МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
Кафедра міжнародного та європейського права

ДОПУСТИТИ ДО ЗАХИСТУ
В.о. Завідувача кафедри
_____Р. О.Максимович
«____»_____2024р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»
спеціальності 293 «Міжнародне право»

Тема: **КІБЕРАТАКИ В КОНТЕКСТІ ПРИНЦИПІВ ЗАБОРОНИ ВТРУЧАННЯ ТА ЗАСТОСУВАННЯ СИЛИ В МІЖНАРОДНОМУ ПРАВІ**

Виконавець: Дінжос Ірина Валеріївна
Науковий керівник: к.ю.н., доцент, доцент кафедри міжнародного та європейського права Замула Аліна Юріївна
Нормоконтролер: викладач кафедри міжнародного та європейського права Головатенко Марина Юріївна

Київ, 2024

ЗМІСТ

ВСТУП

Актуальність теми. У міжнародному праві положення про суверенну рівність держав і заборони на втручання та застосування сили є основними фундаментальними принципами, які мають вирішальне значення для миру та безпеки міжнародного співтовариства. З іншого боку, кіберпростір і кібератаки постають актуальною проблемою, яка в багатьох відношеннях відкрита для юридичного тлумачення, створюючи новий і інший грунт для держав з інших національних територій з розвитком технологій.

Анонімна та транскордонна структура кіберпростору свідчить про необхідність створення нових правил. Поки проводяться різні кодифікаційні дослідження, використовується захисна сила існуючих нормативних актів. По суті, національні та міжнародні дослідження, проведені державами, також підтверджують це питання, і дії вживаються відповідно до основних принципів міжнародного права. У кодифікаційних дослідженнях, хоча це і не є обов'язковим, важливий глобальний консенсус у рамках Талліннського посібника.

У нашому дослідженні кіберпростір і кібератаки оцінювалися разом із концепціями технічної інформації, суверенітету, втручання, застосування сили, самозахисту та міжнародної відповідальності. Кібератаки, здійснені державами або приписувані їм, розглядаються на прикладах, а також розглядається відповідальність держав.

Міжнародне право є одним із найважливіших будівельних блоків міжнародних відносин. З початку 20-го століття держави наполегливо працюють над проблемами, які можуть створити проблеми для забезпечення міжнародного миру та безпеки, і намагаються зробити кожен свій крок законним. На даний момент міжнародне право було сформоване змінами та подіями у світі та набуло свого сучасного вигляду. Для того, щоб основні правила вижили таким чином, щоб вони могли впоратися з новими

проблемами, оновлення правил, враховуючи події, які відбулися та можуть відбутися, завжди зберігало свою важливість.

Фундаментальні концепції міжнародного права, такі як суверенна рівність держав і заборона втручання та застосування сили, є надто важливими для того, щоб мир міжнародної спільноти залишився беззахисним. При виникненні різних питань і проблем з цього приводу слід пропонувати швидкі рішення, щоб уникнути негативних наслідків. Кібератаки належать до проблем, які ми згадали, як одне з питань, які залишаються на порядку денному та потребують вирішення серед явищ, які можуть загрожувати міжнародній безпеці та впливати на держави.

Зміст понять, пов'язаних з кіберпростором і кібератаками, складається з нових і динамічних проблем, пов'язаних з технологіями, обсяг яких ще не є чітким у національному та міжнародному праві. У 21 столітті, хоча держави хочуть захистити свої технологічні активи та розвивати свої повноваження на додаток до своїх фізичних активів, вони також діють і проводять міжнародні дослідження, щоб запобігти незворотному знищенню кіберзагроз. Оскільки кіберпростір, де відбувається кібердіяльність, є новою сферою діяльності, потрібен час для досягнення консенсусу в міжнародному праві та створення нових правил. З цієї причини виникає необхідність оцінити існуючі міжнародні правила в межах поточних умов.

У нашому дослідженні буде обговорено процес забезпечення кібербезпеки, ставлення міжнародного права до кібератак, а також питання щодо норм міжнародного права, які можуть бути застосовані до кібератак. Буде надано інформацію щодо технічної інформації щодо кіберпростору та кібератак, суверенітету, втручання, заборони застосування сили та міжнародних текстів, спеціально підготовлених для кіберпростору. Роль держав у кібератаках та вплив атак на міжнародне право оцінюватимуть за допомогою конкретних подій.

Перелік зарубіжних та укр вчених які досліджували дану проблему Michael Schmitt — автор праць, присвячених праву війни в контексті

кіберпростору, включаючи дослідження міжнародного права та кібербезпеки. Ian Brown — фахівець з міжнародного права, який досліджує правові аспекти кіберзагроз і прав людини в цифровому світі. Ronald Deibert — експерт з кібербезпеки і дослідженням глобальних кібервикликів. Laura DeNardis — вивчає глобальне управління Інтернетом та роль держав і корпорацій у кіберпросторі. David A. Hollis — досліджує аспекти правового режиму кібербезпеки, зокрема принципи застосування сили і втручання.

Мета і завдання дослідження. Мета даної кваліфікаційної роботи полягає в тому, щоб вивчити відповідність кібератак, що стосуються держав, міжнародному праву та виявити засоби правового захисту, які держави можуть застосувати у разі порушення.

Поставлена мета зумовила необхідність вирішення наступних завдань:

- проаналізувати основні поняття інтернету та кіберпростору, їх правову природу та ключові характеристики.

- розкрити сутність, методи та засоби здійснення кібератак, а також роль держав і міжнародних організацій як основних кібератакорів.

- вивчити фундаментальні норми міжнародного права, зокрема: принцип суверенітету держав; принцип заборони втручання у внутрішні справи; принцип заборони застосування сили; право на самозахист та міжнародну відповідальність держав.

- провести аналіз конкретних прикладів кібератак, що порушували принципи міжнародного права, зокрема: порушення суверенітету та втручання у внутрішні справи; порушення заборони застосування сили й реалізації права на самозахист.

- визначити ефективність сучасних механізмів імплементації норм міжнародного права щодо кібератак та сформулювати рекомендації для їх удосконалення.

