції України. 23 грудня 2015 року через кібератаки на 27 розподіляючих станції було пошкоджено постачання електричної енергії на території західної України [53, с. 1]. За різними підрахунками, внаслідок кібератаки від 225 тисяч [54] до 1,4 мільйони [55] українців не мали електропостачання.

Проте, атака на електростанції у 2015 році була лише однією із ряду кібератак на критичні об'єкти інфраструктури України. Подібно до ситуації з електростанціями на Західній Україні, у 2016 році в Києві також було порушено роботу електричних станцій, внаслідок чого одна п'ята частина населення міста була позбавлена електропостачання [56]. Крім цього, об'єктами кібератак стали: залізнична система України (2014 та 2015 рік), регіональні державні установи (2014 рік), медіа (2015 рік), державні архіви (2015 рік), телебачення (2015 рік) та, неодноразово, електростанції (2014 – 2016 роки) [57, с. 7]. Цей ряд кібератак характеризується схожою методикою проведення, а також єдиною ціллю - завдання шкоди окремим секторам промисловості України [58, с. 325].

У своєму аналізі Марі Безнер та Патріс Робін виділяють окремі проросійські групи хакерів, що мають зв'язки з Росією і могли бути залучені до кібератак в Україні: КіберБеркут, АРТ28, АРТ29, Анонімна Україна, Quedagh, Тролі, Молодіжний рух і російські патріотичні хакери «Наші» [52, с. 12-13]. Першою характерною ознакою цих груп є наявність досвіду у їх учасників у проведенні досить відомих кібератак у інших країнах, зокрема, Чеченській Республіці, Грузії, Сполучених Штатах Америки, та міжнародній організації – НАТО [52, с. 12-13]. Другою особливістю є їх яскрава політична спрямованість, зокрема, Кіберберкут підтримує сепаратистів на сході України, Молодіжний рух і російські патріотичні хакери «Наші» була створена на противагу Помаранчевій революції в Україні [52, с. 12-13]. Проте, як зазначає Т. Маурер, не зважаючи на те, що український уряд звинувачував Росію у спонсоруванні і причетності до кібератак, все ж, зв'язки між хакерськими групами та урядом Російської Федерації не були встановлені [59, с. 85].

Загалом кібератаки завдали значної шкоди об'єктам критичної інфраструктури України. Виділяють наступні наслідки проведення кібератак: зниження рівня довіри населення до державних інституцій з точки зору їх захищеності у кіберпросторі; отримання зловмисниками доступу до інформації; ускладнення можливості повноцінного відновлення роботи електричними станціями протягом двох місяців; повне зупинення роботи деяких комп'ютерів без можливості їх відновлення; атаки у кіберпросторі стали допоміжними під час початку збройної агресії Російської Федерації [52, с. 14-16].

Кібератаки на території України поширились навіть за межі Східної Європи [58, с. 326]. У зв'язку з цим, Скот Дж. Шейлфорд, М. Сулмейєр та інші виділяють такі наслідки, з якими зіштовхнулися країни у питаннях кібербезпеки: було виявлено, що досить велика кількість електричних мереж використовує застріле обладнання, яке не може попередити втручання хакерів в систему; кібератаки, спрямовані на завдання шкоди об'єктам критичної інфраструктури підвищують напруженість у міжнародних відносинах, що заважає об'єднувати зусилля у процесі вироблення норм; країни змушені покращувати рівень захищеності своїх об'єктів через постійне підвищення рівня досвідченості хакерів у проведенні кібератак [58, с. 326-327].

Таким чином, випадки здійснення кібератак у Грузії та Україні свідчать, що вони можуть бути альтернативним способом ураження протилежної сторони під час збройного конфлікту. Відтак, вважаємо за доцільне на цій підставі вважати, що до кібератак мають застосовуватись норми та принципи міжнародного права, як і до «традиційного» застосування сили.

1.2.1. Здійснення кібератак з метою втручання у політичні питання держави

Робоча група відкритого типу з питань розвитку інформації та телекомунікацій у Звіті за 2021 рік зазначила про можливе зловмисне застосування інформаційно-комунікаційних технологій з метою підривання довіри до

політичного та виборчих процесів [30]. Раніше, у Звіті за 2015 рік Група урядових експертів наголосила на необхідності утримуватись від погрози або застосування сили, що спрямована проти політичної незалежності держави, а також зауважила про заборону втручання у внутрішні справи держав [31].

Яскравим прикладом втручання у політичні процеси держави є здійснення кібератак під час передвиборчих процесів, пов'язаних з обранням Президента Сполучених Штатів Америки. [60]. Кібератака почалась 14 червня 2016 року і характеризувалась порушенням роботи комп'ютерної мережі Демократичного Національного Комітету [61]. Хакери отримали доступ до бази даних, що містила інформацію про кандидата у Президенти Дональда Трампа, в результаті чого вони отримали можливість прочитати усі електронні листи і чати [61]. Також в результаті атак хакери декілька разів оприлюднили зміст декількох тисяч електронних повідомлень, до яких вони отримали доступ. Зокрема, 22 липня 2016 року WikiLeaks опублікувала електронні листи, в яких обговорювалась стратегія, спрямована на перешкодження діяльності головній опонентці Клінтон Берні Сандерс [62]. Окрім цього, була поширена інформація про адреси, номери кредитних карток, паспортні дані інших членів партії [63]. У жовтні 2016 року WikiLeaks оприлюднила інформацію з аккаунта Капріції Маршал, де зазначалось про засоби, що використовувались під час кампанії, переговори з медіа, а також діяльність в Інтернет мережі [64].

За результатами проведеного розслідування компанія CrowdStrike Services оприлюднила звіт, де зазначила, що в результаті її розслідування, було встановлено, що кібератаки були проведені Російською Федерацією [65]. Цей висновок також був підтверджений незалежним звітом Розвідувальної служби США [65]. 25 липня Федеральне Бюро Розслідувань розпочало проведення розслідування [64]. 7 жовтня WikiLeaks оприлюднила 50 тисяч електронних повідомлень Джон Подеста [66]. Розвідувальна спільнота США зробила відповідну заяву:

Розвідувальна спільнота США (РС США) впевнена, що уряд Російської Федерації направив нещодавні компрометуючі електронні повідомлення від осіб та установ США, включаючи політичні організації США. Нещодавні відкриття згаданих зламаних

електронних повідомлень на таких сайтах як DCLeaks.com та WikiLeaks, а також Guccifer 2.0 online persona відповідають методам і мотивам російсько спрямованих зусиль. Ці крадіжки і відкриття мають на меті втрутитись у процес виборів США [67].

Розвідувальна спільнота США дійшла висновку, що метою кібератак була скоріше допомога Дональду Трампу у виборах [68]. У той же час, уряд Російської Федерації не визнав своєї відповідальності за проведені атаки [69].

Не зважаючи на те, що у кінцевому підсумку Російську Федерацію не було притягнуто до відповідальності, Кемерон Белл вважає, що кібератаки, спрямовані проти США, є прямим порушенням Резолюції Генеральної Асамблеї ООН № 2625 [70]. Так, відповідно до Резолюції 2625, «будь-яка держава повинна утримуватись від будь-яких дій, спрямованих на часткове або повне порушення національної єдності та територіальної цілісності будь-якої іншої держави чи країни» [71]. На переконання Кемерона Белла, про порушення вказаного положення Резолюції 2625 може вказувати крадіжка листувань і їх публічне оприлюднення з метою втручання у виборчий процес і підірвання національної єдності [70]. Ми погоджуємось з вказаною точкою зору науковця, оскільки процес виборів є суверенним правом населення країни і будь-яке втручання, навіть у передвиборчий процес з боку інших держав є недопустимим.

1.3. Діяльність міжнародних організацій з протидії кібератак

1.3.1. НАТО

Проведені у 2007 році кібератаки в одній з країн-членів НАТО - Естонії, стали серйозною загрозою для НАТО, оскільки продемонстрували здатність зашкодити функціонуванню цілої країни, особливо тієї, що значним чином залежна від ІТ інфраструктури [72, с. 1]. У 2008 році на Будапештському Самміті, НАТО зауважила про необхідність зміцнення своїх інформаційних систем для протидії кібератак [73]. В результаті Самміту було створено два органи – Орган управління кіберзахистом та Кооперативний Центр передового досвіду з кіберзахисту [73].

Орган управління кіберзахистом покликаний координувати відповіді країн членів на кібератаки через централізоване бюро, а також підвищувати можливості протидії держав кібератакам [73]. Кооперативний Центр передового досвіду з кіберзахисту - акредитована організація, що не є частиною НАТО, проте надає експертну підтримку у дослідженні і тренуваннях з питань кібербезпеки [74]. Кооперативний Центр передового досвіду з кіберзахисту розробив Керівництво з національної системи кібербезпеки, в якій розділяє кібербезпеку на урядову, міжнародну та національну [75, с. 30-31]. Зокрема, до урядової організація відносить забезпечення функціонування окремих департаментів або агенцій, зокрема, правоохоронних, судових, економічних, інфраструктурних; до міжнародної – кооперацію держав, зокрема шляхом укладення міжнародних та політичних обов'язкових угод; до національної – шляхом кооперації уряду з приватними компаніями щодо питань кібербезпеки [75, с. с. 30-31].

У 2014 році НАТО розробила також Політику про Кібербезпеку, в якій головним пріоритетом виступає захист інформаційних і комунікаційних систем НАТО [74]. Політика про Кібербезпеку також визначає напрямки керуванням захисту від кібератак, допомогу державам-членам Альянсу, різноманітні шляхи кооперації між державами, включаючи навчання і тренування, а також поширення НАТО інформації, кращих практик та взаємну допомогу у попередженні і боротьбі з кібератаками [74].

У 2016 році НАТО визнала кіберпростір як один з таких, що підлягають захисту НАТО і з того часу визначає кіберзахист у якості пріоритетного питання [76].

У 2018 році НАТО зауважила на Самміті у Брюсселі, що кібератаки повторюються все частіше і стають все більш руйнівними [77]. У Декларації зазначено:

НАТО продовжуватиме пристосовуватись до мінливого обсягу кіберзагроз, на який впливають як державні, так і недержавні суб'єкти, в тому числі спонсоровані державою. Кіберзахист є частиною основного завдання колективної оборони НАТО. Ми повинні мати можливість діяти в кіберпросторі так само ефективно, як у повітрі, на суші

та в морі, щоб зміцнити та підтримати загальну позицію стримування та оборони Альянсу. Тому ми продовжуємо впроваджувати кіберпростір як сферу діяльності [77].

Наразі питання з кібербезпеки є пріоритетним на порядку денному НАТО [78]. Зокрема, про це свідчить низка заходів, що вживається НАТО для підвищення здатності до оборони від кібератак. По-перше, НАТО зосереджена на тренуванні спеціалістів з захисту мереж НАТО та держав від кібератак [78]. По-друге, визначною подією було створення Кібер Коаліції, що включає експертів з країн-членів НАТО, Фінляндії, Ірландії, Швеції, Швейцарії, а також Європейського Союзу [79, с. 24]. Саме завдяки Кібер Коаліції відбувається навчання з протидії кіберзагрозам [79, с. 24]. По-третє, НАТО зміцнює співпрацю з Європейським Союзом, Організацією Об'єднаних Націй, Радою Європи та Організацією з безпеки і співробітництва в Європі [74]. У звіті за 2020 рік НАТО окремо наголошує на підвищеній загрозі здійснення кібератак під час пандемії COVID-19, оскільки основні види діяльності перемістились у онлайн площину [79].

1.3.2. Рада Європи

Питання кібербезпеки на європейському рівні поставало ще наприкінці 90-х років минулого століття [80, с. 2]. З цією метою у 1996 році Європейський Комітет з проблем злочинності вирішив призначити експертів, які б займались питаннями кібербезпеки [80, с. 2]. Європейський Комітет з проблем злочинності зазначив: «враховуючи міжкордонну природу інформаційних мереж, необхідні погоджені міжнародні зусилля для боротьби з таким зловживанням» [80, с. 2]. Зокрема, до функцій Комітету входило дослідження злочинів, пов'язаних з комп'ютерами та проблем кримінального процесуального права у сфері інформаційних технологій, інших суттєвих питань з кримінального права, в яких загальний підхід може бути необхідним в цілях міжнародної кооперації, питання юрисдикції по відношенню до порушень у сфері інформаційних технологій, міжнародної співпраці у сфері розслідування кіберпорушень [80, с. 3].

Після численних переговорів та засідань у червні 2001 року проєкт Конвенції був поданий на затвердження Комітету експертів зі злочинів у кіберпросторі [80, с. 4].

Далі наводимо перелік деяких видів порушень, визначених Конвенцією.

Конвенція визначає *незаконний доступ* як навмисний доступ до цілої комп'ютерної системи або її частини шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою [81]. *Під нелегальним перехопленням* розуміється «навмисне перехоплення технічними засобами передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані» [81]. *Втручанням у дані* є «навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це» [81]. *Втручанням у систему* є «навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це» [81]. *Шахрайство, пов'язане з комп'ютерами* – «навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом: а) будь-якого введення, зміни, знищення чи приховування комп'ютерних даних; б) будь-якого втручання функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи» [81].

Однак, варто зауважити, що Конвенція регулює кримінальну відповідальність приватних осіб, які здійснюють кібератаки проти держав та інших приватних суб'єктів. Не зважаючи на це, Конвенція може використовуватись міжнародною спільнотою у якості орієнтиру для розроблення міжнародного документу, що регулював би права і обов'язки держав у кіберпросторі. Зокрема, варто взяти до уваги досить широкий перелік протиправних діянь, наведених у Конвенції, та їх характеристику.

1.3.3. Організація Американських держав

У 2004 році Генеральна Асамблея Організації Американських держав прийняла Резолюцію 2040 (XXXIV-O/04), в якій одним із питань була протидія і запобігання кіберзлочинам [82]. Генеральна Асамблея надала державам рекомендації щодо участі у міжнародному тренуванні, присвяченому кіберзлочинам, участі у технічних зібраннях Групи Урядових Експертів з Кіберзлочину, приділенню уваги механізмам кооперації між державами з метою боротьби з кіберзлочином, розвитку технічних та правових можливостей для надання допомоги у розслідування кіберзлочинів, імплементації принципів Конвенції Ради Європи про кіберзлочинність (2001) та розгляду можливості приєднання до конвенції [82].

Також Генеральна Асамблея Організації Американських держав прийняла Інтер-Американську Стратегію Подолання загроз кібербезпеці у відповідь на Резолюції Генеральної Асамблеї ООН 55/63 та 56/121 з метою створення глобальної культури кібербезпеки [83]. Зокрема, стратегією передбачалось визначення функцій органів, що відповідали за питання кібербезпеки [83]. На Міжамериканський комітет з протидії тероризму покладались функції з формування Міжамериканської мережі з попередження, спостереження та попередження для швидкого розповсюдження інформації про кібербезпеку та реагування на кризи, інциденти та загрози комп'ютерній безпеці, визначення та прийняття технічних стандартів для безпечної архітектури Інтернету [83]. На Групу урядових експертів з кіберзлочинів - забезпечення держав-членів Організації Американських держав юридичними інструментами, необхідних для захисту користувачів Інтернету та інформаційних мереж, введення в дію ефективного законодавства про кіберзлочинність та вдосконалення міжнародної роботи з питань кіберзлочинності [83].

1.4. Висновки до Розділу 1

Таким чином, на сьогодні міжнародною спільнотою не було вироблено єдиного підходу до визначення поняття «кібератака». У зв'язку з цим, науковці аналізують суть кібератак і пропонують власні визначення у своїх працях. Окрім цього, країни активно приймають стратегії розвитку законодавства у сфері кібербезпеки, в яких пояснюють власні підходи до трактування суті кібератак. Деякі країни, такі як Словенія, розглядають кібертаки у якості злочину, що регулюється кримінальним законодавством країни і здійснюється приватними особами до відношенню до інфраструктури держави або інших приватних осіб. Проте, чимало країн, зокрема, Швеція, Фінляндія, Польща, Великобританія все ж розглядають кібертаки як засоби втручання урядами інших держав або ж засоби тиску з метою завдання шкоди національній безпеці.

На основі визначень, наведених у наукових працях та національних стратегіях держав з кібербезпеки можна зробити висновки про їх характерні особливості: вони становлять втручання у об'єкти комп'ютерної мережі, здійснюються державами або приватними особами з політичними мотивами із використанням шкідливих інформаційно-телекомунікаційних засобів, спрямовані на ураження або втручання у функціонування таких комп'ютерних мереж; основною метою є перешкоджання нормальному функціонуванню держави або завдання шкоди; внаслідок кібератак зазнають шкоди важливі об'єкти інфраструктури держави, компанії, державні інституції чи громадяни.

До основних цілей кібератак належить: завдання шкоди об'єктам критичної інфраструктури; застосування додаткових заходів ураження протилежної сторони під час збройного конфлікту; та втручання у політичні справи іншої держави. Як правило, кібертаки спрямовані на перешкоджання роботи таким об'єктам критичної інфраструктури, таких як сайти органів державної влади, банківських і фінансових установ, підприємств, електричних мереж, медіа і телекомунікаційних компаній. Тривалість кібератак варіюється залежно від ситуації, проте зазвичай здійснюється періодично протягом декількох днів чи декількох місяців. При цьому, ступінь спричиненої шкоди залежить не лише від використаних інструментів, а й від залежності інфраструктури країни від інтернет-мережі.

В результаті активного поширення кібератак у світі, міжнародна спільнота постала перед необхідністю об'єднати зусилля для врегулювання на міжнародно-правовому, регіональних та національних рівнях питання попередження та відповідальності за здійснення кібератак. Міжнародні організації, такі як НАТО, Європейська Рада та Організація Американських Держав активно почали розробляти власні стратегії з кібербезпеки. Більше того, НАТО призначила спеціальні органи відповідальні за цей напрям, а Рада Європи прийняла Конвенцію з кібербезпеки, що врегулювала питання кібератак з точки зору злочину, здійсненого приватними особами.

Утім, на сьогодні міжнародною спільнотою не було вироблено єдиного підходу до визначення поняття кібератака. У зв'язку з цим, науковці аналізують суть кібератак і пропонують власні визначення у своїх працях.

РОЗДІЛ 2.

МЕХАНІЗМИ МІЖНАРОДНОГО ПРАВА ДЛЯ ПРИТЯГНЕННЯ ДЕРЖАВ ДО ВІДПОВІДАЛЬНОСТІ

Відповідно до статті 2 Статей про відповідальність держав за міжнародно-протиправні діяння, міжнародно-протиправне діяння має місце, якщо будь-яка поведінка, що полягає у дії або бездіяльності, яке: а) належить державі за міжнародним правом; та б) являє собою порушення міжнародно-правового зобов'язання цієї держави [84].

Відповідно, у цьому розділі ми дослідимо підстави та критерії належності поведінки осіб, які здійснюють кібератаки, державі, приділяючи особливу увагу належності діянь приватних осіб державі.

Також у цьому розділі буде приділено увагу питанню кваліфікації кібератаки у якості міжнародно-протиправного діяння з огляду на відсутність міжнародно-правового акту, який би прямо вказував на протиправність кібератак.

2.1. Належність поведінки держави

2.1.1. Належність поведінки представників органів держави

Відповідно до статті 4 Статей про відповідальність держав за міжнародно-протиправні діяння, поведінка будь-якого органу держави розглядається як діяння цієї держави незалежно від того, чи здійснює цей орган законодавчі, виконавчі, судові або будь-які інші функції, незалежно від положення, яке він займає в системі держави, і незалежно від того, чи є він органом центральної влади або адміністративно-територіальної одиниці держави [84]. Орган включає будь-яку приватну чи юридичну особу, яка має такий статус відповідно до внутрішнього законодавства держави [84].

У коментарі до статті 4 Статей про відповідальність держав за міжнародно-протиправні діяння зазначено, що до органів слід відносити державні органи будь-

якої ієрархії, а також як керуючих, так і підпорядкованих посадових осіб, не зважаючи на обмежений обсяг їх повноважень [85, с. 40-41]. Також до органів слід відносити територіальний орган федеральної держави, а також автономної території, незалежно від того чи наділений він федеральним парламентом повноваженнями щодо виконання міжнародних зобов'язань [85, с. 41].

Також окремо варто звернути увагу, чи визначає законодавство країни статус органу [85, с. 42]. У разі, якщо законодавством не визначено, що певне утворення є органом держави, варто визначити чи можна його вважати де факто органом. Як зазначає науковець Таніїзді, для встановлення, чи є суб'єкти кібератак де факто органами держави, варто визначити чи вони були створені державою, на скільки вони залежні від спонсуючої держави, чи залежить їх існування від залучення держави, організації і плануванні операцій [86, с. 160]. Зв'язок з державою також виникає, коли суб'єкти здійснення кібератак виконують делеговані державою функції для проведення операції [86, с. 161]. Зокрема, у своїй праці автор наводить позицію К. Масака, зазначаючи на прикладі Естонії, що звичайне поширення Російською Федерацією цілей лише спровокувало здійснення кібератак приватними особами, проте це не є підставою для встановлення належності їх поведінки державі [86, с. 161].

Концепцію де факто органу застосував Міжнародний суд справедливості ООН, зокрема, у справі Боснія і Герцеговина проти Сербії і Чорногорії, застосувавши так званий тест «повної залежності» від держави:

особи, групи осіб або утворення можуть, в цілях міжнародної відповідальності, прирівнюватися до державних органів, навіть якщо такий статус не впливає із внутрішнього законодавства, за умови, що фактично особи, групи або утворення діють у «повній залежності» від держави, для якої вони є лише інструментом [87].

У цій же справі Міжнародний суд справедливості ООН зазначив, що віднесення осіб до органів «має бути винятковим, що вимагає доказів особливо сильного ступеню державного контролю» [87]. Цю ж концепцію застосував Міжнародний суд справедливості ООН у Нікарагуа проти США, де, не зважаючи на те, що судом було встановлено, що діяння приватних осіб були спонсоровані і діяли згідно вказівок військового або розвідувального персоналу США, їм також

надавалась допомога, тренування, надання необхідного обладнання і підтримка США, контраст не були визнані органом США, оскільки суд не вбачав у цьому «повної залежності» [88].

Окрім цього, у справі Демократична Республіка Конго проти Уганди, Міжнародний суд справедливості ООН також здійснив аналіз щодо можливості визнання військового угруповання - Визвольного руху Конго – органом Уганди [89, с. 874]. Міжнародний суд справедливості ООН висловив позицію, за якою Визвольний рух Конго можна було визнати у якості державного органу Уганди, не зважаючи на те, що були наявні докази щодо їх тренування і воєнної підтримки з боку Уганди [90]. Відповідно, у своєму рішенні від 19 грудня 2005 року суд зазначив:

немає жодних достовірних доказів, які б свідчили про те, що Уганда створила ВРК. Уганда визнала проведення навчань та військову підтримку, про що свідчать докази. Суд не отримав належних доказів того, що Уганда контролювала або могла контролювати поведінку, за якої б пан Бемба міг скористатись такою допомогою. На погляд суду, поведінка ВРК не є такою, яка належить «органу» Уганди [90].

Отже, Міжнародний суд справедливості ООН досить обережно тлумачить критерії «повної залежності», що, безумовно, майже унеможливило віднесення осіб та утворень до де факто органів держави.

На наше переконання, у разі виявлення того, що кібератаку було здійснено посадовою особою органу держави, є підстави для притягнення держави до відповідальності. Проте, беручи це до уваги, навряд чи держави діятимуть безпосередньо через своїх посадових осіб. У зв'язку з цим, варто звернути більшу увагу на концепцію де факто органу. Зокрема, варто погодитись з Джейсоном Д. Джоллі, який зазначає, що встановлення повної залежності в кіберпросторі є ще складнішим, ніж у кінетичному [91, с. 93]. Зокрема, на наше переконання, це зумовлено технічними можливостями приховування справжнього місцезнаходження суб'єкта здійснення кібератак. Оскільки вирішальним питанням у відносинах з де факто органом є наявність контролю, вважаємо за необхідне проаналізувати його сутність на підставі 8 Статей про відповідальність держав за міжнародно-протиправні діяння.

2.1.2. Здійснення контролю над поведінкою приватних суб'єктів

Відповідно до статті 8 Статей про відповідальність держав за міжнародно-протиправні діяння, поведінка особи або групи осіб розглядається у якості діяння держави за міжнародним правом, якщо ця особа або група осіб фактично діють за вказівками або під керівництвом цієї держави при здійсненні такої поведінки [84]. Як зазначається у коментарі до статті 8, «три терміни «інструкція», «керівництво» та «контроль» є відокремленими; достатньо встановити будь-який з них» [85, с. 48]. Проте, що саме розуміється під цими поняттями та коли саме керівництво держави над діями приватних осіб буде вважатись контролем у значенні статті 8, коментар до Проекту статей про відповідальність держав за міжнародно-протиправні діяння не визначає. У зв'язку з цим, вважаємо за необхідне звернутись до судової практики Міжнародного суду справедливості ООН та Апеляційної Палати Міжнародного трибуналу по колишній Югославії.

Поведінка приватних суб'єктів лише тоді буде належати державі, коли держава здійснює контроль над кожною окремою операцією, а не тоді, коли поведінка приватних осіб просто пов'язана з операцією і не здійснюється під її контролем [85, с. 47]. Саме з такої позиції виходить Міжнародний суд справедливості ООН у своїх рішеннях. Зокрема у справі Нікарагуа проти США Міжнародний суд справедливості ООН зазначив: «не зважаючи на значну допомогу та іншу підтримку, що була їм надана Сполученими Штатами, відсутні чіткі докази, що Сполучені Штати фактично здійснювали такий ступінь контролю у всіх сферах, щоб визначити, що контраст діяли від їх імені» [88]. У справі Боснія і Герцеговина проти Сербії і Чорногорії Міжнародний суд справедливості ООН аналогічно застосував концепцію ефективного контролю при визначенні належності Югославії поведінки воєнних груп, які діяли на її території. Суд зазначив:

Позивач не довів, що вказівки були надані федеральною владою у Белграді, чи будь-яким іншим органом ФРЮ, щодо здійснення масових вбивств, тим більше, що такі вказівки були надані з конкретним наміром (*dolus specialis*), що характеризує злочин

геноциду...Все вказує на зворотнє: що рішення вбити доросле чоловіче населення мусульманської спільноти у Сребреніці було прийняте деякими членами головного штабу ЗРС, але без вказівок від чи під ефективним контролем ФРЮ [87].

Проте, з такою позицією Міжнародного суду справедливості ООН не погодився Віце-Президент суду Аль-Хасауна. У окремій думці суддя зазначив:

вимагати наявності контролю над недержавними суб'єктами, так і конкретних операцій в контексті яких були скоєні міжнародні злочини, є занадто високим порогом. Неминуchoю небезпекою такого підходу є те, що він дає державам можливість проводити злочинну політику через недержавних суб'єктів або утворення, не несучи безпосередньої відповідальності [92].

Науковці Уна Хетеуей та інші автори у своїй праці аналогічно критикують такий підхід Міжнародного суду справедливості ООН, зазначаючи, що високий поріг доказовості належності поведінки приватних осіб державі може спричинити прогалину у регулюванні відповідальності держав, що дозволить державам зловживати залученням приватних суб'єктів для здійснення тих чи інших діянь за їх вказівками [93, с. 554].

На наше переконання, в контексті кібератак, встановлення ступеню контролю держави над приватними суб'єктами є ще більш складним завданням. Встановити і довести, що держава надавала інструкції щодо кожної окремої операції у кіберпросторі надзвичайно непросто, враховуючи різні техніки приховування IP адрес. Більше того, представники держави можуть наймати приватних осіб які володіють необхідними знаннями для здійснення кібератак, а відтак, самостійно прийматимуть ті чи інші проміжні рішення під час виконання завдання.

Альтернативно, існує також концепція загального контролю. Ця концепція була застосована Апеляційною Палатою Міжнародного трибуналу по колишній Югославії у справі Прокурор проти Душко Тадіча, де Апеляційна Палата зазначила: «влада над збройними силами, як вимагається міжнародним правом для розгляду збройного конфлікту як міжнародного, полягала в загальному контролі, який виходив за рамки простого фінансування та оснащення таких сил, а також включав участь у плануванні та нагляді за військовими операціями» [94]. При цьому, Апеляційна Палата відхилила концепцію ефективного контролю,

застосовну Міжнародним судом справедливості ООН, оскільки метою прийняття статті 8 Статей про відповідальність держав за міжнародно-протиправні діяння було саме «запобігання уникненню державами міжнародної відповідальності через виконання завдання приватними особами, які не можуть або не повинні бути здійсненні державними посадовими особами» [94]. Міжнародний суд ООН у справі Боснія і Герцеговина проти Сербії і Чорногорії зазначив: «тест «загального контролю» є непридатним і тягнеться занадто далеко, майже до точки руйнування, зв'язок якої повинен існувати між поведінкою органів держави та її міжнародною відповідальністю» [87].

Порівнюючи концепції ефективного та загального контролю, науковиця У. Хетеуей зазначає, що кожен із підходів використовує власні критерії для визначення приналежності поведінки державі, проте жоден із них не наводить тієї межі, коли держава буде відповідальною за поведінку приватних осіб [93, с. 561]. З одного боку, високий поріг доказування контролю створює можливості для уникнення ними відповідальності, з іншого боку, занадто низький поріг доказування призвів би до притягнення відповідальності держав за діяння приватних осіб, які вони не могли об'єктивно попередити [93, с. 561].

Як зазначає Конград Велінські, жоден з вище зазначених видів контролю майже не застосований до кібератак [1, с. 83]. Вчений зазначає, що оскільки саме лише застосування шкідливого програмного забезпечення до об'єктів інфраструктури, розташованій на території іншої країни не є вагомим аргументом для виникнення відповідальності, оскільки обладнання, за допомогою якого здійснювалась кібератака, може знаходитись від контролем недержавних суб'єктів [1, с. 83]. У той же час, вчений наголошує на важливості питання належності поведінки державі для притягнення її до відповідальності і відзначає невідповідність міжнародного права сучасному рівню розвитку технологій [1, с. 83].

Філіп Пул також дотримується тієї точки зору, що визначення належності поведінки є надзвичайно складним питанням у контексті кібервійни [95, с. 311]. Вчений обґрунтовує це самою природою зброї, що використовується, і тактикою

[95, с. 311]. Наприклад, у 2009 році кібератака була здійснена на комп'ютерні системи Ірану, Бангладешу, Латвії, Індонезії, Філіпін, Брунею, Барбадосу [96]. Загалом було здійснено атаки щодо 103 країн світу [97]. В результаті розслідування дослідників з Моніторингу інформаційної війни були встановлені лише опосередковані зв'язки з урядом Китаю, оскільки організатори кібератаки діяли через сервери різноманітних організацій, зокрема, телекомунікаційних компаній, в'єтнамських паливних компаній та посольств [97]. У той же час, існувало припущення, за яких кібератаки здійснювались китайськими хакерами за межами Китаю з територій інших країн, використовуючи китайські проксі [97]. У цьому аспекті є слушною думка Філіпа Пула, який зазначає, що навіть якщо поведінка недержавних суб'єктів буде вважатись поведінкою держави, то постає питання, чи буде нести відповідальність та держава, з території якої було здійснено кібератаку [95, с. 311].

Отже, виходячи із двох концепцій – ефективного та загального контролю над поведінкою приватних суб'єктів, доходимо висновків, що в контексті кібератак більш релевантною є друга концепція. У іншому випадку, довести зв'язок держави і приватних осіб буде майже неможливо, чим і користуватимуться недобросовісні суб'єкти.