Об’єктом дослідження є правовідносини, що виникають у контексті здійснення кібератак та їхнього регулювання фундаментальними принципами

міжнародного права, такими як заборона втручання у внутрішні справи держав і заборона застосування сили.

Предметом дослідження міжнародно-правові аспекти регулювання кібератак, зокрема дотримання принципів заборони втручання у внутрішні справи держав, заборони застосування сили та права на самозахист у сучасному кіберпросторі.

Методологічну основу роботи складає комплексний підхід, що включає загальнонаукові та спеціальні методи, такі як: аналіз та синтез (для дослідження основних понять, принципів і норм міжнародного права, а також для виявлення сутності кібератак у правовому контексті), системний підхід (для розгляду взаємозв'язків між принципами міжнародного права, державним суверенітетом та кібератаками), історико-правовий метод, порівняльно-правовий метод, метод правового моделювання, емпіричний метод. Цей методологічний підхід дозволяє забезпечити об'єктивність, повноту та глибину дослідження.

Апробація результатів дослідження:

Структура та обсяг дипломної роботи. Структура дипломної роботи зумовлена предметом, метою та завданнями дослідження. Дипломна робота складається із вступу, трьох розділів, якими охоплюються десять підрозділів, висновків та списку використаних джерел (178 найменувань). Загальний обсяг дипломної роботи 125 сторінок, у тому числі список використаних джерел - 18 сторінок.

РОЗДІЛ 1
ПРАВОВА ПРИРОДА ПОНЯТТЯ ІНТЕРНЕТ ТА КІБЕРПРОСТІР

1.1. Технологія що забезпечила світ у віку - інтернет.

Інтернет – це технологія масової комунікації, яка має відносно коротку історію і широко використовується в усьому світі.

У своїй основній формі це означає «мережа мереж» і визначається як система, яка об’єднує комп’ютери по всьому світу за допомогою своєї інфраструктури.1 Інтернет, сфера використання якого розширюється з кожним днем, з часом став невід’ємною частиною нашого життя та веде розвиток інформаційного суспільства разом із комп’ютером, одним із основних продуктів інформаційних технологій.

Інтернет, по суті, є продуктом періоду холодної війни між Сполученими Штатами Америки (США) та Союзом Радянських Соціалістичних Республік (СРСР).2 Після того як у 1957 році СРСР успішно завершив проект «Супутник» і відправив у космос перший штучний супутник, США зробили крок вперед у гонці в галузі науки і техніки і у 1958 році створили Агентство перспективних дослідницьких проектів (ARPA) при Міністерстві оборони.

Основна мета ARPA - забезпечити продовження зв'язку між базами США, розташованими в різних частинах світу, проти можливого ядерного нападу. Для цього шлях зв’язку, який буде використовуватися, не повинен бути з’єднаний з одним центром, він повинен забезпечувати одночасний доступ до кількох з’єднань, і якщо одне з з’єднань пошкоджено, інші повинні мати можливість продовжувати зв’язок. Було виконано багато проектів для маршруту зв'язку, який включав би всі ці функції, і врешті-решт була розроблена комп'ютерна мережа, яка отримала назву ARPANET. Після того, як у 1969 році в Каліфорнії були закладені фізичні основи ARPANET, перші дії, пов’язані з Інтернетом, були конкретизовані та проклали шлях для багатьох досліджень, які продовжують розвиватися до сьогодні.3

ARPANET, проект, ініційований Міністерством оборони США з метою використання його як військового маршруту зв'язку, є першим етапом становлення інтернет-технологій. У 1970-х роках Англія та Норвегія були інтегровані в мережеву структуру, що об’єднує 38 хост-комп’ютерів, і разом із розширенням трафіку зв’язку були розроблені нові мережеві протоколи. Ці протоколи, які називаються протоколом керування передачею (TCP) та протоколом Інтернету (IP), служать для організації даних, які запитуються від сервера, у пакети та досягнення місця призначення в правильному порядку та без помилок.4 Після того, як протоколи, про які йде мова, почали використовуватися, сигнали мережевої системи, яка буде незалежною та відкритою для громадськості, були подані за допомогою терміну «інтернет» у статті, написаній Вінтоном Г. Серфом і Робертом Е. Каном про Протокол керування передачею.5 До 1983 року всі мережі, підключені до ARPANET, почали використовувати TCP та IP, а старий мережевий протокол ARPANET був повністю замінений. Таким чином, сукупність взаємопов'язаних і загальнодоступних мереж була названа «інтернетом».6

Сьогодні Інтернет став платформою, де багато різноманітних послуг і транзакцій можна здійснити за короткий час.7 Можна пояснити основні характеристики Інтернет-технології, яка швидко набуває широкого поширення і продовжує набирати популярність, наступним чином: 8

- децентралізованість: немає спеціального головного комп'ютера, який керує використанням Інтернету. Інтернет не можна зробити недоступним, вимкнувши будь-яку машину або комп’ютер;
- свобода: незважаючи на різні заборони в Інтернеті, все ще можна обійти ці заборони через Інтернет;
- глобальність: використання Інтернету не обмежується певною географічною територією. Доступ до даних, опублікованих з будь-якого регіону світу, можна отримати з іншого регіону;

- динамічність: люди можуть робити внесок у дані в Інтернеті, створювати дані самостійно та висловлювати свою думку щодо наявних даних;
- необмеженість: користування Інтернетом не паралельно державним кордонам. Доступ до нього можна отримати через Інтернет скрізь, де є інтернет-інфраструктура.
- асинхронність: на відміну від радіо- та телевізійних трансляцій, інтернет-трансляції не повинні споживатися протягом певного часу. Усі дані, записані в Інтернеті, доступні без будь-яких часових обмежень.

Очевидно, що особливості, які ми описали, мають багато позитивних і негативних впливів на світ. Однак слід зазначити, що використання Інтернету стало необхідною потребою інформаційного суспільства, з його перевагами та шкодою.

Зі швидким розвитком комп'ютерних технологій і технологій мобільних телефонів спектр інструментів, які можуть здійснювати транзакції через Інтернет, значно розширився. Таким чином, дискусії щодо вразливості безпеки, яку може спричинити Інтернет, вийшли на перший план у національному та міжнародному праві. Наприкінці 20-го та на початку 21-го століть держави зосередилися на національній кібербезпеці почав розробляти свою політику, і «кіберпростір» став частиною нашого життя.9

1.2. Кіберпростір у поняттях та термінах: походження, основні риси та концепції.

Інтернет і комп'ютерні технології не тільки залишилися бездіяльними технологіями, які досягли значного прогресу з моменту свого винаходу, але також зіграли певну роль у появі нових концепцій і розвитку існуючих концепцій. Кіберпростір є одним із цих понять. Слово «кібер» засноване на понятті «кібернетика» та науки про кібернетику, які походять від давньогрецьких слів «kübernetes», що означає «кермовий, який керує

кораблем», і латинських слів «gobernare», значення «управління, керівництво, адміністрування».10

Виникнення науки кібернетики бере свій початок від Ебу'л Із Ісмаїла Ібні Реззаза Аль-Джазарі, який надихнув інших вчених, створивши багато машин і винаходів у Середньовіччі. Аль-Джазарі є винахідником 60 різних машин, таких як науково-технічні роботи, годинники, автомати з водою, термоси, автоматичні дитячі іграшки, кодові замки та сейфи. Аль-Джазарі, видатний ісламський вчений, відомий як людина, яка заклала основи комп'ютера та була піонером науки кібернетики.11 Проте про кібернетику як науку почали згадувати набагато пізніше, у 1900-х роках.

Кібернетика вперше була використана в 1948 році математиком Норбертом Вінером у книзі під назвою «Кібернетика або управління та зв'язок у тварин і машин» 12, у значенні «наука про зв'язок-контроль між тваринами та машинами». Кібернетика, яку в Турецькій мовній асоціації називають «керівною наукою», визначається як наука про ефекти, яка служить для вивчення контролю та зв'язку в технологічних, біологічних, соціологічних та економічних системах.13 Підводячи підсумок, можна сказати, що наукою, яка вивчає контроль абстрактного зв'язку між живими істотами та машинами, є кібернетика, яка взаємодіє з багатьма галузями науки. Концепція кібернетики, яка є основою науки кібернетики, відноситься до віртуального утворення, в якому живі істоти та машини можуть діяти на одній площині.

Кіберпростір – це не технічний термін, створений вченими. Це поняття, яке вперше використав у 1982 році Вільям Гібсон, один із письменників-фантастів, у своїй праці під назвою «Палаючий хром»14. Він детально описав кіберпростір у своїй праці «Нейромант»15, опублікованій у 1984 році. Визначення кіберпростору в роботі таке:16

Кіберпростір. Згодна галюцинація, яку щодня відчувають мільярди законних користувачів у кожній країні, коли дітей навчають математичним концепціям… Графічне представлення даних, взятих із банків кожного

комп’ютера в системі людини. Немислима складність. Лінії світла лежать у кволості розуму, у кластерах і сузір’ях даних. Як вогні міста, віддаляються…

У 1990-х роках визначення кіберпростору стали науковими та розширеними, йдучи в ногу з розвитком у світі. Бенедикт пояснював кіберпростір як «глобальний мережевий віртуальний і штучний комунікаційний простір, який підтримується за допомогою комп’ютерів, забезпечує доступ і виробляє дані»17.

Як видно, кіберпростір не має іншого значення, ніж його вигадана сторона в процесі свого виникнення. Проте з часом, з поступовим зростанням, кіберпростір став важливим у багатьох сферах. Однією з таких галузей є міжнародне право. У 2009 році Лібіцкі визначив кіберпростір як «менш відчутне багатошарове віртуальне середовище, яке використовує комунікаційні інфраструктури, схожі на наземні, морські, повітряні та космічні домени, але незалежні від них»18. Дане визначення зайняло своє місце в літературі як інше та детальне пояснення для пояснення структури кіберпростору та його місця в міжнародному праві.

Виходячи з цих визначень, можна сказати, що кіберпростір – це інформаційний пул, який має дві частини: конкретну через свою фізичну інфраструктуру, незалежну від реального світу, та абстрактну з розумінням віртуального простору. З іншого боку, він постійно розвивається завдяки своїй динамічній структурі. Кіберпростір, до якого за своєю природою можна отримати доступ з будь-якого місця, створив нову реальність зі своїм розмахом і масштабом впливу.

З усіх цих причин політичне значення кіберпростору, як і будь-якого питання, яке може змінити баланс між державами, є надто великим, щоб його заперечувати. Кіберпростір, який інтенсивно вивчали уряди, армії, приватні компанії та цивільні мережі, став центром багатьох дискусій, приносячи з собою нові функції та концепції.19

Тепер розглянемо основні риси кіберпростору. Для того, щоб якусь територію можна було вважати кіберпростором, вона повинна мати певні

характеристики. Простір, який не містить усіх розглянутих функцій, може бути лише однією з частин, які складають кіберпростір. Кіберпростір складається з чотирьох рівнів: користувачі, які беруть участь у кібер-досвіді, дані у віртуальному середовищі, логічні будівельні блоки та фізичні основи, які створюють послуги та підтримують структуру платформи.20 Однак його ексклюзивні характеристики підсумовуються таким чином:21

- Тимчасовість: кіберпростір перетворює традиційне сприйняття часу на майже миттєві ситуації.

- Фізичність: кіберпростір ігнорує обмеження географічного та фізичного розташування.

- Проникність: кіберпростір має силу проникати через кордони та юрисдикції.

- Плинність: кіберпростір перебуває в стані постійних змін і реструктуризації.

- Участь: кіберпростір зменшує бар'єри для дій і політичного самовираження.

- Атрибуція: актори та посилання на дії в кіберпросторі приховані.

- Підзвітність: механізми відповідальності можуть бути легко порушені в кіберпросторі.