2.1.3. Визнання державою поведінки приватних осіб як власної

Відповідно до статті 11 Статей про відповідальність держав за міжнародно-протиправні діяння, поведінка, яка не належить державі, все-рівно, має вважатись поведінкою цієї держави відповідно до міжнародного права, якщо і до тієї міри, в якій держава визнає та приймає поведінку, про яку йдеться, як власну [84]. Насправді, такі ситуації досить рідко виникають на практиці. Про це свідчить і поодинокі справи, що розглядались Міжнародним судом справедливості ООН. Наприклад, у справі Сполучені Штати Америки проти Ірану, досліджувалась відповідальність Ірану за окупацію посольства США приватними особами. У цій

справі Міжнародний суд справедливості ООН визнав Іран відповідальним, зазначивши:

Політика, оголошена Аїятола Хомейні, щодо продовження окупації посольства та затримання його ув'язнених як заручників з метою тиску на уряд США була підтримана іншими іранськими представниками влади та схвалена ними неодноразово у заявах, зроблених у різному контексті ... Схвалення, надане цим факти Аїятола Хомейні та інших органів іранської держави, і рішення про їх ув'язнення переклало продовження окупації Посольства та затримання заручників у діях цієї держави [98].

Однак, наразі жодна держава не схвалила або ж визнала публічно діяння приватних суб'єктів, що здійснювали кібератаки, як свої власні. Більше того, коментар до Проєкту статей про відповідальність держав за міжнародно-протиправні діяння вказує на те, що для визнання держави відповідальною на підставі статті 11, недостатньо, щоб держава просто знала про наявність протиправно діяння приватних суб'єктів [85, с. 53]. Держава має також визнати таку протиправну поведінку, що може виражатись не лише у формі схвалення, а й вираженні шкоди за заподіяне [85, с. 53].

На наше переконання, можливість визнання держави відповідальною за вчинення кібератак приватними суб'єктами на підставі статті 11 більшою мірою залежить від її волі та наміру нести відповідальність. Маловірогідно, що держави добровільно визнають поведінку приватних суб'єктів у якості власної з тим, щоб у подальшому нести відповідальність за їх діяння. У зв'язку з цим, стаття 11 Статей про відповідальність держав за міжнародно-протиправні діяння є скоріше теоретичною підставою для притягнення держав до відповідальності, аніж практично можливою.

2.2. Кібератака у якості винного діяння держави

2.2.1. Незаконне втручання у внутрішні справи держави

Одним із можливих підходів до кваліфікації кібератак з точки зору протиправного міжнародно-правового діяння є порушення принципу втручання у внутрішні справи держави.

Принцип заборони втручання у внутрішні справи держави відображений у статті 2(7) Статуту ООН, відповідно до якого ООН не має права втручатись у внутрішні справи держави і держави не зобов'язані виносити ці справи на вирішення в порядку, передбаченому Статутом ООН [99]. Також у Декларації про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй 1970 року зазначено:

Ні держава чи група держав не має права втручатись, прямо або опосередковано, з будь-якої причини, у внутрішні та зовнішні справи іншої держави. Як наслідок, озброєне втручання і будь-які інші форми втручання або спроби погроз проти правосуб'єктності держави або проти її політичних, економічних або культурних основ, є порушенням міжнародного права [71].

Міжнародний суд справедливості ООН у справі Нікарагуа проти США зазначив, що принцип заборони втручання становить звичаєве право [88]. У цій справі Міжнародний суд справедливості ООН виділяє два критерії, які визначають, чи мало місце втручання з боку держави: по-перше, примус однієї держави по відношенню до іншої; по-друге, такий примус має бути спрямований проти справ, які кожна держава має право вирішувати самостійно, зокрема, політичні, економічні, соціальні, культурні, а також питання зовнішньої політики [88]. Міжнародний суд справедливості ООН також посилався на цей принцип у справі Демократична Республіка Конго проти Уганди, вказуючи що інтервенція може бути «з або без збройної сили, на підтримку внутрішньої опозиції всередині держави» [90].

Міжнародна група експертів у Таллінській книзі висловлює точку зору, що кібератака може вважатись втручанням у справи іншої держави, лише у випадку застосування примусу [9, с. 44]. Зокрема, втручанням може вважатись порушення захисних віртуальних бар'єрів, таких як, паролі, а також політичне втручання, зокрема, порушення роботи новинних сервісів, або онлайн сервісу якоїсь партії [9, с. 45].

І. Кіловату зазначає, що наразі регулювання принципу заборони втручання не відповідає новим реаліям у контексті кіберпростору [100, с. 169]. На

переконання автора, критерії до визначення втручання держави мають бути переглянуті [100, с. 169]. Зокрема, з огляду на відсутність фізичних складових та сильний вплив кібератак на внутрішні чи зовнішні справи держави, втручання має визначатись не за критерієм примусовості, а за критерієм сильної руйнівної сили [100, с. 169].

Відповідно, у контексті поручення принципу заборони втручання у справи іншої держави внаслідок кібератак вважаємо за необхідне проаналізувати природу державного суверенітету у кіберпросторі.

Відповідно до статті 2(1) Статуту ООН, Організація заснована на принципах суверенної рівності усіх її членів [99]. Також у Декларації про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй 1970 року зазначено, що усі держави користуються суверенною рівністю [71]. Вони мають «рівні права і обов'язки і є рівноправними членами міжнародної громади, незважаючи на різницю економічної, соціального, політичного чи іншого характеру» [71]. Зокрема, суверенна рівність включає такі елементи: «рівноправність у судовому порядку; держава користується правами, що притаманні при повному обсягу суверенітету; повага до інших держав; територіальна цілісність та політична незалежність; право вільно вибирати та розвивати політичну, соціальну, економічну та культурну системи; зобов'язання виконувати цілком і належним чином міжнародні зобов'язання» [71]. Окрім цього, Міжнародний суд справедливості ООН висловлював свою позицію стосовно суверенітету держав у декількох справах.

Зокрема, Міжнародний суд справедливості ООН у справі Сполучене Королівство Великобританії та Північної Ірландії проти Албанії зазначив, що «між незалежними державами, повага до територіального суверенітету є надзвичайно важливою основою міжнаціональних відносин» [101]. У справі Нікарагуа проти США, Міжнародний суд справедливості ООН також зазначив про необхідність поваги державного суверенітету, зазначивши, що суверенітет держав «поширюється на внутрішні води і територіальне море кожної держави, а також

повітряний простір над його територією» [88]. У справі Франція проти Туреччини, Міжнародний суд справедливості США зазначив: «першим і найважливішим обмеженням, покладеним міжнародними правом на державу - це відсутність існування дозволеної норми навпаки – це те, що вона не може здійснювати свою владу в будь-якій формі на території іншої держави» [102]. У справі Нідерланди проти США, арбітр Макс Хьюбер стосовно суверенітету держав зазначив: «суверенітет у відносинах між державами означає незалежність. Незалежність щодо частини земної кулі - це право здійснювати в ній, за винятком будь-якої іншої держави, функції держави» [103].

На основі висновків Міжнародного суду справедливості ООН можна дійти висновку, що суд прямо пов'язує суверенітет держав з територією. Проте як визначити суверенітет держави у кіберпросторі?

Варто звернути увагу на звіти Групи урядових експертів у галузі інформації та телекомунікацій в контексті міжнародної безпеки за 2013 та 2015 роки. Зокрема, у звіті 2013 року Група урядових експертів зазначила, що «суверенітет та міжнародні норми та принципи, що впливають з нього, застосовуються до поведінки держав у сфері діяльності з ІКТ, та в їх юрисдикції щодо інфраструктури ІКТ на їх території» [29]. У звіті 2015 року Група урядових експертів зазначила аналогічну позицію [31].

Ма Ксінмін визначає перелік прав та обов'язків держав у кіберпросторі. Зокрема, до прав держав у кіберпросторі науковець відносить: права щодо кіберінфраструктури, права на онлайн інформацію, публічне управління у кіберпросторі [104, с. 127]. До обов'язків держав належить: повага суверенітету інших держав, мирне використання кіберпростору, повага прав людини та основоположних свобод [104, с. 127].

Люк Чіркоп вважає за доцільне визначати, чи було порушено принцип суверенітету держави, виходячи зі ступеню втручання у справи держави [105, с. 9]. Відповідно, науковець розробив шкалу ступеню втручання у справи іншої держави внаслідок здійснення кібератак [105, с. 10-12]. Зокрема, шкала передбачає наступні форми втручання (від найменш до найбільш серйозних): відслідковування або

вилучення інформації; додавання інформації; маніпулювання інформацією; видалення інформації; завдання тимчасової втрати функціональності; завдання постійної втрати функціональності; завдання фізичної шкоди чи ураження [105, с. 10-12]. Відповідно, науковець виділяє чотири підходи до втручання у суверенітет держави у кіберпросторі. Першим таким підходом є завдання матеріальних збитків, що відповідає таким формам втручання у кіберпросторі, як завдання постійної втрати функціональності та завдання фізичної шкоди чи ураження [105, с. 12]. Оскільки на території кожної держави розташовується та чи інша інфраструктура, над якою держава здійснює контроль, то заподіяння шкоди її функціонуванню чи цілісності ставитиме порушення суверенітету [106, с. 11]. При цьому, така інфраструктура може бути розташована як на літаках, так і на морських суднах [106, с. 12]. Підтвердженням цьому є, наприклад, стаття 95 Конвенції Організації Об'єднаних Націй з морського права, відповідно до якої, військові кораблі користуються у відкритому морі повним імунітетом від юрисдикції будь-якої держави, крім держави прапора [107]. Міжнародна група експертів у Таллінській книзі також пов'язує суверенітет держави з контролем над кіберінфраструктурою та діями на її території [9, с. 15]. Так, кібератаки порушують суверенітет держави у разі, якщо вони завдають фізичної шкоди кіберінфраструктурі [9, с. 16]. Однак, у разі, якщо жодної фізичної шкоди не було завдано, питання щодо порушення державного суверенітету є неоднозначним [9, с. 16].

Другим підходом є так званий «проміжний підхід», за якого кібератаки середньої тяжкості можуть завдати шкоди та порушити суверенітет держави, зокрема, до них належать: додавання інформації; маніпулювання інформацією; видалення інформації; завдання тимчасової втрати функціональності [105, с. 13].

За третього підходу, «суворого підходу до недоторканості», порушенням принципу суверенітету буде вважатись будь-яке мінімальне завдання шкоди інфраструктурі держави [105, с. 14]. Відповідно, за цього підходу порушенням суверенітету держави становитимуть усі види втручання або втручання, що перевищує мінімальний поріг [105, с. 14]. Зокрема, до таких втручань можуть

належати: обмеження у доступі до даних, втрата функціональності або функціонування даних, заподіяння фізичної шкоди або травми [105, с. 15].

На наше переконання, прив'язка принципу суверенітету держави до завдання фізичної шкоди не є доцільним у контексті кібератак. Варто розглянути, зокрема, зазначений вище випадок атаки під час президентської передвиборчої кампанії США, де не було заподіяно фізичної шкоди, але кібератака становила втручання у процес, що є суверенним питанням для будь-якої держави. Також теоретично можна припустити ситуацію, коли внаслідок кібератак змінюються результати виборів. Не зважаючи на відсутність фізичної шкоди, громадяни позбавлені права самостійно вирішувати питання державного рівня. На переконання автора, при визначенні того, чи було порушено суверенітет держави, варто виходити не з виду чи форми кібератаки, а з об'єкту її ураження. Наприклад, сама лише кібератака, що спричинить порушення функціонування сайту чи сервісу приватної особи не становитиме порушення суверенітету. Проте, порушення функціонування урядових сервісів, веб-сайтів, особливо, за допомогою яких надаються послуги громадянам, може становити порушення принципу суверенітету держави.

2.2.2. Кібератака як застосування сили

Відповідно до статті 2(4) Статуту ООН, всі члени Організації Об'єднаних Націй утримуються у їх міжнародних відносинах від погрози силою або її застосування як проти територіальної цілісності або політичної незалежності будь-якої держави, так і будь-яким іншим чином, несумісним з Цілями Об'єднаних Націй [99].

Відповідно до статті 51 Статуту ООН, Статут жодною мірою не зачіпає права на індивідуальну або колективну самооборону, якщо буде здійснена збройний напад на Члена Організації, до тих пір, поки Рада Безпеки не прийме заходи, необхідні для підтримання міжнародного миру та безпеки [99].

З огляду на наявність понять «атака» та «збройна» атака, Нілс Мелзер зазначає, що статті 2(4) та 51 Статуту ООН створюють певну прогалину у

термінології, проте, науковець доходить до висновку, що обсяг статті 2(4) є ширшим, ніж статті 51, оскільки вона передбачає заборону не лише збройної, але і неозброєної сили, а також її непрямого застосування, а також загрози її застосування [108, с. 11].

Підтвердженням позиції щодо тлумачення категорії «застосування сили» з точки зору збройної сили, є визначення агресії, наведене у Резолюції Генеральної Асамблеї ООН 3314 (XXIX). У статті 1 додатку до Резолюції Генеральної Асамблеї ООН 3314 (XXIX) вказано, що під агресією розуміється саме збройне застосування сили [109]. Додаток до Резолюції Генеральної Асамблеї ООН 3314 (XXIX) також наводить невичерпний перелік діянь, що можуть бути визнані агресією, зокрема, вторгнення або атака збройних сил, збройна окупація, бомбардування, блокада збройними силами, відправлення державою воєнних загонів або груп тощо [109].

Науковець Сілвер у своїй роботі, присвяченій аналізу статті 2(4) ООН в контексті застосування кібератак також доходить до висновку, застосування сили все ж тлумачиться з точки зору збройної сили [110, с. 80]. Науковець аналізує у своїй праці питання щодо віднесення економічних та політичних санкцій до застосування сили і наводить такі аргументи: по-перше, автор посилається на працю Едварда Гордона, де аналізується історичний контекст прийняття Статуту ООН [110, с. 81]. Так історія прийняття Статуту свідчить про спроби міжнародної спільноти зменшити застосування збройної сили державами [111, с. 271-275]. По-друге, *travaux preparatoires* Статуту свідчить про відхилення пропозиції розширити застосування сили до економічних та політичних санкцій, оскільки у членів Організації не було спільного розуміння для підтримки цього рішення [110, с. 81]. По-третє, Міжнародний суд справедливості ООН у жодному своєму рішенні не тлумачив застосування сили у якості економічного чи політичного примусу [110, с. 81]. При співвідношенні статті 2(4) Статуту ООН та кібератак, автор доходить висновку, що кібер-атаки є «новою формою ворожої діяльності» [110, с. 82]. Проте, на рівні з економічними та політичними санкціями наразі вони не підпадають під обсяг регулювання статті 2(4) Статуту ООН, у той час як науковець вважає, що має бути застосований протилежний підхід [110, с. 82].

Одним із підходів до віднесення кібератак до застосування сили є тип застосованої «зброї». У Консультативному висновку Міжнародного суду справедливості ООН під назвою «Законність погроз або використання ядерної зброї» суд, в контексті аналізу статей 2(4) і 51 Статуту ООН, зазначив, що положення вказаних статей «не стосуються конкретної зброї. Вони застосовуються до будь-якого застосування сили, незалежно від застосованої зброї. Статут ні прямо забороняє, ні дозволяє використання будь-якої конкретної зброї» [112].

Якщо проаналізувати положення Статуту ООН, то у статті 41 сформульовані заходи впливу, які не є застосуванням збройної сили і які може застосовувати Рада Безпеки для реалізації своїх рішень [99]. У статті зазначено, що до таких заходів, зокрема, належать повне або часткове розірвання залізничних, морських, повітряних, поштових, телеграфних, а також інших засобів зв'язку [99]. На думку науковиці Уни Хетеуей та інших, стаття 41 може виступати на підтримку інструментального підходу до визначення кібератак з точки зору застосування сили [6, с. 846].