Враховуючи всі ці особливості, можна чітко зрозуміти, наскільки важливі події може спричинити кіберпростір. У той час як зміни та розвиток, що відбуваються у фізичному світі, впливають на кіберпростір, дії, що відбуваються в кіберпросторі, також можуть мати наслідки у фізичному світі. З кожним днем різниця між реальним світом і кіберпростором зникає, і кіберпростір можна включити в кожен аспект нашого життя.22 З цієї причини дослідження оборони та безпеки, пов’язані з кіберпростором, продовжують зростати в національній і міжнародній діяльності.

Концепції кіберпростору в національному та міжнародному полях. З розвитком технологій та інформаційних систем до дебатів щодо суверенітету держав додалася нова тема, а кіберпростір зайняв своє місце як один із знаків

запитання в міжнародному праві. У міру того як кіберпростір досяг потенціалу раптового впливу на різні аспекти нашого життя, виникли актуальні дискусії щодо того, чи слід вважати його п’ятою зоною для військових дій, окрім суші, моря, повітряної та космічної зон, які вважаються просторовими та підпорядковуються нормам міжнародного права.

Подібним чином тривають дискусії щодо того, чи має кіберпростір структуру на кшталт «глобального партнерства»23, яке знаходиться поза межами суверенітету держав і може розглядатися як зона загального користування для людства.24 У цьому контексті держави висловлюють свої думки в своїх внутрішніх законах і політиці з метою захисту своїх власних активів.

Основні поняття щодо кіберпростору в Туреччині. Туреччина проводить дослідження кібербезпеки під назвою «Національна стратегія кібербезпеки та план дій» з 2013 року та надає важливого значення концепціям і визначенням у межах цих досліджень. У цьому контексті кіберпростір визначається як «усі системи та служби, які прямо чи опосередковано підключені до Інтернету, електронних комунікацій та комп’ютерних мереж». 25 Виходячи з даного визначення, слід зазначити, що розвиток кіберпростору та всіх понять, пов’язаних з кіберпростором, пов’язаний з інтернет-послугами.

Кібербезпека визначається наступним чином:26

Діяльність, яка включає захист інформаційних систем, які складають кіберпростір, від атак, забезпечення конфіденційності, цілісності та доступності інформації/даних, що обробляються в цьому середовищі, виявлення атак і кіберінцидентів, активацію механізмів реагування на ці виявлення, а потім повернення систем до їх стану перед кіберінцидентом

Кібератаки, які призведуть до порушення кібербезпеки, визначаються таким чином:27

Це навмисні дії, вжиті людьми та/або інформаційними системами будь-де в кіберпросторі, щоб усунути конфіденційність, цілісність або

доступність інформації та промислових систем управління в космосі або інформації/даних, які обробляються цими системами.

Кіберінциденти визначаються як «порушення конфіденційності, цілісності або доступності IT та промислових систем управління або інформації/даних, що обробляються цими системами».28 У цьому контексті можна побачити, що основні відмінності між кібератаками та кіберінцидентами – це мета заподіяння шкоди та навмисні дії. Крім того, можна чітко сказати, що руйнівна сила кіберінцидентів знаходиться на нижчому рівні, ніж кібератаки.

Основні концепції кіберпростору США. Кіберпростір є дуже важливим для США, які є піонерами багатьох технологічних розробок. Згідно з визначенням у Словнику Міністерства оборони США, кіберпростір визначається як «глобальний простір в інформаційному середовищі, що складається з взаємопов’язаних інфраструктур інформаційних технологій і вбудованих мереж передачі даних, включаючи Інтернет, телекомунікаційні мережі, комп’ютерні системи, вбудовані процесори та контролери». 29 Крім того, у буклеті «Концепція операцій у кіберпросторі», підготовленому армією США на 2016-2028 роки, поточна ситуація в кіберпросторі була описана як «п’ята зона після повітря, землі, моря та космічних територій", і було зазначено, що ці п'ять сфер взаємопов'язані.30

Інші важливі питання в Словнику, підготовленому Міністерством оборони США, стосуються безпеки в кіберпросторі та визначення атак. Безпека кіберпростору записується так:31

Автентифікація, конфіденційність і відмова в ідентифікації, що здійснюються в кіберпросторі, щоб запобігти та захистити комп’ютери, системи електронного зв’язку та інші інформаційні технології, включаючи інформаційні технології платформи, а також існуючу інформацію від несанкціонованого доступу, використання або пошкодження всіх цих проблем, щоб забезпечити доступність і цілісність кіберпростору. Дії у формі невразливості включають безпеку кіберпростору.

Атаки в кіберпросторі визначаються як «дії, що здійснюються в кіберпросторі, які створюють помітні ефекти відмови (перешкоди, порушення або руйнування) у кіберпросторі, або маніпуляції, які з'являються у фізичному просторі та вважаються різновидом пожежі та призводять до відмови».32 Коротко пояснюючи, дії, які відбуваються в кіберпросторі і можуть спричинити збій, порушення та руйнування як у кіберпросторі, так і у фізичній зоні, вважаються атаками в кіберпросторі.

Основні концепції кіберпростору в Організації Північноатлантичного договору (НАТО). НАТО, яка була створена після закінчення Другої світової війни з метою захисту балансу сил і суверенітету держав Західного блоку від загрози СРСР, членом якої є Туреччина, є однією з найважливіших міжнародною організацією в політичній історії. Зіштовхнувшись зі складною структурою кіберпростору з 1990-х років, НАТО наполегливо працювала та розробляла різні методи та стратегії для створення превентивних заходів проти кібератак.33

У результаті кібератак на країни-члени після втручання в Косово в 1999 році НАТО включила кіберзахист до свого порядку денного, щоб зберегти свою владу, створила підструктури для роботи над цією темою та запровадила багато міжнародних документів. На самітах НАТО чітко розуміється, що кібербезпека розглядається як нова військова сфера, і оборонна політика дотримується відповідно.34 Зрештою, в рамках «Талліннського посібника з міжнародного права, що застосовується до кібероперацій»35, розробленого в НАТО, кіберпростір визначається як «середовище, утворене фізичними та нефізичними компонентами для зберігання, обміну та передачі даних за допомогою комп'ютерних мереж. "36.

Путівник по Таллінну був підготовлений у 2009–2012 роках під керівництвом Майкла Н. Шмітта, опублікований у 2013 році та оновлений у 2017 році. У той період, коли були усвідомлені сильні наслідки кібератак, Міжнародна група експертів, яка працювала разом із Об'єднаним центром передового досвіду кіберзахисту НАТО (CCDCOE), також взяла участь у

підготовці Талліннського посібника.37 Керівництво по суті охоплює кібердіяльність держав у мирний час за міжнародним правом. Це початок довгих і важливих дебатів щодо його імплементації. 38 Талліннський посібник, який не є обов'язковим, але є найповнішим міжнародним польовим дослідженням, підготовленим на даний момент, є звітом, який відображає перспективи багатьох держав і має міжнародне значення. Текст, про який йде мова, буде розглянуто більш детально в наступних частинах нашого дослідження.

Основні концепції кіберпростору в Шанхайській організації співробітництва. Інструментальна перспектива для кіберпростору та кібератак була розроблена в роботі Шанхайської організації співробітництва, очолюваної Росією та Китаєм, до складу якої входили також Киргизстан, Таджикистан, Казахстан, Узбекистан, Індія та Пакистан, з Туреччиною як " партнером по діалогу' 39

З розвитком інформаційно-комунікаційних технологій було укладено «Угоду про співробітництво щодо забезпечення міжнародної інформаційної безпеки між державами-членами Шанхайської організації співробітництва»41. У додатку до договору 42 було зазначено багато визначень понять, пов'язаних з кіберпростором, таких як інформаційний простір, інформаційна безпека, інформаційна зброя та інформаційна війна.43

Згідно з додатком до договору, сфера інформації визначається як «сфера діяльності, пов'язана з формуванням, виробництвом, перетворенням, передачею, використанням і зберіганням інформації, що впливає, серед іншого, на індивідуальну та суспільну свідомість». Інформаційна безпека визначається як «стан та інтереси особи, суспільства і держави, коли вони захищені від загроз, деструктивних та інших негативних впливів в інформаційному полі». Інформаційна зброя означає «інформаційні технології, засоби та методи, що використовуються для ведення інформаційної війни».44

Нарешті, концепція інформаційної війни, яка охоплює весь процес кібератаки, пояснюється Шанхайською організацією співробітництва наступним чином:45

Інформаційна війна — конфлікт між двома або більше державами в інформаційному просторі з метою нанесення шкоди інформаційним системам, процесам і ресурсам, структурам критичного значення та іншим структурам, підриву політичних, економічних і соціальних систем, психологічного маніпулювання масами населення з метою дестабілізації їх.

Як бачимо, потреба держав у забезпеченні кібербезпеки в межах національних кордонів подібним чином проявилася в міжнародних відносинах. Таким чином, визначення кіберпростору та термінів, пов'язаних з кіберпростором, стало важливим. Розвиток технологій продовжує прискорювати ці дослідження.

1.3. Основні засоби та методи кібератак.

Хоча в кіберпросторі можуть відбуватися дії, які позитивно вплинуть на окремих людей і держави, можуть мати місце і негативні дії та кібератаки, які можуть становити потенційну загрозу. Існує багато типів кібератак. У цьому контексті програмне забезпечення для кібератак було згруповано з урахуванням деяких ознак. Це угрупування допомагає зрозуміти функціонування кібердій. У цьому розділі, який має переважно технічну сторону, ми обмежимося інформацією про основні теми. Одразу після наших пояснень ми також торкнемося основних методів кібератак, у яких програмне забезпечення, про яке йдеться, використовується як інструмент.

Тепер розглянемо програмне забезпечення для кібератак, що залежить від іншої програми.

1. Вірус

Віруси складаються з фрагментованих кодів, які можуть копіювати себе у більші програми та мати можливість втручатися в цю програму. Щоб вірус

став активним, програма, яку він містить, має бути запущена. Поки відповідна програма працює, вірус повторюється та поширюється на інші програми.46 По суті, віруси схожі на біологічні віруси з точки зору того, як вони працюють, і є типом програмного забезпечення, яке часто використовується в кібер-діях.

Віруси зазвичай з'являються у вигляді файлів програми. Хоча деяким вірусам для копіювання потрібен Інтернет і локальні мережі, деякі можуть використовувати пристрої зберігання, такі як жорсткі диски, USB-диски, компакт-диски та DVD-диски. Під дією вірусу деякі дані в програмах змінюються або видаляються. Ступінь небезпеки в цьому відношенні змінюється залежно від мети та знань особи, яка створила вірус і дозволила проникнути в програму.47

Вірус Melissa, створений Девідом Л. Смітом і з'явився в 1999 році, був першим вірусом, якому вдалося поширитися через систему електронної пошти. Коли користувачі Microsoft Outlook цікавилися вмістом важливих електронних листів і відкривали їх, вони бачили, що файл було надіслано з контактів у їхній адресній книзі, і завантажували його на свої комп’ютери. Після того, як відповідний файл було відкрито, електронний лист такого ж типу було надіслано першим 50 особам в адресній книзі користувача за вказівкою вірусу Melissa. Крім того, вірус знищував документи, створені за допомогою шаблону Microsoft Word, і продовжував заражати новостворені документи. Вірус Melissa заразив приблизно 1,2 мільйона комп’ютерів і 53 тисячі серверів, і, за оцінками, вирішення проблеми коштуватиме від 249 до 561 мільйона доларів.48

У сучасних умовах існують також просунуті та складні віруси, які можуть зробити комп’ютерні системи непридатними для використання та завдати фізичної шкоди різному обладнанню.49 З цієї причини дуже важливо, щоб системи постійно перевірялися, вживалися необхідні заходи безпеки, а технічне обслуговування та ремонт не переривалися.