Інструментальний підхід є відносно простим у застосуванні до атак, що використовують воєнну зброю, оскільки доволі нескладно визначити зброю, за допомогою якої здійснювались такі атаки [6, с. 846]. Проте, кібератаки завдають не менш суттєву шкоду і без застосування традиційної зброї [6, с. 846]. З огляду на це, на переконання автора, такий підхід до визначення кібератак у якості застосування сили не є доцільним.

Альтернативним підходом до визначення того, чи мало місце застосування сили, є встановлення цілей та об'єктів, на які направлено такі атаки [6, с. 846]. Відповідно, за такого підходу необхідно визначити, чи було завдано шкоди об'єктам критичної інфраструктури [6, с. 847]. Відтак, ключовими питаннями є, по-перше, визначення в загальному, що саме належить до об'єктів критичної інфраструктури держави, а, по-друге, яким об'єктам критичної інфраструктури може бути завдано шкоди внаслідок здійснення кібератак.

Ліор Табанський доречно зауважує, що з розвитком технологій, комп'ютери були фактично інкорпоровані до функціонування традиційних систем об'єктів

критичної інфраструктури [4, с. 85]. Відповідно, науковець визначає об'єкти критичної інфраструктури як «систему з комп'ютерним виміром, яка контролює функціонування іншої фізичної системи, що має важливе значення для функціонування економіки та державної безпеки» [4, с. 85]. Якщо ж традиційні об'єкти критичної інфраструктури хоча б частково функціонують у кіберпросторі, це означає, що таким об'єктам може бути завдано фізичного ушкодження за допомогою кібератак [4, с. 85].

Відповідно, аналізуючи підходи до визначенні об'єктів критичної інфраструктури у першому розділі, та визначення об'єктів критичної інфраструктури в контексті кіберпростору, можна дійти висновку, що такі об'єкти стосуються основних сфер, що забезпечують життєдіяльність людини та функціонування держави. У випадку, якщо у таких сферах використовується комп'ютерне обладнання, то це автоматично робить такі об'єкти критично важливими з точки зору кібербезпеки. Це підтверджується прикладами здійснення кібер-атак в Естонії, Грузії, Україні та США, де було завдано шкоди банківським системам, урядовим сайтам та послугам, електростанціям. Відтак, на переконання автора, у аспекті кібербезпеки можна орієнтуватись на ті традиційні підходи, що визначають об'єкти критичної інфраструктури.

Іншим підходом до віднесення кібератак до застосування сили є характер спричинених наслідків [6, с. 847]. Цей підхід визначає ступінь тяжкості спричинених наслідків. При цьому під тяжкістю може розумітись як серйозність завданої шкоди, так і причинно-наслідковий зв'язок між кібератакою і кінцевою завданою шкодою [6, с. 847]. Міжнародний суд справедливості ООН у справі Нікарагуа проти США вказав, що окреме діяння може визначатись у якості збройної сили з урахуванням його масштабу і завданих наслідків [88]. Проте, не усі судді погодились із таким підходом Міжнародного суду справедливості ООН [113].

У той же час, суд не вказав, які саме наслідки і масштаб становитиме застосування збройної сили. У зв'язку з цим вчені пропонують власні підходи до визначення наслідків, що дозволять віднести кібератаки до застосування сили. Зокрема, Шмітт пропонує орієнтуватись на якісні наслідки здійснення кібератак,

ніж на кількісні [114, с. 288]. Автор переконаний, що втручання, завдання шкоди чи маніпулювання інформацією не становитиме застосування збройної сили, оскільки це знизить допустимий рівень, коли держави можуть правомірно відповідати на такі атаки проти них [114, с. 288]. У той же час, фізичні наслідки також є досить вузьким підходом до визначення ступеню завданих наслідків, що характеризують застосування збройної сили. Натомість, у контексті визначення наслідків, що дозволяють віднести кібератаки до застосування сили, можна включати серйозні економічні наслідки, або втручання у соціальні функції [114, с. 288].

Група експертів Таллінської книги наводить цілий ряд критеріїв, що характеризують наслідки як такі, що дають підстави вважати кібератаки застосуванням сили. До таких факторів належить: тяжкість (наприклад, завдання шкоди особами чи майну буде вважатись застосуванням сили); швидкість настання (чи мають держави час врегулювати конфлікт мирним шляхом або іншим чином попередити негативні наслідки); безпосередність (ступінь причинно-наслідкового зв'язку між атакою і наслідками); ступінь втручання (ступінь захищеності системи держави, на яку було здійснено кібератаку); можливість визначення наслідків (легкість ідентифікації наслідків та їх очевидність); воєнний характер (зв'язок кібератак з воєнними операціями); втручання держави (ступінь державного втручання у процес здійснення кібератак); презумпція законності (визначення, чи заборонене те чи інше діяння у кіберпросторі міжнародним правом) [9, с. 48-51]. Проте, група експертів зазначає, що наведені критерії не є вичерпними, і держави можуть також враховувати політичну обстановку, особу, що здійснила атаку, тип ураженої інфраструктури [9, с. 51-52]. На основі запропонованих групою критеріїв, Філіп Пул, посилаючись на працю Майкла Джервейса, доходить до висновку, що кібератаки, здійснені в Естонії, не можна вважати застосуванням сили, оскільки кібератаки завдали скоріше незручності, а не суттєві ушкодження [95, с. 310].

Деніел Сілвер, аналізуючи критерії, запропоновані групою експертів, вважає за необхідне кваліфікувати кібератаки у якості застосування сили на підставі критерію тяжкості. При цьому, науковець вважає, що застосування сили має лише

тоді місце, коли завдано фізичної шкоди або матеріальної шкоди [110, с. 84-85]. Це доволі вузький підхід до кваліфікації кібератак, проте такий підхід науковця можна пояснити тим, що він розглядає кібератаки у якості збройного застосування сили. При цьому Сілвер визначає критерії, за якими до кібератак можна застосувати положення статті 2(4) Статуту ООН у випадках, коли: кібератаки є не єдиною формою діяльності, кібератаки спричиняють пряму і передбачувану фізичну шкоду, вид шкоди є подібним до того, що спричиняється у випадку традиційного застосування сили та наслідки мають не лише економічний та політичний характер [110, с. 84-85]. Щодо останнього критерію, то Уна Хетеуей навпаки зауважує, що кібератаки якраз таки можуть бути здійснені з економічною або політичною метою [6, с. 842].

Якщо ж використовувати підхід за наявності серйозних наслідків для визначення того, чи мало місце застосування сили з точки зору завданих збитків на прикладі Стакснету в Ірану, то, можна дійти висновку, що ця атака не є застосуванням сили, оскільки не було жодного фізичного знищення, що становило б руйнування, спричинене збройною силою, а також атака з використанням Стакснету не призвела до втрати життя [89, с. 871].

Іншої точки зору дотримується Ендрю Фольц. Він аналізує випадок зі Стакснет на основі критеріїв, вироблених Групою експертів Таллінської книги для визначення ступеню серйозності завданих ним наслідків. З точки зору тяжкості, Стакснет є застосуванням сили, оскільки він все ж таки завдав фізичної шкоди об'єктам критичної інфраструктури [115, с. 44]. До того ж, тривалість завданих Стакснетом збитків, оскільки у Ірану протягом певного часу відбулась затримка у розвитку ядерної програми [115, с. 44]. З точки зору негайності, Стакснет не можна вважати застосуванням сили, оскільки у Ірану був час для того, щоб виявити атаку і зменшити шкідливі наслідки [115, с. 44]. З точки зору безпосередності, то очевидним є зв'язок між Стакснетом і шкодою, завданою центрифугам [115, с. 44]. З точки зору ступеню втручання, то це є прямим втручанням у суверенітет Ірану, оскільки Стакснет завдав шкоди важливим захищеним системам країни [115, с. 44-45]. З точки зору можливості визначення наслідків, оскільки велика кількість

центрифуг перестала працювати внаслідок кібер-атаки, то Стакснет є застосуванням сили з точки зору цього критерію [115, с. 45]. З точки зору презумпції законності, то Стакснет не можна вважати дозволеним з точки зору міжнародного права, оскільки він завдав шкоди ядерним установкам Ірану [115, с. 45]. І хоча жодну державу не було притягнуто до відповідальності за здійснення кібер-атаки на Іран, на переконання Ендрю Фольца, за вказаними критеріями винну державу можна визнати відповідальною за застосування сили [115, с. 44-45].

Головним недоліком підходу щодо визначення застосування сили з точки зору спричинених наслідків є те, що неможливо точно визначити які саме наслідки становитимуть застосування сили у кіберпросторі. Максимум, що можуть завдати кібератаки – це ураження інфраструктури, фінансових мереж, електричні мережі тощо. Відтак, за відсутності уніфікованих критеріїв, визначення наслідків, що становлять застосування сили залишається суб'єктивним фактором. У той же час, на наше переконання, з усіх вище перелічених підходів при визначенні того, чи є кібератака застосуванням збройної сили, найбільш прийнятним є саме підхід за спричиненими наслідками.

2.2.3. Кібератаки як результат порушення принципу належної обачності

Принцип належної обачності передбачає обов'язок держав поважати суверенітет інших держав та не дозволяти використовувати власну територію для здійснення міжнародних протиправних діянь [31]. Цей принцип набув найбільшого поширення у міжнародному довкільному праві. Окрім цього, Міжнародний суд справедливості ООН та Рада Безпеки ООН неодноразово посилялись на принцип належної обачності при кваліфікації діянь держав. Зокрема, відповідно до рішення Міжнародного суду справедливості ООН у справі Сполучене Королівство Великобританія проти Північної Ірландії: «зобов'язанням кожної держави є свідомо не дозволяти використовувати її територію для дій, що суперечать правам інших держав» [101]. У справі Нікарагуа проти США Міжнародний суд

справедливості ООН також наголосив про необхідність поваги політичної цілісності держави [88]. У справі Боснія і Герцеговина проти Сербії та Чорногорії Міжнародний суд справедливості ООН зазначив про відповідальність держави, яка, незважаючи на можливість, не здійснила усіх належних заходів для запобігання порушенню [87]. У цьому ж рішенні суд навів ряд критеріїв для визначення того, чи порушено державою принцип належної обачності. До першого критерію належить можливість вплинути на поведінку інших осіб. Цей критерій, зокрема включає, такі аспекти як географічна віддаленість від місця вчинення порушення, а також зв'язків держави з особами [87]. До того ж, окрім можливості впливу на осіб, варто також звернути увагу на правові засоби, надані міжнародним правом державі для попередження протиправної поведінки [87]. Відтак, Міжнародний суд справедливості ООН визнав порушення принципу належної обачності з боку Югославії з огляду на політичні, воєнні та фінансові зв'язки з утвореннями Боснії та Герцеговини, що не могло не свідчити про її обізнаність з можливими ризиками [87].

Окрім цього, у справі Сполучені Штати Америки проти Канади, Трибунал зазначив: «жодна держава не має права використовувати або дозволяти використання своєї території таким чином, щоб заподіяти шкоду ... на території або по відношенню до території або об'єктам чи особам на ній, коли справа має серйозні наслідки і шкода встановлена чіткими та переконливими доказами» [116].

Хоча наразі чітких критеріїв принципу належної обачності не було вироблено, варто звернути увагу на статей щодо Попередження транскордонної шкоди від небезпечної діяльності. Так, у статтях 3-6 наведено такі форми належної обачності: зобов'язання здійснити відповідні заходи для запобігання значної транскордонної шкоди або в будь-якому випадку для мінімізації її ризику (стаття 3); зобов'язання добросовісно співпрацювати та за необхідності звертатися за допомогою до однієї або кількох компетентних міжнародних організацій у запобіганні значній транскордонній шкоді (стаття 4); зобов'язання вжити необхідних законодавчих, адміністративних чи інших дій, включаючи створення відповідних механізмів моніторингу (стаття 5); та ставити вимогу про отримання

дозволу на діяльність, що входить у сферу дії статей, що здійснюється на її території або іншим чином знаходиться під її юрисдикцією або контролем [117].

Відповідно, Ліу Я. Ю. пропонує застосовувати вказаний перелік зобов'язань держав і до відносин у кіберпросторі [118, с. 205]. Проте, при застосуванні вказаних критеріїв до визначення дотримання державою обов'язку належної обачності, варто враховувати специфіку кібератак. По-перше, варто враховувати технічні можливості держави попередити кібератаку або припинити її [121, с. 74]. Держави не мають нести відповідальність за неможливість їх попередження через обмеженість власних технічних можливостей [121, с. 74]. Так, Група з міжнародного права, що досліджує зобов'язання з належної обачності зауважує про необхідність врахування контексту, в якому виникає такий обов'язок [119]. Відтак, слушним є твердження Міжнародного Трибуналу з морського права, який у одному зі своїх Консультативних висновків, досліджуючи концепцію запобіжного заходу, розмежував розвинені країни та країни, що розвиваються і зазначив: «у конкретній ситуації враховується рівень наукових знань та технічні можливості, доступні певній державі у відповідних наукових та технічних галузях» [120].

По-друге, важливо враховувати баланс між шкодою, що може бути спричинена кібератаками, та наслідками для держави, яка має здійснити заходи для їх попередження [121, р. 75]. Відповідно, у разі, якщо шкода, заподіяна внаслідок кібератак є незначною, а заходи, спрямовані на їх попередження чи усунення будуть обтяжливими, держава не має вважатись такою, що порушила принцип належної обачності [121, р. 75]. Відповідно, обов'язок щодо дотримання принципу належної обачності виникає, коли кібератаки завдають шкоди населенню, спричиняють фізичну шкоду або руйнування, порушують функціонування мережі, збирання інформації, а також здійснення комп'ютерних злочинів [118, с. 244-251].

По-третє, обов'язок щодо дотримання принципу належної обачності виникає лише у тому випадку, коли держава обізнана про протиправні діяння, що вчиняються на її території [118, с. 232]. Проте, ступінь і форма обізнаності держави може бути різною у кожному окремому випадку. Наприклад, держава може мати дійсні знання про кібератаку, може допускати вчинення кібератак, знаючи про

наявну можливість їх здійснення, або ж є докази, що держава могла знати про вчинення кібератак [118, с. 233].

Генеральна Асамблея ООН у Резолюції 55/63 здійснила спробу окреслити обов'язки держав здійснити заходи, необхідні для запобігання вчиненню неправомірному використанню інформаційних технологій. Зокрема, до таких Генеральна Асамблея ООН віднесла: розроблення законодавчих механізмів, які б не дозволяли використовувати територію держави у якості безпечного місця для неправомірного використання інформаційних технологій; захист комп'ютерних систем, зокрема за допомогою розроблених правових механізмів; інформування населення про необхідність запобігання неправомірному використанню інформаційних технологій; розроблення інформаційних технологій, які б дозволили ідентифікувати, відстежувати та збирати необхідні докази про неправомірне використання інформаційних технологій; та розробляти необхідні рішення для захисту прав і свобод людини [122].

Під час сесії Робочої групи відкритого типу з питань розвитку інформації та телекомунікацій у контексті міжнародної безпеки яка тривала з 8 по 12 березня 2021 року, декілька держав висловили власні позиції, щодо удосконалення керівних принципів, визначених у звіті 2015 року, що стосуються безпеки держав у кіберпросторі. Зокрема, Канада звернула увагу на пункт 13 (с) Звіту Групи урядових експертів за 2015 рік [123, с. 11]. Цей пункт фактично адаптує положення принципу належної обачності до відносин держав у кіберпросторі, забороняючи державам дозволяти використовувати свої території іншим суб'єктам для зловмисного використання інформаційно-телекомунікаційних технологій [31]. Канада запропонувала досить розгорнутий перелік дій як ураженої держави, так і держави, з території якої здійснюються кібератаки. По-перше, якщо держава виявить кібератаку, здійснену з території іншої держави, вона має надіслати повідомлення такій державі, що може містити інформацію про IP адресу та комп'ютери, з яких здійснювалась кібер-атака [124, с. 11]. У свою чергу, держава, з території якої здійснюється кібер-атака, має вжити усіх необхідних заходів, щоб припинити протиправне діяння [124, с. 11]. У разі, якщо держава не володіє

достатньою кількістю засобів, необхідних для припинення таких протиправних діянь, вона може звернутись за допомогою до інших держав, або ж приватних суб'єктів [124, с. 12]. Також, держави мають вживати всіх необхідних заходів, щоб запобігти здійсненню шкідливих операцій з використанням інформаційно-телекомунікаційних технологій на шкоду третім особам [124, с. 12].