2. Троянський кінь

Троянський кінь складається з фрагментованих кодів, які проникають у систему, ховаючись у корисній програмі, і таємно спрямовані на нанесення шкоди системі.50 Це програмне забезпечення, яке часто може проникати в систему, розміщуючи його в електронних листах, не активується, доки не запуститься програма, у якій воно приховано. Якщо троянський кінь активований, інформація про незахищене програмне забезпечення хоста та сервери захоплюється та надсилається зловмиснику, який приховує троянського коня.51

Одним із цікавих прикладів троянів є програмне забезпечення GPCoder, яке було виявлено в 2005 році. GPCoder заражав системи Windows і цільові файли з певними розширеннями, він шифрував їх і видаляв оригінали з системи. Власник або користувачі системи не можуть отримати доступ до файлів, зашифрованих за допомогою сильного методу шифрування. Крім того, на головному екрані системи розміщено текстовий файл, який спрямовує вас до деталей необхідної виплати викупу та інших процедур дешифрування, які необхідно виконати, щоб отримати доступ до файлів. Згодом також з'явилося більш комплексне та складне програмне забезпечення для троянів, наприклад Archiveus, Krotten, Cryzip і MayArchive.52

Основне призначення троянського коня, який може виконувати різноманітні операції у фоновому режимі без дозволу та відома системного адміністратора, — поставити існуючу систему під контроль зловмисника. Таким чином, зловмисник може пересуватися непоміченим у проникнутій системі та завдати більшої шкоди за допомогою дистанційних атак.53 Враховуючи, що вміло створений троянський кінь рухається, не розкриваючись і не залишаючи слідів, очевидно, наскільки важливо бути обережним у цьому відношенні та підтримувати безпеку системи.

3. Логічна бомба

Логічна бомба, на відміну від іншого програмного забезпечення, є шкідливим програмним забезпеченням, яке розміщується всередині програми

та стає активним залежно від настання певного часу або умови запуску.54 Логічна бомба, яка є нешкідливою протягом інкубаційного періоду, може змінювати, видаляти, або змінити дані після його активації. Це може спричинити багато небажаних наслідків, наприклад, зробити систему непридатною для використання, вибух тощо.

У 1982 році, коли тривав період холодної війни, комп'ютерні технології стали важливим інструментом для Центрального розвідувального управління США (ЦРУ). Радянський Союз викрав у канадської компанії програмне забезпечення, здатне контролювати газопроводи. Однак виявилося, що це програмне забезпечення насправді було пасткою з логічною бомбою, закладеною ЦРУ. Це програмне забезпечення, яке працювало інтегровано з комп’ютерними системами, через деякий час зламалося, і система заплуталася. Таким чином, логічна бомба скидає швидкість насоса та налаштування клапанів у трубопроводах природного газу, збільшуючи потік до аномальних рівнів і підвищуючи тиск у магістралі. Зрештою, США вдалося підірвати Сибірський газопровід, який вийшов з-під контролю. Цей інцидент, який був скоєний США як вибух сибірського природного газу, є першим випадком, у якому програмне забезпечення для кібератак було використано на національному та міжнародному рівнях. Крім того, цей вибух був описаний як найбільший неядерний вибух, який будь-коли бачили.55

Логічну бомбу можна просунути в систему різними способами. З цієї причини їй важко запобігти та виявити. Хоча періодичне сканування системи за допомогою програмного забезпечення безпеки є корисним рішенням для усунення логічних бомб, немає ніякої гарантії від миттєвих атак.56 З усіх цих причин важливо приділяти увагу миттєвим і періодичним перевіркам, робити оновлення безпеки та виконувати процес знищення, якщо виявлено логічні бомби.

4. Backdoor (Бекдор/люк)

Бекдор або люк — це механізм, який розміщується в системі його творцем або за його згодою. Мета бекдору полягає в тому, щоб гарантувати,

що засоби захисту нормально функціонуючої системи можна легко обійти, а зловмисник, який встановлює систему та розміщує бекдор, може легко проникнути.57

Завдяки бекдорам, які неможливо виявити навіть під час періодичних перевірок, зловмисник має можливість увійти в систему та отримати, змінити та видалити наявні дані та інформацію.58 Зловмисник може використовувати систему сам, як і користувач системи. .

Одне з найвідоміших тверджень про бекдори полягає в тому, що Microsoft отримувала допомогу від Агентства національної безпеки США (АНБ) під час розробки операційних систем Windows і додала бекдори до систем в обмін на цю допомогу.59 У цьому контексті можна легко сказати, що навіть запатентованій програмі не варто повністю довіряти. Звичайному користувачеві практично неможливо визначити, чи містить програма шкідливий код.

Необхідно бути надзвичайно обережним щодо руйнування, яке може бути спричинене програмним забезпеченням, яке може проникати в інформаційні системи залежно від різних програм і добре приховувати себе. У цьому контексті важливо проводити регулярні перевірки та роботи з посилення існуючого програмного забезпечення фахівцями в цій галузі.

Програмне забезпечення для захисту від кібератак, незалежне від інших програм.

1. Бактерії (Bacterium)

Бактерії — це зловмисне програмне забезпечення, яке може розмножуватися незалежно один від одного та створювати різні версії системи, у яку вони проникають. Кожна нова версія, яка постійно збільшується, займає все більше місця на диску і послаблює роботу системи. Використання системних ресурсів у такий спосіб негативно впливає на операційну систему, і зрештою система стає непридатною для використання, коли весь простір заповнено.60

2. Хробак

Хробак — це програмне забезпечення для кібератак, яке може існувати незалежно в системі та поширюватися на різні системи, копіюючи себе. Його можна швидко скопіювати на сховище та мережеві пристрої, підключені до системи, у якій він знаходиться.61

Найважливішою особливістю хробаків є те, що вони не потребують ніякої взаємодії з людиною, крім їх створення.62 Спонтанно створюючи тунель у системі, він відкриває шлях для дистанційного керування системою. Це може призвести до збою мережі, розриву з'єднань, уповільнення роботи системи та збою.63

Перший комп'ютерний черв'як з'явився в 1988 році. Деякі проблеми виникли в 6000 комп'ютерних терміналів, які були одними з перших зразків комп'ютерних систем у США. Користувачі не могли користуватися комп'ютерними терміналами, а системи виходили з ладу. Під час розслідування джерела інциденту було виявлено програму-хробак, створену особою на ім'я Роберт Морріс і залишену в Інтернеті.64 В результаті дій цієї особи, яка в своїй заяві заявила, що хоче проявити себе та розважитися, система вийшла з-під контролю, мережа Інтернет зруйнувалася та завдано збитків у розмірі 98 мільйонів доларів.65 Крім того, є важливими прикладами використання хробаків, таких як Conficker і Slammer, які мають великий міжнародний вплив, коли вони з'являються.66

Далі рознлянемо основні методи кібератак.

1. Відмова в обслуговуванні (DoS/DDoS)

Відмова в обслуговуванні, одна з найруйнівніших кібератак, призводить до того, що система або мережа, підключена до послуги, що надається через Інтернет, стає непридатною для використання. Ця атака здійснюється шляхом блокування сервера, пристрою, служби, мережі, програми та окремих процесів у програмі. Спочатку обслуговуючий сервер заповнює простір обробки системи, надсилаючи системі запити, яких насправді не існує. Система, яка не може відповісти на надмірні запити даних та інформації, дає

збій або виходить з ладу. 67 Якщо атаки типу «відмова в обслуговуванні» спрямовані на одну ціль із кількох джерел, це називається атакою розподіленого типу «відмова в обслуговуванні» (DDoS). У таких атаках мета полягає в тому, щоб повністю зруйнувати одну систему з сотень або навіть тисяч машин.68

Атаки типу «відмова в обслуговуванні» зазвичай здійснюються проти веб-серверів державних, комерційних, банківських і медіа організацій. У цьому контексті багато фінансових втрат зазнають у процесі усунення атаки та повернення серверів до нормального курсу.69 Важливо продемонструвати необхідну відданість, щоб запобігти пошкодженню критичної кібер інфраструктури та систем контролю, щоб запобігти незворотній шкоді.

2. Зомбі/підлеглий комп'ютер (ботнет)

Комп’ютер-зомбі/підлеглий комп’ютер – це система, яка може використовуватися зловмисниками без відома власника та в яку введено програмне забезпечення для кібератак. Взаємопов’язані комп’ютерні мережі-зомбі часто використовуються для розповсюдження шкідливих програм і здійснення кіберзлочинів. Групою комп’ютерів-зомбі, захоплених для здійснення кібератаки, керує адміністратор під назвою «ботмайстер». Botmaster перетворює відповідні комп’ютери на армію, готову атакувати за командою та атакувати всю територію в межах своєї інфраструктури.70

Комп’ютер-зомбі, який сьогодні вважається одним із найнебезпечніших методів кібератак, має очевидний вплив і може використовуватися з великими та спланованими групами комп’ютерів, якщо його розумно спроектувати. Не слід забувати, що якщо на персональних комп’ютерах не вжити необхідних заходів безпеки, багато кіберзлочинів можуть бути легко вчинені без відома користувачів і можуть викликати скарги.

3. Підвищення привілеїв

Ескалація авторизації є одним із важливих кроків, які відкривають шлях для кібератак. Зловмисники використовують уразливості системи безпеки, щоб отримати доступ до адміністраторів або розробників у цільовій системі

або використовувати їхні привілеї в системі. Зрештою, зловмисник може будь-коли проникнути в систему, отримавши коди авторизації. Таким чином, це може пошкодити програми в системі, змінити існуючі коди, запобігти доступу реальних користувачів системи, і, крім того, воно може повністю порушити роботу системи, отримавши доступ до паролів адміністратора.71

4. Соціальна інженерія

Соціальна інженерія — це метод кібератак, який використовується, коли люди вважаються найслабшим компонентом систем безпеки. У цьому процесі люди піддаються дії впливу, обману, примусу та зниження чесності чи відданості з боку соціального інженера та передачі даних та інформації про систему, до якої вони мають доступ. Таким чином, соціальний інженер досягає своєї мети, обходячи захист системи через людський фактор і опосередковано завдає шкоди репутації.72

Основна мета соціального інженера полягає в тому, щоб дозволити хакерам отримати, пошкодити, видалити дані та зробити систему непридатною для використання після отримання доступу до системи.73 Соціальні інженери, які знають, як використовувати фізичні вразливості та психологічні слабкості, надзвичайно небезпечні. Однак слід підкреслити, що дослідження соціальної інженерії самі по собі нічого не означають, їх потрібно підтримувати іншими інструментами та методами в кіберпросторі.

5. Розширені стійкі загрози

Розширені стійкі загрози, які зробили собі ім’я за останні кілька років, являють собою структуру атак, яка повністю орієнтована на ціль, добре організована, поширюється протягом тривалого періоду часу та має за собою велику підтримку. Основна мета цієї атаки, яка не припиняється до тих пір, поки вона не захопить цільову систему, полягає в отриманні даних з повним доступом. Приховані, цілеспрямовані, універсальні та адаптовані, ці атаки постійно змінюються.74

Розширені стійкі загрози, на відміну від інших кібератак, спрямовані на заздалегідь визначену та досліджену ціль, спрямовану на вивчення,

поширення та отримання конфіденційної інформації після входу в систему, не вимагають жодної програми чи підключення до мережі, і можуть приховуватися та продовжувати атаку. 75 Запобіжні заходи повинні бути вжиті якомога інтенсивніше проти цієї загрози, яка є масштабним проектом із етапами виявлення, підготовки, ідентифікації цілі, отримання та підтримки доступу, збору даних та витоку.

Потреба держав у забезпеченні кібербезпеки в межах національних кордонів так само проявилася в міжнародних відносинах, і визначення цієї сфери та встановлення кордонів стало важливим. У цьому контексті внутрішні та зовнішні суб'єкти повинні бути добре відомі проти цього програмного забезпечення та методів кібератак, заходи безпеки мають бути посилені, а існуючі правила повинні бути підкріплені конкретними ефектами.