2.3. Висновки до Розділу 2

Таким чином, внаслідок відсутності єдиного міжнародного акту, який би регулював права та обов'язки держав у кіберпросторі, необхідно керуватись тими нормами та принципами, які були розроблені державами та існують на сьогодні. Оскільки доволі часто кібератаки здійснюються не безпосередньо самими представниками держави, а за допомогою приватних суб'єктів, то першою проблемою при визнанні певної держави відповідальною, є встановлення зв'язку між нею та безпосередньо приватними суб'єктами. Варто взяти до уваги Статті про відповідальність держав за міжнародно-протиправні діяння. На основі них можна дійти висновку, що підставами для визнання поведінки приватних суб'єктів державі є: визнання приватних осіб у якості де факто органу; здійснення контролю державою над поведінкою приватних суб'єктів; визнання поведінки приватних суб'єктів у якості власної. Однак, на практиці встановити належність поведінки приватних суб'єктів державі є досить складним завданням. Це підтверджується практикою Міжнародного суду справедливості ООН, який встановлює досить високі стандарти зв'язку держави і приватних осіб. Зокрема, така проблема пов'язана з визначенням ступеню контролю держави над поведінкою приватних суб'єктів. Вважаємо за необхідне застосовувати до відносин між державою та приватними суб'єктами не стандарт «ефективного контролю», а стандарт «загального контролю», який передбачає керування не кожною окремою операцією, а надання загальних інструкцій. Інакше, за умови здійснення кібератак приватними особами, притягнути державу до відповідальності державу буде майже неможливо.

Щодо визнання кібератак у якості протиправного діяння, то за відсутності міжнародного акту, присвяченому регулюванню кібератак, вважаємо за доцільне керуватись нормами та принципами міжнародного права, що регулюють здійснення збройних атак. До них належить принцип заборони втручання у внутрішні справи держави, заборона застосування сили та обов'язок дотримання принципу належної обачності. Вважаємо, що принцип заборони втручання у внутрішні справи держави завжди має місце при здійсненні кібератак на об'єкти критичної інфраструктури держав, оскільки так чи інакше кібератаки спрямовуються на завдання шкоди або перешкоджанню функціонування таких об'єктів. Щодо заборони застосування сили, то вважаємо за доцільне застосовувати цей принцип лише за наявності серйозних ушкоджень об'єктів або осіб іншої держави. Обов'язок дотримання принципу належної обачності також виникає у держав, з територій яких здійснюються кібератаки. Проте, необхідно враховувати обізнаність держав про здійснення кібератак з їх територій.

РОЗДІЛ 3.

СУЧАСНІ ВИКЛИКИ

3.1. Можливі відповіді уражених держав на кібератаки

3.1.1. Застосування права на самооборону

Стаття 51 Статуту ООН встановлює, що статут жодним чином не зачіпає невід’ємне право на індивідуальну чи колективну самооборону, якщо буде здійснено збройний напад на Члена Організації, до тих пір, поки Рада Безпеки не здійснить заходи, необхідних для підтримання міжнародного миру та безпеки [99]. Проте, право на самооборону виникає лише тоді, коли має місце застосування збройної сили [88]. При цьому, згідно позиції Міжнародного суду справедливості ООН у справі Нікарагуа проти США, для визначення того, чи мало місце застосування збройної сили, необхідно визначити обсяг і наслідки такої атаки [88].

Шмітт зазначає, що в контексті кібербезпеки, право на самооборону викликає два основні питання: по-перше, чи виникає таке право у разі, коли кібератака не завдає фізичної шкоди та, по-друге, співвідношення між застосуванням сили та застосуванням збройної сили [125, с. 282-284]. На переконання Шмітта, оскільки поки що відсутній підхід до визначення, який саме ступінь тяжкості кібератаки буде становити збройну силу, держави будуть використовувати право на самооборону у тих випадках, коли наслідки достатньо серйозні [125, с. 283]. Оскільки кібератаки можуть завдати значної шкоди нормальному функціонуванню держави, то підхід до трактування права на самооборону однозначно зазнає змін [125, с. 283].

У випадку, якщо держава все ж таки має право на самооборону, вона має дотримуватись принципів пропорційності, необхідності. Такі критерії не зазначені безпосередньо у самому Статуті ООН. Також ці принципи були сформульовані судовою практикою Міжнародного Суду Справедливості ООН. Так у справі Нікарагуа проти США, суд зазначив: «визначення, чи була відповідь на атаку

правомірною, залежить від дотримання критеріїв необхідності та пропорційності заходів, здійснених у якості самооборони» [88]. У Консультативному висновку під назвою «Законність погроз або використання ядерної зброї», Міжнародний суд Справедливості ООН вказав, що дотримання принципів пропорційності і необхідності при реалізації права на самооборону є звичаєвим правом [112]. У справі Іранська Республіка проти Сполучених Штатів Америки суд також зазначив про необхідність дотримання державами вказаних принципів у випадку застосування права на самооборону [126].

Загалом, принцип необхідності означає, що застосування державою сили є єдиним можливим заходом для протидії збройному нападу [9, с. 62]. З точки зору кібербезпеки, виникає безліч питань: в якій формі держава може скористатись правом на самооборону, чи така самооборона має бути кібератакою, що не становить застосування збройної сили, чи може бути застосована у відповідь кінетична (фізична) сила. Група експертів висловлює позицію, відповідно до якої уражена держава має право на самооборону у разі, коли не вдалось мирно вирішити спір, застосувати кібератаку проти держави, що першою здійснила атаку [9, с. 62]. Філіп Пул зазначає у свою чергу, що при реалізації права на самооборону, така самооборона не обов'язково має бути здійснена у ідентичній атаці формі. Відтак, на переконання науковця, при кібератаці, що призвела, наприклад, до відмови в обслуговуванні, уражена держава у відповідь може застосувати кінетичну силу, наприклад, повітряну атаку для знищення обладнання, з якого було здійснено кібератаку [95, с. 313]. Аналогічної позиції притримується і Шаап, посиляючись на позицію Консультативному висновку Міжнародного суду справедливості ООН під назвою «Законність погроз або використання ядерної зброї» стосовно відсутності обмежень щодо виду застосовної у відповідь атаки [2, с. 148-149]. У свою чергу, Ваксман, наголошує на важливості застосування збройної відповіді на кібератаки з двох причин: по-перше, з метою захисту об'єктів критичної інфраструктури; по-друге, для попередження подальших кібератак [127, с. 116].

Хоча, на переконання автора, такий підхід є дещо суперечливим, оскільки, по-перше, застосування вогнепальної зброї не відповідатиме критерію

пропорційності, а, по-друге, знищення обладнання далеко не завжди є можливим, з огляду на те, що комп'ютери, з яких здійснюються кібер-атаки, часто використовуються хакерами не на території державних об'єктів, а на приватній території.

Дотримання принципу пропорційності передбачає визначення дозволеного обсягу зброї, що може бути застосований під час самооборони [9, с. 62]. Також варто взяти до уваги статті 51(5)(b) та 57 Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів. Так, відповідно до статті 51(5)(b) Додаткового протоколу, невідбирковим є напад, котрий, як можна очікувати, попутно потягне за собою втрати життя серед цивільного населення, поранення цивільних осіб та шкоду цивільним об'єктам, або те й інше разом, які були б надмірними щодо конкретної і безпосередньої воєнної переваги, якої передбачається таким чином досягти [128]. Також відповідно до статті 57 Додаткового протоколу, при проведенні воєнних операцій повинна постійно виявлятися турбота про те, щоб оберігати цивільне населення, цивільних осіб і цивільні об'єкти [128]. З огляду на положення зазначених статей, дотримання принципу пропорційності є дещо ускладненим в контексті атаки в межах кіберпростору, оскільки велика кількість операцій здійснюється у загальнодоступних цивільних мережах [95, с. 313].

Міжнародна група експертів у Таллінській книзі також зауважує, що право на самооборону виникає не лише тоді, коли атаку було завдано, а і тоді, коли така атака є неминучою [9, с. 63]. На підтвердження своєї позиції, міжнародна група експертів наводить Керолайн тест, який був вперше сформульований у листі Деніела Вебстера, адресованого Лорду Ешбуртону. Відповідно до вказаного тесту, право на самооборону виникає тоді, коли «необхідність такої самооборони є миттєвою, переважаючою і відсутній вибір засобів, а також час для роздумів» [129]. Однак, для завчасного застосування права на самооборону необхідно відрізнити від підготовчі дії від початкової стадії атаки [9, с. 65]. Відтак, на початкову стадію атаки можуть вказувати рішення держави щодо здійснення атаки, період часу,

протягом якого у потенційно враженої держави буде можливість відповісти на атаку [9, с. 65].

Проте, право на самооборону викликає не мало питань на практиці. Одним із таких є можливість застосування права на самооборону у відповідь на кібератаки, здійснені приватними особами за вказівкою держави. При цьому, кібератаки часто здійснюються приватними суб'єктами за вказівкою держави на територіях інших держав. У такому разі, виникає питання, якщо країна «А» дала вказівку приватним особам здійснити кібератаку з території «Б», то чи має право уражена держава «В» застосувати право на самооборону як проти держави «А», так і проти держави «Б»? Частково відповідь на це питання дає Міжнародний суд справедливості ООН, який у справі Демократична Республіка Конго проти Уганди не визнав права на самооборону Угандою проти Конго, оскільки остання не була жодним чином залучена до атак, що здійснювались з її території [90]. Таким чином, Міжнародний суд справедливості ООН заперечує можливість застосування права на самооборону проти держави, з території якої здійснено атаки, але яка жодним чином не залучена до їх здійснення [89, с. 887].

Іншим питанням в контексті права на самооборону є можливість його застосування проти самих приватних суб'єктів. Зокрема, у Консультативному висновку «Правові наслідки будівництва стіни на окупованій палестинській території» Міжнародний суд справедливості ООН зазначив про незастосовність статті 51 Статуту ООН, оскільки: «стаття 51 Статуту визнає існування невід'ємного права на самооборону у випадку збройної атаки однією державою проти іншої. Однак, Ізраїль не заявляла про те, що атаки, здійснені проти неї, здійснені іноземною державою» [130]. Однак, на відміну від позиції Міжнародного суду ООН, Рада Безпеки ООН висловлювала позицію на підтримку права на самооборону, наприклад, у випадку здійснення тероризму. Зокрема, у Резолюції 1368, яка була прийнята у відповідь на терористичну атаку 11 вересня 2001 року, Рада Безпеки виразила готовність відповісти на терористичні атаки і визнала право на самооборону [131]. Аналогічну позицію Рада Безпеки визначила у Резолюції 1373, зауваживши про можливість застосування і колективної самооборони [132].

Однак, для реалізації права на самооборону потрібно чітко ідентифікувати державу, що здійснює кібератаки. У кіберпросторі це питання постає досить гостро. По-перше, є можливість застосувати так звані проксі сервери [133]. Такі сервери дозволяють приховати справжню IP адресу суб'єкта здійснення атак. По-друге, навіть якщо встановити, з території якої країни здійснюється кібератака, це не означає, що така держава дійсно причетна до організації кібератак. Наприклад, під час здійснення кібератак проти Грузії, суб'єкти кібератак розташовувались в різних країнах, зокрема, Латвії та Україні [49, с. 3]. Відповідно, держави постають перед дилемою: або ж не здійснювати жодних дій у відповідь, або ж реалізувати право на самооборону, ризикуючи нести відповідальність, якщо такі заходи будуть спрямовані проти держави, що не була причетна до кібератак [89, с. 884-885].

3.1.2. Застосування санкцій ураженими державами

Альтернативною відповіддю уражених кібератаками держав, яка наразі починає застосовуватись державами, може бути застосування санкцій.

Наприклад, після здійснення кібератак у 2016 році під час передвиборчої гонки у США, тодішній Президент Сполучених Штатів Барак Обама вирішив прийняти декілька указів, що стосувались блокування активів осіб, залучених до кібератак [134;135]. Перший такий указ було прийнято 1 квітня 2015 року, який розповсюджувався на: осіб, що прямо або опосередковано були залучені у кібердіяльності, що були здійснені або які керувались особами, що знаходились за межами Сполучених Штатів Америки і в результаті яких було завдано значної шкоди національній безпеці, закордонній політиці, економічній та фінансовій стабільності; осіб, які отримали будь-яким чином вигоду від таємної інформації, що була отримана ними у результаті здійснення кібератак; осіб, які надавали фінансову, матеріальну чи технічну допомогу у здійсненні кібероперацій; осіб, які намагались взяти участь у кіберопераціях [135]. До кібероперацій Указ відносив: пошкодження комп'ютерної мережі або серверів, які забезпечували роботу критично важливої інфраструктури; перешкоджання у доступі до комп'ютерів чи

комп'ютерної мережі; привласнення грошових коштів, комерційної таємниці, особистої інформації для отримання переваги або особистої фінансової вигоди [135]. Указом було накладено заборону на отримання зазначеними особами майна та активів у власність, а також їх розпорядження [135].

Указ від 28 грудня 2016 року доповнив Указ від 1 квітня 2015 року таким видом кібероперації як фальсифікація, зміна чи незаконне отримання інформації для втручання у виборчий процес [134]. Окрім цього, Барак Обама оголосив персонами non-grata тридцять п'ять дипломатів та консулів Російської Федерації [134].

Окрім цього, нещодавно, 15 квітня 2021 року Президент Сполучених Штатів Америки Джон Байден видав Указ Про блокування майна внаслідок визначеної шкідливої зовнішньої діяльності уряду Російської Федерації. Зазначеним Указом передбачається накладення санкцій на осіб, які тим чи іншим чином були причетні до здійснення кібератак [136]. Указ також передбачав заборону розпорядження будь-яким майном, яке належало особам, причетних до здійснення кібератак. Так, до таких осіб було віднесено, зокрема, тих, які здійснюють діяльність у технологічному, оборонному секторі або економічному секторі Російської Федерації; тих, які прямо або побічно були залучені до здійснення зловмисних кібероперацій; осіб, які належать до керівного складу: уряду Російської Федерації, утворень, чії учасники причетні до вчинення зловмисних кібероперацій; члени політичного утворення Російської Федерації; родичі осіб, які були залучені до здійснення зловмисних кібероперацій; осіб, які надавали матеріальну або фінансову допомогу; осіб, які діяли від імені уряду Російської Федерації [136].

30 липня 2020 року Рада Європейського Союзу застосувала санкції до приватних осіб та організацій, причетних до здійснення кібератак на інформаційні системи держав-членів Європейського Союзу [137]. Не зважаючи на те, що санкції стосувались більшою мірою приватних осіб, деякі з них були частиною урядових угруповань Російської Федерації. Наприклад, Олег Сотніков брав участь у здійсненні кібератаки у складі розвідувальної групи російських збройних сил [137]. Група намагалась здійснити несанкціонований доступ до мережі Організації з

заборони хімічної зброї [137]. Окрім цього, санкції були накладені на Головний центр спеціальних технологій Головного управління Генерального штабу Збройних Сил Російської Федерації. Шкідливе програмне забезпечення «NotPetya» та «EternalPetya» призвело до перешкоджання доступу до даних ряду компаній як Європейського Союзу, так і поза його межами, що завдало значних економічних збитків [137].

Вважаємо, що наразі застосування санкцій хоча і частково, але вже ж забезпечує реалізацію механізму притягнення винних осіб до відповідальності. Однак, такі санкції не завжди спрямовані проти посадових осіб держав, що брали участь у кібератаках. Це слугує ще однією підставою для залучення приватних осіб для здійснення кібератак.

3.2. Розроблення єдиного міжнародного акту, що регулює поведінку держав у кіберпросторі

Як нами було вже зазначено раніше, на сьогодні міжнародна спільнота не розробила акту, який би визначав єдиний підхід до належної поведінки держав у кіберпросторі. У зв'язку з цим, не зважаючи на численну кількість випадків кібератак, спрямованих проти об'єктів критичної інфраструктури держав, жодну країну не було притягнуто до відповідальності. Питання щодо розроблення єдиного акту, який би врегулював діяльність держав у кіберпросторі, неодноразово поставало на міжнародному рівні.

При розробці уніфікованого акту, варто керуватись фундаментальними принципами, встановленими Статутом ООН, зокрема, рівність суверенних держав, заборона втручання у внутрішні справи, мирне врегулювання спорів [99]. Окрім цього, необхідним є дотримання балансу між загальним міжнародним правом та спеціальним правом, що регулює відносини у кіберпросторі [104, с. 131]. Наприклад, концепція ефективного контролю, що визнана Міжнародним судом справедливості ООН, не є належною для застосування до відносин у кіберпросторі,

оскільки держави дають лише певне завдання приватним особам, які в подальшому реалізують його за допомогою технічних засобів.

Також необхідно забезпечити баланс між національним та міжнародним правом, для визначення питань, які підлягають регулюванню міжнародним правом чи національним [104, с. 131]. Насамкінець, важливим є баланс між мирними та примусовими заходами для найбільш ефективного врегулювання спорів [104, с. 131].

Відтак, першим кроком до уніфікації правил у кіберпросторі може стати декларація, яка визначатиме загальні принципи поведінки та слугуватиме своєрідним керівництвом поведінки для всіх держав. Ма Ксінмін пропонує включити до декларації, зокрема, наступні принципи: застосування загального міжнародного права, включаючи Статут ООН, до відносин у кіберпросторі; міжнародна співпраця у кіберпросторі; мирне використання кіберпростору; захист свободи у кіберпросторі; запобігання вчинення та відповідальність за кіберзлочини [104, с. 132]. Наступним кроком є розроблення та прийняття конвенції, що визначатиме права та обов'язки держав, а також відповідальність за порушення зобов'язань у кіберпросторі [104, с. 132].

Наразі міжнародна спільнота лише знаходиться на стадії розроблення єдиних правил поведінки держав у кіберпросторі.

Першим проявом реакції ООН була Резолюція 53/70, прийнята на основі пропозиції Російської Федерації у 1998 році [138].

У 2004 році була створена Група урядових експертів у галузі інформації та телекомунікацій в контексті міжнародної безпеки, яка досліджувала питання міжнародної безпеки в контексті інформаційних та телекомунікаційних загроз [138]. Як уже зазначалось раніше у 2010, 2013 та 2015 роках Група урядових експертів та у 2021 році Робоча група відкритого типу з питань розвитку інформації та телекомунікацій у контексті міжнародної безпеки підготували звіти, що слугують рекомендаціями для держав щодо належної поведінки у кіберпросторі [29; 30; 31; 139]. Відтак, вважаємо за доцільне зупинитись більш детально на їх характеристиці.

Зокрема, у звіті від 30 липня 2010 року Група Урядових Експертів запропонувала країнам: вести діалог щодо розроблення норм у сфері інформаційно-комунікаційних технологій, які б захистили національну та міжнародну інфраструктуру; поширювати національні погляди на використання інформаційно-телекомунікаційних технологій під час конфлікту; обмінюватись інформацією щодо національного законодавства, стратегій, технологій, політик і кращих практик у сфері інформаційно-телекомунікаційних технологій; визначити заходи для розбудови потенціалу менш розвинених країн; та розробити загальноприйняті терміни і визначення у відповідності з Резолюцією Генеральної Асамблеї 64/25 [139].

У 2013 році Група урядових експертів розробила більш детальні рекомендації для країн щодо співпраці у сфері інформаційно-телекомунікаційних технологій, розділивши їх на три окремі групи: рекомендації стосовно норм, правил та принципів відповідальної поведінки держав; рекомендації щодо заходів зміцнення довіри та обміну інформацією; та рекомендації щодо заходів розбудови потенціалу [29]. Зокрема у першій групі принципів зосереджені рекомендації щодо тісної співпраці у сфері захисту прав людини та основоположних свобод, протидії кримінальному чи терористичному використанню інформаційно-телекомунікаційних технологій, гармонізації правових підходів та зміцненні взаємодії між відповідними органами виконавчої влади та органами розслідування [29]. Також Група урядових експертів надала рекомендацію, щоб держави забезпечили, що на їх територіях недержавні суб'єкти не використовуватимуть інформаційно-телекомунікаційні технології незаконним способом [29]. До другої групи рекомендацій належить обмін інформацією, стратегіями, політиками для підвищення міжнародної співпраці; розроблення двосторонніх, регіональних та багатосторонніх консультативних механізмів; обмін інформацією щодо випадків в галузі безпеки інформаційно-телекомунікаційних технологій [29]. До третьої групи рекомендацій належить підтримка і розвиток електронного навчання, тренування та підвищення обізнаності щодо безпеки у сфері інформаційно-телекомунікаційних технологій, зміцнення можливостей національних правових напрацювань,

можливостей реалізації права, протидії використанню інформаційно-телекомунікаційних технологій у кримінальних і терористичних цілях [29].

У 2015 році Група урядових експертів розробила ще один звіт, де надала рекомендації щодо заходів зміцнення довіри та міжнародної співпраці та допомоги у сфері безпеки інформаційно-телекомунікаційних технологій та зміцнення потенціалу [31]. Ці рекомендації певним чином повторюють ті, які були надані Групою експертів у звітах за 2010 та 2013 роки. Проте, до нових рекомендацій Групи експертів можна віднести надання державами власних національних підходів до визначення критичних об'єктів інфраструктури, зокрема, підходів національного законодавства і політик у цій сфері, розвиток механізмів та процесів для двосторонніх, регіональних, субрегіональних та багатосторонніх консультацій щодо захисту об'єктів критичної інфраструктури, класифікація випадків у сфері безпеки інформаційно-телекомунікаційних технологій для визначення ступеню та серйозності випадку для цілей обміну інформацією між країнами [31].

Окрім звітів Групи експертів, Генеральна Асамблея ООН присвятила декілька Резолюцій питанню безпеки у сфері інформаційно-комунікаційних технологій. Зокрема, у Резолюції 73/27 Генеральна Асамблея закликала країни продовжувати інформувати Генерального Секретаря з приводу їх поглядів на такі питання як загальне сприйняття питань інформаційної безпеки, національні заходи та концепції, розроблені з метою зміцнення інформаційної безпеки, можливі заходи, що можуть бути здійснені на міжнародному рівні для зміцнення інформаційної безпеки на глобальному рівні [13].

Проте, такі заклики до співпраці у сфері кібербезпеки не змогли забезпечити держав від подальших кібератак. У зв'язку з цим слушною є думка Уни Хетвей на інших, які зазначають, що «роль Об'єднаних Націй стосовно кібербезпеки є більшою мірою чином обмеженою обговореннями та поширенням інформації» [6; с. 861].

Окрім цього, Резолюція 73/27 встановила: необхідність співпраці держав при здійсненні заходів щодо зміцнення безпеки під час використання інформаційно-телекомунікаційних технологій, виконання державами своїх міжнародних

зобов'язань у разі здійснення ними протиправних діянь, недопустимість надання дозволу на використання території держав для здійснення протиправних діянь з використанням інформаційно-телекомунікаційних технологій, необхідність співпраці держав для протидії злочинному використанню інформаційно-телекомунікаційних технологій, необхідність дотримання прав людини в процесі забезпечення безпечного використання інформаційно-телекомунікаційних технологій, заборону підтримки діяльності з використанням інформаційно-телекомунікаційних технологій, що суперечить їх міжнародним зобов'язанням, необхідність здійснення заходів для захисту об'єктів критичної інфраструктури, задоволення запитів про надання допомоги для захисту об'єктів критичної інфраструктури внаслідок зловмисних дій в сфері інформаційно-телекомунікаційних технологій, попередження розповсюдження зловмисних та технічних засобів, поширення інформації з іншими державами про протидію факторам уразливості в сфері інформаційно-телекомунікаційних технологій, сприяння участі приватних суб'єктів в у зміцненні безпеки під час використання інформаційно-телекомунікаційних технологій [13].

10 березня 2021 року Робоча група відкритого складу з питань розвитку в галузі інформації та телекомунікацій в контексті міжнародної безпеки оприлюднила Фінальний основний звіт, що визначає належну поведінку держав під час застосування інформаційно-комунікаційних технологій [30]. Робоча група визначила у якості основних загроз розвиток інформаційно-телекомунікаційних технологій у воєнних цілях, підвищення частоти зловмисного використання інформаційно-телекомунікаційних технологій як державами, так і недержавними суб'єктами, можливість порушення безпеки, а також завдання шкоди об'єктам критичної інфраструктури держав у зв'язку з залежністю держав від цифрових технологій [30]. На основі наведеного переліку загроз, Робоча група виклала правила, норми та принципи належної поведінки держав, що стосуються використання інформаційно-телекомунікаційних технологій. По-перше, держави мають як утримуватись від підтримки діянь з використанням інформаційно-телекомунікаційних технологій, що суперечать їх міжнародним зобов'язанням, так

і здійснювати заходи для захисту власних об'єктів критичної інфраструктури від кіберзагроз, зокрема, за підтримки міжнародних організацій [30]. По-друге, держави мають інформувати Генерального Секретаря про національні підходи та погляди щодо застосування міжнародного права під час використання інформаційно-телекомунікаційних технологій, а також розробляти нові підходи, зокрема, у міжнародному праві, для загального розуміння державами щодо застосування міжнародного права до діяльності, пов'язаної із застосуванням інформаційно-телекомунікаційних технологій [30]. По-третє, Робоча група наголосила на важливості заходів щодо зміцнення довіри між державами, що полягає у прозорих діях держав та міжнародній співпраці. У цьому аспекті, держави можуть інформувати Генерального Секретаря щодо можливих заходів зі зміцнення довіри і поширювати інформацію, наприклад, через Портал кіберполітики Інституту ООН з досліджень роззброєння [30]. По-четверте, держави мають приділяти увагу зміцненню потенціалу, для захисту об'єктів критичної інфраструктури від впливу зловмисних діянь, здійснених за допомогою інформаційно-телекомунікаційних технологій [30]. При цьому, необхідно враховувати, що при зміцненні потенціалу основною метою є забезпечення відкритого і мирного середовища функціонування інформаційно-телекомунікаційних технологій [30]. Також важливим є забезпечення партнерських відносин з іншими учасниками на основі взаємної довіри та визнання національної власності [30]. Окрім цього, зміцнення потенціалу має узгоджуватись з повагою до прав людини та основоположних свобод, зокрема, щодо забезпечення конфіденційності чутливої інформації [30]. По-п'яте, держави мають постійно брати участь у діалозі в контексті міжнародної безпеки, пов'язаної із використанням інформаційно-телекомунікаційних технологій [30]. Загалом, головною метою Фінального основного звіту був заклик держав до постійного обміну поглядами та ідеями з Робочою групою у контексті використання інформаційно-телекомунікаційних технологій державами [30].

3.3. Вплив пандемії Covid-19 на кібербезпеку держав

З поширенням пандемії Covid-19, на початку 2020 року уряди країн по всьому світу прийняли рішення про заборону масових заходів, відвідування громадських місць задля максимального усунення фізичного контакту між людьми. Відповідно, комунікація перейшла у площину кіберпростору. У зв'язку з цим, як приватні, так і державні установи стали більш залежні від Інтернет-мережі, та, у той же час, їх системи комунікації та обміну інформації стали вразливіші до можливих кібератак.

Особливої охорони потребують установи, діяльність яких пов'язана з охороною здоров'я та медициною. Інформація, пов'язана з розробленням політик щодо протидії коронавірусу, лікарських препаратів та іншими релевантними питаннями наразі викликає чималий інтерес в урядів інших країн [140, с. 4]. У Фінальному звіті Робочої групи відкритого складу з питань розвитку в галузі інформації та телекомунікацій в контексті міжнародної безпеки 2021 зазначено, що «пандемія Covid-19 наголосила на важливості захисту інфраструктури охорони здоров'я, включаючи медичні послуги та заклади, шляхом впровадження норм, що стосуються критичної інфраструктури» [30].

Підтвердженням цьому є ряд кібератак, здійснених у 2020 році. Зокрема, навесні 2020 року Всесвітня Організація Охорони Здоров'я зазнала кібератак на власні системи, що мало наслідком витік інформації про електронні адреси та паролі працівників організації. Внаслідок кібератаки, зловмисники використовували отримані електронні адреси співробітників [141]. За допомогою отриманих електронних адрес, вони надсилали повідомлення нібито від імені співробітників Всесвітньої Організації Охорони Здоров'я з приводу заохочення фінансування фонду, спрямованого на боротьбу з коронавірусним захворюванням [141]. У вчиненні атак підозрювали уряд Ірану, проте сам Іран заперечував такі твердження [142].

У березні 2020 року комп'ютерні системи однієї з найбільших лікарень Чеської Республіки, яка проводила тести на коронавірус, також були уражені

внаслідок кібератак [143]. Внаслідок кібератаки, довелось відкласти проведення операцій, перенаправляти пацієнтів до іншої лікарні та закрити усю інформаційну мережу лікарні [144].

У середині травня 2020 року Федеральне Бюро Розслідувань Сполучених Штатів Америки та Агентство з кібербезпеки та безпеки інфраструктури застерегли установи, що здійснюють діяльність, пов'язану з дослідженням вірусу COVID-19 щодо можливих загроз їх нормальній діяльності [145]. Зокрема, вони зазначили про можливі спроби викрадення інформації, пов'язаної з розробленням вакцин, лікування та тестування щодо COVID-19 [145]. У зв'язку з цим, Федеральне Бюро Розслідувань Сполучених Штатів Америки та Агентство з кібербезпеки та безпеки інфраструктури закликали організації виправити усі вразливі ділянки систем, здійснювати періодичне виправлення вразливих ділянок сервісів, пов'язаних з інтернет-мережею, постійно здійснювати перевірку на предмет незаконного доступу до систем, посилити вимоги до даних для входу до систем та процесу аутентифікації, а також припиняти доступ користувачів, що здійснюють нетипову діяльність під час користування системами [145].

Таким чином, пандемія COVID-19 ще сильніше підкреслила необхідність захищати інформаційні та комп'ютерні системи установ, що є об'єктами критичної інфраструктури держав та виявила ті прогалини у кібербезпеці, що мають бути усунені державами. Зокрема, COVID-19 висунула на перше місце функціонування лікарень з точки зору важливості функціонування для усього населення відповідної держави. Однак, часто інформаційні системи лікарських установ не є достатньо захищеними, що робить їх досить уразливими до можливих кібератак [140, с. 7]. У зв'язку з цим, на сьогодні державам варто зосередити особливу увагу на фінансуванні інформаційних систем установ, пов'язаних з забезпеченням охорони здоров'я населення [140, с. 7].

3.4. Висновки до Розділу 3

Таким чином, вважаємо, що можливою відповіддю держав на кібератаки може бути реалізація права на самооборону. При цьому, зауважуємо на дотриманні критеріїв необхідності та пропорційності. Наприклад, у якості самооборони може виступати технічне ушкодження серверів, з яких здійснюються кібератаки. На наше переконання, здійснення кібератак не є підставою для застосування збройної сили у відповідь. При цьому, вважаємо за необхідне звернутись до принципу завчасного права на самооборону у разі наявності підстав вважати, що внаслідок кібератак буде завдано значної шкоди. Зокрема, у якості завчасної самооборони може виступати використання програмного забезпечення проти серверів іншої держави. Альтернативно, держави можуть застосовувати санкції, зокрема, до посадових осіб держав, причетних до здійснення кібератак. На сьогодні цей механізм не набув особливого поширення і застосовувався лише Сполученими Штатами Америки та Європейським Союзом. Однак, вважаємо підкреслити основний недолік цього механізму. Оскільки у організації та здійсненні кібератак може брати участь ціла група осіб, як посадових, так і приватних, то вибіркове застосування санкцій не забезпечить належного ступеню покарання для самої держави.

Окрім цього, вирішальне значення для притягнення держав до відповідальності має наявність єдиного міжнародного акту, який визначає права і обов'язки держав у кіберпросторі. Хоча на сьогодні перші спроби уніфікації правил вже здійснюються Групою урядових експертів у галузі інформації та телекомунікацій в контексті міжнародної безпеки, вони мають лише рекомендаційний характер. Позитивним напрямком діяльності міжнародної спільноти у галузі кібербезпеки є акумуляція підходів різних держав для вироблення уніфікованих критеріїв визначення протиправної поведінки у кіберпросторі. Це засвідчує політичну волю держав до протидії кібератакам, а також притягнення до відповідальності винних держав.

При цьому, вважаємо за доцільне наголосити, що при розробці нормативних актів як на державному, так і на міжнародному рівні, варто звертати увагу на визначення об'єктів критичної інфраструктури. Це стало особливо актуальним в

період пандемії Covid-19, оскільки внаслідок кібератак було уражене функціонування таких критичних для життєдіяльності населення об'єктів, як медичні заклади. З іншого боку, на наше переконання, держави мають забезпечити належний рівень кібербезпеки таких об'єктів.

ВИСНОВКИ

Таким чином, з точки зору кібербезпеки держав у міжнародному праві, ключовою проблемою на сьогодні є відсутність ефективного механізму, який би дозволяв притягнути держави за здійснення кібератак. Не зважаючи на те, що кібератаки стали альтернативним інструментом завдання шкоди з середини 2000-х років, міжнародна спільнота не розробила єдиного уніфікованого підходу до визначення кібератак. У зв'язку з цим, держави відособлено розробляють національні стратегії та законодавчі акти, якими визначають перелік протиправних діянь у кіберпросторі та відповідальність за їх здійснення. Проте, важливо звернути увагу, що далеко не в кожній національній стратегії з кібербезпеки, держави приділяють увагу кібератакам, здійсненим саме державами або приватними суб'єктами, підконтрольними державам. Наразі більша увага зосереджена на кримінальній відповідальності приватних суб'єктів. Однак, на наше переконання, варто все ж таки приділяти більше уваги питанню кібербезпеки з точки зору міждержавних відносин, оскільки часто за діями приватних суб'єктів стоїть контроль або фінансування з боку держав. При цьому, такі кібератаки за підтримки держав часто спричиняють серйозні негативні наслідки, які можуть поширюватись на територію всієї країни протягом тривалого часу.

Не зважаючи на те, що наразі єдиного поняття «кібератака» не було розроблено, можна виділити спільні риси кібератак на основі тих підходів, які були запропоновані державами та міжнародними організаціями. Так, до спільних рис належать: втручання і завдання шкоди комп'ютерній мережі; пошкодження або знищення важливих об'єктів інфраструктури, або інформації, що належать державі; можливість здійснення кібератак як представниками держави, так і приватними особами; здійснення за допомогою шкідливого програмного забезпечення.

Окрім цього, однією з центральних проблем є встановлення зв'язку між приватними суб'єктами, що здійснюють кібератаки та державою, що контролює їх здійснення. Не зважаючи на те, що Статті про відповідальність держав за

міжнародно-протиправні діяння наводить перелік підстав для визнання поведінки приватних осіб у якості поведінки держави, досить високі стандарти, вироблені судовою практикою, не дозволяють встановити необхідний ступінь зв'язку між державою і приватними особами. Відтак, вважаємо за необхідне встановити більш гнучкі критерії належності поведінки приватних осіб державі. Вважаємо, що найбільш поширеною підставою для визнання належності поведінки приватних осіб державі є встановлення контролю над діями приватних осіб. Відтак, в контексті кібератак, держави зазвичай дають загальні інструкції особам, які можуть знаходитись навіть на території іншої держави. При цьому, технологічна частина може повністю забезпечуватись самими приватними особами. У зв'язку з цим, такий стандарт, як «ефективний контроль», що передбачає контроль держави за здійсненням кожної окремої дії, не є обґрунтованим для застосування у здійсненні кібератак. Вважаємо, що концепція «загального контролю» дозволить ефективніше реалізовувати механізм притягнення держав до відповідальності.

Окремо варто зауважити, що на сьогодні міжнародна спільнота дійшла висновку про застосовність норм Статуту ООН та міжнародного гуманітарного права до здійснення кібератак. Це є безумовно важливим кроком, оскільки дозволяє застосовувати вже наявні норми та принципи міжнародного права до кваліфікації діянь держави у кіберпросторі. У зв'язку з цим, очевидними порушеннями зобов'язань, пов'язаними зі здійсненням кібератак, є заборона застосування сили та заборона втручання у внутрішні справи. На наше переконання, найбільш вдалим підходом до визначення того, чи мало місце застосування сили, є ступінь шкоди та обсяг збитків внаслідок здійснення кібератак. У зв'язку з цим, ми дійшли висновку, що будь-яка кібератака є втручанням у внутрішні справи держави, оскільки вона так чи інакше завдає шкоди або отримує несанкціонований доступ до даних чи інформації. У разі ж, якщо внаслідок кібератак спричинено серйозну шкоду об'єктам критичної інфраструктури або ж особі чи групі осіб, то таке діяння варто кваліфікувати у якості застосування сили. На основі цього, можна дійти висновку що у разі кваліфікації кібератаки у якості застосування сили, уражена держава має право на самооборону, на підставі положень Статуту ООН. Це є важливим

механізмом, оскільки на сьогодні уражені держави не здатні належним чином захистити свою інфраструктуру. Особливо актуальним це є для тих держав, на інфраструктуру яких здійснювалась серія кібератак протягом тривалого часу. Наразі ж держави застосовують санкції до окремих приватних осіб та юридичних утворень, що, на нашу думку, не є достатньо ефективним заходом впливу безпосередньо на державу. Це зумовлено тим, що такі санкції зачіпають скоріше приватні інтереси, а не державні.

У той же час, не зважаючи на наявні механізми, які дають правові підстави для кваліфікації кібератак з точки зору протиправних діянь у міжнародному праві, на наше переконання варто продовжувати докладати зусилля для розроблення єдиного міжнародного акту з кібербезпеки держав. Ми вважаємо, що у цьому акті має бути відображене визначення кібератак, критичних об'єктів інфраструктури, суб'єктів здійснення кібератак, права та обов'язки держав у кіберпросторі. Окрім цього, варто визначити критерії для встановлення зв'язку між державою та приватними суб'єктами. У зв'язку з цим, вважаємо за необхідне підтримувати наявну кооперацію держав з питань вироблення уніфікованих правил належної поведінки у кіберпросторі з метою подальшого прийняття конвенції чи багатосторонньої угоди між державами, що матиме обов'язкову силу для держав-учасниць.

Насамкінець, вважаємо за необхідне звернути увагу на необхідність додаткового захисту як за допомогою правових механізмів, так і технічних, об'єктів критичної інфраструктури, діяльність яких пов'язана з охороною здоров'я населення. Наразі ці об'єкти є досить чутливими до здійснення кібероперацій, оскільки зазвичай їх системи не захищені належним чином. Оскільки внаслідок кібератак їх функціонування може бути частково або повністю припинене, необхідно винести питання щодо їх охорони на міжнародний рівень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Węgliński K. Cyberwarfare and responsibility of states. Torun International Studies. 2016. No. 1 (9). P. 79-86.
2. Schaap, A. J., Cyber warfare operations: Development and use under international law. Air Force Law Review. 2009. Vol. 64. P. 121-174.
3. Statute of the International Court of Justice, 1945. URL: <https://www.icj-cij.org/en/statute> (дата звернення 3 лютого 2021 року).
4. Tabansky L. Basic Concepts in Cyber Warfare. Military and Strategic Affairs. 2011. Vol. 3. P. 75- 92.
5. McKenzie T. M. Is Cyber Deterrence Possible? Air University Press. Alabama, 2017. 20 p.
6. Hathaway O. A. et. al. The law of cyber-attack. California law review. 2012. Vol. 100. P. 817-886.
7. Cohen M. S., Freilich Ch. D. Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 2015. P. 1-15.
8. Payne Ch., Finlay L. Addressing obstacles to cyber-attribution: a model based on state response to cyber-attack. Geo. Wash. Int'l L. Rev. 2017. Vol. 49. P. 535-568.
9. Tallin Manual on the International law applicable to cyber warfare. Prepared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence / Schmitt M. N. (ed.). 2013. Cambridge University Press. 282 p.
10. NATO Glossary of Terms and definitions (English and French). URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf (дата звернення 4 лютого 2021 року).

11. Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), 17 April 2019. URL: <https://eur-lex.europa.eu/eli/reg/2019/881/oj> (дата звернення 4 лютого 2021 року).

12. Конвенція про кіберзлочинність: Міжнародний договір від 23 листопада 2001 року. Дата оновлення: 7 вересня 2005 року. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 21 січня 2021 року).

13. United Nations General Assembly Resolution 73/27 Developments in the field of information and telecommunications in the context of international security, 5 December 2018. URL: <https://undocs.org/en/A/RES/73/27> (дата звернення 4 лютого 2021 року)

14. United Nations General Assembly Resolution 62/17 Developments in the field of information and telecommunications in the context of international security. URL: <https://undocs.org/pdf?symbol=en/A/RES/62/17> (дата звернення 4 лютого 2021 року).

15. National cybersecurity strategy. 2019. URL: <https://www.ccn-cert.cni.es/en/pdf/documentos-publicos/3812-national-cybersecurity-strategy-2019/file.html> (дата звернення 5 лютого 2021 року). 68 p.

16. Cyber security strategy for Germany. 2016. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en (дата звернення 5 лютого 2021 року). 36 p.

17. National Cyber Security Strategy 2016-2021. URL: [National Cyber Security Strategy 2016-2021 \(publishing.service.gov.uk\)](https://publishing.service.gov.uk/national-cyber-security-strategy-2016-2021) (дата звернення 5 лютого 2021 року). 82 р.

18. Austrian Cyber Security Strategy. 2013. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSSL.pdf (дата звернення 5 лютого 2021 року). 24 р.

19. The National cyber security strategy of the Republic of Croatia. 2015. URL: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSSEN.pdf> (дата звернення 5 лютого 2021 року). 31 р.

20. A national cyber security strategy for Sweden. URL: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/SwedishNCSSSEN.pdf> (дата звернення 5 лютого 2021 року). 29 р.

21. Finland's Cyber security Strategy. URL: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf (дата звернення 5 лютого 2021 року). 42 р.

22. National Cyber Security Agenda: A cyber secure Netherlands. URL: https://www.enisa.europa.eu/news/member-states/CSAagenda_EN.pdf (дата звернення 5 лютого 2021 року). 46 р.

23. Cybersecurity Strategy: Establishing a System to Ensure a High Level of Cyber Security. URL: https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf (дата звернення 5 лютого 2021 року). 18 р.

24. National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf (дата звернення 5 лютого 2021 року). 28. р.

25. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 24.10.2020. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 5 лютого 2021 року).

26. DOD Dictionary of Military and Associated Terms. URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> (дата звернення 7 лютого 2021 року). 364 p.

27. Secretary of the Air Force. Air Force Policy Directive, 4 August 2014 10-7. URL: <https://fas.org/irp/doddir/usaf/afpd10-7.pdf> (дата звернення 7 лютого 2021 року).

28. CRS Report for Congress Information Operations and Cyberwar: Capabilities and Related Policy Issues. Updated 14 September 2006. URL: <https://fas.org/irp/crs/RL31787.pdf> (дата звернення 7 лютого 2021 року).

29. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013. URL: <https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf> (дата звернення 7 лютого 2021 року). P.2.

30. Final Substantive Report of Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021. URL: <https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf> (дата звернення 1 квітня 2021 року).

31. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015. URL:

https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (дата звернення 7 лютого 2021 року).

32. United Nations General Assembly Resolution 58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (дата звернення 9 лютого 2021 року).

33. Presidential Decision Directive NSC-63. URL: <https://fas.org/irp/offdocs/pdd/pdd-63.htm> (дата звернення 9 лютого 2021 року).

34. Commission of the European Communities Communication from the Commission to the Council and the European Parliament Critical Infrastructure Protection in the fight against terrorism, 2004. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=nl> (дата звернення 9 лютого 2021 року). 11 p.

35. Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security. 2011. Vol. 4. No. 2. P. 49-60.

36. McGuinness D. How a cyber attack transformed Estonia. URL: <https://www.bbc.com/news/39655415> (дата звернення 1 березня 2021 року).

37. Popescu N., Secrieru S. Hacks, leaks and disruptions: Russian cyber strategies. Research report. Paris, 2018. 128 p.

38. Kohler K. Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations. Zurich, 2020. 21 p.

39. Joubert V. Five years after Estonia's cyber attacks: lessons learned for NATO? URL: https://www.files.ethz.ch/isn/143191/rp_76.pdf (дата звернення 1 березня 2021 року).

40. Brown G. Why Iran Didn't Admit Stuxnet Was an Attack. JFQ. 2011. Issue 63. P. 70-73.

41. Iasiello E. Cyber Attack: A Dull Tool to Shape Foreign Policy. 5th International Conference on Cyber Conflict. URL: https://www.ccdcoe.org/uploads/2018/10/24_d3r1s3_Iasiello.pdf (дата звернення 1 березня 2021 року).

42. Baezner M., Robin P. Hotspot Analysis: Stuxnet. CSS Cyber Defense Project. Zurich, 2017. 15 p.

43. Timeline of Iran's controversial nuclear program. URL: <https://edition.cnn.com/2012/03/06/world/meast/iran-timeline/index.html> (дата звернення 1 березня 2021 року).

44. United Nations Security Council Resolution 1737, 27 December 2006. URL: [https://www.undocs.org/S/RES/1737%20\(2006\)](https://www.undocs.org/S/RES/1737%20(2006)) (дата звернення 1 березня 2021 року).

45. Chen T. M. Stuxnet, the Real Start of Cyber Warfare? IEEE Network. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5634434> (дата звернення 1 березня 2021 року).

46. Yannakogeorgos P. A. Was Russia Behind Stuxnet? URL: <https://thediplomat.com/2011/12/was-russia-behind-stuxnet/> (дата звернення 1 березня 2021 року).

47. Gotsiridze A. The Cyber Dimension of the 2008 Russia-Georgia War. URL: <https://www.gfsis.org/blog/view/970> (дата звернення 1 березня 2021 року).

48. Shakarian P. The 2008 Russian Cyber Campaign Against Georgia. Military Review. 2011. P. 63-68.

49. Bumgarner J., Borg S. Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. U.S. Cyber Consequence Unit Special Report, August 2009. 9 p.

50. Kozlowski A. Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. European Scientific Journal. 2014. Vol. 3. P. 239.

51. Corbin K. Lessons from the Russia-Georgia Cyberwar. URL: <http://www.internetnews.com/government/article.php/3810011/Lessons+From+the+RussiaGeorgia+Cyberwar.html> (дата звернення 3 березня 2021 року).

52. Baezner M., Robin P. Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict. Zurich, 2018. 54 p.

53. Siboni G., Magen Z. The Cyber Attack on the Ukrainian Electrical Infrastructure: Another Warning. INSS Insight. 2016. No. 798. P.1-3.

54. Ukraine power cut 'was cyber-attack'. URL: <https://www.bbc.com/news/technology-38573074> (дата звернення 3 березня 2021 року).

55. Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done. URL: <https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802> (дата звернення 3 березня 2021 року).

56. Ukraine power cut 'was cyber-attack'. URL: <https://www.bbc.com/news/technology-38573074> (дата звернення 3 березня 2021 року).

57. Styczynski J., Beach-Westmoreland N. When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure. Booz Allen Hamilton Inc, 2019. 80 p.

58. Shackelford S. J., Sulmeyer M., Craig Deckard A. N., Buchanan B., Micic B. From Russia with Love: Understanding the Russian Cyber Threat to U.S.

Critical Infrastructure and What to Do about It. Nebraska Law Review. 2017. Vol. 96. P. 320-338.

59. Maurer T. Cyber Proxies and the Crisis in Ukraine. Cyber War in Perspective: Russian Aggression against Ukraine (Chapter 9). NATO CCD COE Publications. Tallinn, 2015. P. 80-86.

60. US accuses Russia of cyber attacks. URL: <https://www.bbc.com/news/election-us-2016-37592684> (дата звернення 3 березня 2021 року).

61. Nakashima E. Russian government hackers penetrated DNC, stole opposition research on Trump. URL: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.db4bb76508ad (дата звернення 23 березня 2021 року).

62. Salinger T. Leaked Democratic National Committee email floated plan to question Sanders' religion: 'I think I read he is an atheist'. URL: <https://www.nydailynews.com/news/politics/leaked-dnc-email-floated-plan-question-sanders-religion-article-1.2722203> (дата звернення 23 березня 2021 року).

63. Robertson A. WikiLeaks posts leaked DNC emails, including donor personal information. URL: <https://www.theverge.com/2016/7/22/12259258/wikileaks-leaked-democratic-national-committee-emails-personal-information> (дата звернення 23 березня 2021 року).

64. 2016 Presidential Campaign Hacking Fast Facts. URL: <https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html> (дата звернення 23 березня 2021 року).

65. CrowdStrike's work with the Democratic National Committee: Setting the record straight. URL: <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> (дата звернення 23 березня 2021 року).

66. Fishel J., Stracqualursi V. A Timeline of Russia's Hacking Into US Political Organizations Before the Election. URL: [https://abcnews.go.com/Politics/%20timeline-russias-hacking-us-political-organizations-ahead-election/story?id=44140526%20\[http://perma.%20cc/3DL9-4QC7](https://abcnews.go.com/Politics/%20timeline-russias-hacking-us-political-organizations-ahead-election/story?id=44140526%20[http://perma.%20cc/3DL9-4QC7) (дата звернення 23 березня 2021 року).

67. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security. URL: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> (дата звернення 23 березня 2021 року).

68. Secret CIA assessment says Russia was trying to help Trump win White House. URL: https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.367a5f52a2c8 (дата звернення 23 березня 2021 року).

69. Staff R. Moscow denies Russian involvement in U.S. DNC hacking. URL: <https://www.reuters.com/article/us-usa-election-hack-russia-idUSKCN0Z02EK> (дата звернення 23 березня 2021 року).

70. Bell C. Cyber Warfare and International Law: The Need for Clarity. P. 36 URL: <https://cpb-us-w2.wpmucdn.com/wp.towson.edu/dist/b/55/files/2018/05/SPRING-2018-BELL-ARTICLE-thj0tu.pdf> (дата звернення 23 березня 2021 року).

71. United Nations General Assembly Resolution Declaration on Principles of International Law concerning Friendly Relations and Co-Operation Among

States in accordance with the charter of the United Nations, 24 October, 1970.
URL: [https://www.undocs.org/A/RES/2625\(XXV\)](https://www.undocs.org/A/RES/2625(XXV)) (дата звернення 23 березня 2021 року).

72. Joubert V. Five years after Estonia's cyber attacks: lessons learned for NATO? URL: https://www.files.ethz.ch/isn/143191/rp_76.pdf (дата звернення 23 березня 2021 року). 8 р.

73. Rex B. Hughes NATO and Cyber Defence - Mission Accomplished? URL:
<https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/NATO%20and%20Cyber%20Defence%20-%20Mission%20Accomplished.pdf> (дата звернення 23 березня 2021 року).

74. NATO Cyber Defence. URL:
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf (дата звернення 23 березня 2021 року).

75. Klimburg A. National Cyber Security Framework Manual. NATO CCD COE Publication. Tallinn, 2012. 235 P. 30-31.

76. Cyber defence. URL:
https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення 23 березня 2021 року).

77. Brussels Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 11-12 July 2018. URL: [20180713_180711-summit-declaration-eng.pdf \(nato.int\)](https://www.nato.int/docu/summit/2018/180711-summit-declaration-eng.pdf) (дата звернення 23 березня 2021 року).

78. NATO readies for cyber threats. URL:
https://www.nato.int/cps/en/natohq/news_179481.htm?selectedLocale=en (дата звернення 23 березня 2021 року).

79. The Secretary General Annual Report 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf#page=25 (дата звернення 25 березня 2021 року). 143 p.

80. Explanatory Report to the Convention on Cybercrime. European Treaty Series. 2001. No. 185. 60 p.

81. Конвенція про кіберзлочинність: Міжнародний договір від 23 листопада 2001 року. Дата оновлення: 7 вересня 2005 року. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 25 березня 2021 року).

82. General Assembly Resolution 2040 (XXXIV-O/04) Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, 8 June 2004. URL: http://www.oas.org/juridico/english/ga04/agres_2040.htm (дата звернення 25 березня 2021 року).

83. General Assembly Resolution 2004 (XXXIV-O/04) Adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity, 8 June 2004. URL: <https://ccdcoe.org/uploads/2018/10/OAS-040608-InterAmericanCyberSecurityStrategy.pdf> (дата звернення 25 березня 2021 року).

84. Responsibility of States for Internationally Wrongful Acts, 2001. URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (дата звернення 25 березня 2021 року).

85. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001. URL: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (дата звернення 25 березня 2021 року). 143 p.

86. Tanyildizi M. E. State responsibility in cyberspace: the problem of attribution of cyberattacks conducted by non-state actors. *Law & Justice Review*. 2017. Issue 14. P. 119-176.

87. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro. ICJ Judgement of 26 February 2007. URL: <https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf> (дата звернення 1 квітня 2021 року).

88. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). ICJ Judgement of 27 June 1986. URL: <https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf> (дата звернення 1 квітня 2021 року).

89. Lotrionte K. State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights. *Emory International Law Review*. 2012. Vol. 26. Issue 2. P. 825-919.

90. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda). ICJ Judgement of 19 December 2005. URL: <https://www.icj-cij.org/public/files/case-related/116/116-20051219-JUD-01-00-EN.pdf> (дата звернення 1 квітня 2021 року).

91. Jolley J. D. Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law. PhD Thesis. University of Glasgow. 2017. URL: <https://poseidon01.ssrn.com/delivery.php?ID=91607306510210107311100400511309300703100503106803000501112106701011006812709111710905001810005055097010094124102090120077005055038014069012122118101029010119005122091065085008079025097074069021029116108072114004018096069064087024114069005067085005081&EXT=pdf&INDEX=TRUE> (дата звернення 1 квітня 2021 року). 317 p.

92. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro. Dissenting Opinion Of Vice-President Al-Khasawneh. URL: <https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-01-EN.pdf> (дата звернення 1 квітня 2021 року).

93. Hathaway O.A. et al. Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors. Texas Law Review. 2017. Vol. 95. P. 539-590.

94. The Prosecutor v. Dusko Tadić. Judgenet of the Appeals Chamber of 15 July 2019. URL: <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf> (дата звернення 1 квітня 2021 року)

95. Pool Ph. War of the Cyber World: The Law of Cyber Warfare. The International Lawyer. 2013. Vol. 47. No. 2. P. 299-323.

96. Major cyber spy network uncovered. URL: <http://news.bbc.co.uk/2/hi/americas/7970471.stm> (дата звернення 1 квітня 2021 року).

97. Bradbury D. GhostNets in the machine. URL: <https://www.theguardian.com/technology/2009/apr/16/china-cybercrime-hacking> (дата звернення 1 квітня 2021 року).

98. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran). ICJ Judgement of 24 May 1980. URL: <https://www.icj-cij.org/public/files/case-related/64/064-19800524-JUD-01-00-EN.pdf> (дата звернення 1 квітня 2021 року).

99. Charter of the United Nations, 1945. URL: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf> (дата звернення 1 квітня 2021 року).

100. Kilovaty I. Doxfare: Politically motivated leaks and the future of the norm of non-intervention in the era of weaponized information. Harvard National Security Journal. 2018. Vol. 9. P. 146-179.

101. Corfu Channel Case (United Kingdom v. Albania). ICJ Judgement of 15 December 1949. URL: <https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf> (дата звернення 5 квітня 2021 року). P. 35.

102. S.S. Lotus Case (France v. Turkey). P.C.I.J. Judgement of 7 September 1927. URL: https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf (дата звернення 5 квітня 2021 року). P.18

103. Island of Palmas case (Netherlands v. USA). Award of 4 April 1928. URL: https://legal.un.org/riaa/cases/vol_II/829-871.pdf (дата звернення 5 квітня 2021 року). P. 838

104. Xinmin M. Key Issues and Future Development of International Cyberspace Law. China Quarterly of International Strategic Studies. 2016. Vol. 2. No. 1. P. 119-133.

105. Chircop L. Territorial Sovereignty in cyberspace after Tallinn Manual 2.0. Melbourne Journal of International Law. 2019. Vol. 20. P.1-29.

106. Von Heinegg W. H. Legal Implications of Territorial Sovereignty in Cyberspace. 2012 4th International Conference on Cyber Conflict. URL: https://www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf (дата звернення 5 квітня 2021 року). P. 7-19.

107. United Nations Convention on the Law of the Sea, 1982. URL: https://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf (дата звернення 5 квітня 2021 року).

108. Melzer N. Cyberwarfare and International Law. URL: <https://undir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> (дата звернення 5 квітня 2021 року). 38 p.
109. United Nations General Assembly Resolution 3314 (XXIX), 29 November 1974. URL: [https://undocs.org/en/A/RES/3314\(XXIX\)](https://undocs.org/en/A/RES/3314(XXIX)) (дата звернення 5 квітня 2021 року).
110. Silver D.B. Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter. International Law Studies. 2002. Vol. 76. P. 73-91.
111. Gordon E. Article 2(4) in Historical Context. Yale Journal of International Law. 1985. Vol. 10. P. 271-278.
112. Legality of the Threat or Use of Nuclear Weapons. ICJ Advisory Opinion of 8 July 1996. URL: <https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf> (дата звернення 5 квітня 2021 року).
113. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Dissenting Opinion of Judge Schwebel. URL: <https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-09-EN.pdf> (дата звернення 5 квітня 2021 року).
114. Schmitt M. N. “Attack” as a Term of Art in International Law: The Cyber Operations Context. 4th International Conference on Cyber Conflict. 2012. P. 283-293.
115. Foltz A. C. Stuxnet, Schmitt Analysis, and the Cyber “Use-of-Force” Debate. JFQ. 2012. Issue 67. P. 40-48.
116. Trail smelter case (United States v. Canada). Arbitral awards of 16 April 1938, and 11 March 1941. URL: https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf (дата звернення 12 квітня 2021 року).

117. Prevention of Transboundary Harm from Hazardous Activities, 2001.
URL:

https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_7_2001.pdf

(дата звернення 12 квітня 2021 року).

118. Liu I. Y. State Responsibility and Cyberattacks: Defining Due Diligence Obligations. IV Indonesian Journal of International & Comparative Law. 2017. P. 191-260.

119. ILA Study Group on Due Diligence in International Law. First Report Duncan French (Chair) and Tim Stephens (Rapporteur). URL: https://olympereseauinternational.files.wordpress.com/2015/07/due_diligence_-_first_report_2014.pdf (дата звернення 12 квітня 2021 року).

120. Responsibilities and obligations of States sponsoring persons and entities with respect to activities in the Area (Request for Advisory Opinion Submitted to the Seabed Disputes Chamber). International Tribunal for The Law of The Sea. Advisory opinion of 1 February 2011. URL: [17_adv_op_010211_en.pdf \(itlos.org\)](http://www.itlos.org/publications/documents/17_adv_op_010211_en.pdf) (дата звернення 12 квітня 2021 року).

121. Schmitt M. N. In Defense of Due Diligence in Cyberspace. The Yale Law Journal Forum. 2015. p. 68-71.

122. United Nations General Assembly Resolution 55/63 Combating the criminal misuse of information technologies. URL: <https://undocs.org/en/A/RES/55/63> (дата звернення 12 квітня 2021 року).

123. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (Chair's Summary), 2021. URL: <https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf> (дата звернення 12 квітня 2021 року). 20 p.

124. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (Chair's Summary), 2021. URL: <https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf> (дата звернення 12 квітня 2021 року). 20 р.

125. Schmitt M. N. The Law of Cyber Warfare: Quo Vadis? Stanford Law & Policy Review. 2014. Vol. 25. p. 269-300.

126. Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America). ICJ Judgment of 6 November 2003. URL: <https://www.icj-cij.org/public/files/case-related/90/090-20031106-JUD-01-00-EN.pdf> (дата звернення 12 квітня 2021 року).

127. Waxman M. C. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. International Law Studies. 2013. Vol. 89. P. 109-122.

128. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text (дата звернення 12 квітня 2021 року).

129. Letter of Mr. Webster to Lord Ashburton. Washington, 27 July 1842. URL: https://avalon.law.yale.edu/19th_century/br-1842d.asp (дата звернення 18 квітня 2021 року).

130. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory. ICJ Advisory Opinion of 9 July 2004. URL: <https://www.icj-cij.org/public/files/case-related/131/131-20040709-ADV-01-00-EN.pdf> (дата звернення 12 квітня 2021 року).

131. United Nations Security Council Resolution 1368, 2001. URL: [https://undocs.org/S/RES/1368\(2001\)](https://undocs.org/S/RES/1368(2001)) (дата звернення 12 квітня 2021 року).

132. United Nations General Assembly Resolution 1373, 2001. URL: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (дата звернення 12 квітня 2021 року).

133. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013. URL: [A/68/98 - E - A/68/98 -Desktop \(undocs.org\)](#) (дата звернення 12 квітня 2021 року).

134. Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities: Executive Order 13757. 28 December 2016. URL: <https://fas.org/irp/offdocs/eo/eo-13757.pdf> (дата звернення 12 квітня 2021 року).

135. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities: Executive Order 13694. 1 April 2015. URL: <https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities> (дата звернення 12 квітня 2021 року).

136. Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation: Executive Order 14024. 15 April 2021. URL: <https://www.govinfo.gov/content/pkg/FR-2021-04-19/pdf/2021-08098.pdf> (дата звернення 12 квітня 2021 року).

137. Amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States: Council of The European Union Decision 2020/1127. 30 July 2020. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN> (дата звернення 21 квітня 2021 року).

138. Developments in the field of information and telecommunications in the context of international security. URL: <https://www.un.org/disarmament/ict-security/> (дата звернення 22 квітня 2021 року).

139. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2010. URL: [A/65/201 - E - A/65/201 -Desktop \(undocs.org\)](#) (дата звернення 22 квітня 2021 року).

140. Wiggen J The impact of COVID-19 on cyber crime and state-sponsored cyber activities. Facts & Findings. 2020. No. 391. 11 p.

141. WHO reports fivefold increase in cyber attacks, urges vigilance. URL: <https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance>. (дата звернення 17 квітня 2021).

142. Menn J. et al. Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus – sources. URL: <https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus%02sources-idUSKBN21K1RC>. (дата звернення 17 квітня 2021).

143. Lyngaas S. Czech Republic's second-biggest hospital is hit by cyberattack. URL: <https://www.cyberscoop.com/czech-hospital-cyberattack-coronavirus/>. (дата звернення 17 квітня 2021).

144. Cimpanu C. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak. 2020. URL: <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/>. (дата звернення 17 квітня 2021).

145. People's Republic of China (PRC) Targeting of COVID-19 Research Organizations. URL: https://www.cisa.gov/sites/default/files/publications/Joint_FBI-

[CISA PSA PRC Targeting of COVID-19 Research Organizations S508C.pdf](#)

(дата звернення 23 квітня 2021 року).