1.4. Держави та міжнародні інституції як кіберактори

Кіберактор — це ім'я, яке можна дати всім особам, установам і державам, які існують у кіберпросторі та мають здатність вживати заходів і створювати зміни в кіберпросторі. Хоча держави є акторами, які мають найбільше голосу в цьому питанні та керують процесом кіберактивності, важливість недержавних акторів також незаперечна. Кордони між державами та недержавними акторами можуть стати розмитими в кіберпросторі. Держави, міжнародні інституції та недержавні актори демонструють свою присутність у кіберпросторі з багатьма хорошими та поганими цілями.

Міжнародна відповідальність і приписування в кіберпросторі є важливими в процесі визначення особи та місця знаходження особи, яка вчинила кібердіяння. Дії, що здійснюються в кіберпросторі, можуть призвести до проблем щодо відповідальності між державами, не підпадаючи під географічні обмеження. З цієї причини точки з'єднання, пов'язані з кіберактивністю, є одним із питань, на які держави повинні звернути увагу.

Особи, які складають суспільство, можуть взаємодіяти та спілкуватися за межами держав через мережеву інфраструктуру та Інтернет.76 З цієї причини при розробці політики в кіберпросторі та інтеграції їх в існуюче політичне утворення слід також враховувати діяльність окремих осіб. По суті, ставлення та поведінка окремих людей до кібер-діяльності може викликати серйозну плутанину навіть у будь-якій державі.

Важко зробити чітку класифікацію в кіберпросторі, яка значною мірою змінює класифікацію держави, недержавного актора та особи.77 По суті, визначення меж у кіберпросторі відрізняється в кожному конкретному випадку через природу та унікальність кіберпростору. Однак буде легше досліджувати це питання, розрізняючи державу та недержавних акторів.

Міжнародна арена, де головними акторами виступають держави, тісно пов'язана з факторами суверенітету та зовнішньої політики. Для держав, які проявляють себе та підтримують своє існування через офіційну діяльність, кіберпростір є новим утворенням, яке змушує їх розглядати ідею суверенітету та національних кордонів з іншої точки зору. Основний момент у зміні класичної перспективи полягає в тому, що кіберпростір з його унікальними характеристиками має здатність завдавати шкоди державам.78

З глобалізацією міжнародна співпраця набула важливості у вирішенні основних проблем, які виходять за межі національних кордонів у таких сферах, як права людини, навколишнє середовище, економіка та глобальне потепління. У цьому контексті слід також оцінювати проблеми кіберпростору, який зберігає своє місце на порядку денному завдяки інноваційним розробкам у технологіях і комунікації. На відміну від традиційних збройних атак, атаки в кіберпросторі більш гнучкі у розпізнаванні правил і перешкод. По суті, більшість дій, які вживаються державами для захисту та зміцнення національних мережевих інфраструктур, реалізуються шляхом спільних кроків між приватним сектором, постачальниками послуг, експертами, групами промислово розвинутих країн і урядами, які співпрацюють.79 На

даному етапі можна легко сказати, що тонка грань між державами та іншими кібератакорами стала розмитою, а національні кордони стали неважливими.

Окрім міжнародного співробітництва, держави прагнуть забезпечити безперервність кіберпростору за допомогою підходу, орієнтованого на безпеку. Видно, що дії в цьому середовищі впливають на держави пропорційно залежності від інтернет-інфраструктури та кіберпростору та формують свою політику відповідно до цих факторів. 80 У результаті конкуренції в кіберпросторі, який багато держав почали розглядати як «п'яте поле бою», значні інвестиції здійснюються в кіберармії, системи захисту та розвідки.81 Цей ланцюг командування, який відіграватиме активну роль у боротьбі, має завдання стежити за кібервійною та розробляти методи ведення війни.82

Кіберармія, оборонні та розвідувальні структури можуть бути підрозділами, створеними та офіційно використовуваними державою, або вони можуть складатися з добровольчих підрозділів, які підтримуються державою, але не є офіційними. 83 Ці структури, укомплектовані фахівцями з інформаційної безпеки, які здатні захистити від загроз і атак, які можуть надходити з кіберпростору, і реагувати в разі потреби, подібні до невидимої руки, яка захищає кожну інституцію держави.

Недержавні структури, які йдуть після держав у міжнародному праві та політиці, зазвичай виступають як міжнародні інституції та відіграють певну роль у створенні міжнародних правил. Однак у кіберпросторі поняття недержавного актора використовується для опису ширшої спільноти. Кожна людина та інституція, яка може вносити зміни в кіберпросторі з індивідуальними цілями та дотиками, є частиною недержавних акторів. Насправді, хоча недержавні суб'єкти перебувають на задньому плані у створенні правил щодо кіберпростору, їхні ролі змінюються, коли справа доходить до кібератак.

Очевидно, що в той момент, коли актори в кіберпросторі можуть діяти у своїх власних цілях, кожен з них повинен бути взятий до уваги незалежно.

Насправді всі кіберактори мають можливість впливати на віртуальне середовище в кіберпросторі. З цієї причини дуже важливо пояснити, про яких учасників йдеться, беручи до уваги національну та міжнародну безпеку. Таким чином, люди, які можуть становити небезпеку в кіберпросторі, не залишаться без уваги.

Досить достатньою та інформативною є класифікація факторів, цілей і методів, за якими діють недержавні актори в кіберпросторі, запропонована Йоханом Сігольмом. До категорії недержавних кібератокрів потрапляє будь-який актор, який не має жодних зв'язків із державами чи державної підтримки. Хоча ці суб'єкти можуть принести позитивні результати, вони також можуть призвести до негативних результатів. У рамках мого дослідження ми детальніше розглянемо акторів, які можуть спричинити державні проблеми та міжнародні суперечки. Ми дамо наші пояснення, відповідно до загального визнання, щодо цих акторів, які мають різні визначення та правові рамки в кожній державі.

Хактивісти

Комп'ютерний активізм – це законне чи нелегальне використання ресурсів кіберпростору як загальний засіб протесту, вжиття заходів для донесення до всіх раніше висловленої ідеології або просування політичного порядку денного. Комп'ютерні активісти, які опосередковано переслідують таємні, політичні, військові чи комерційні цілі, беруть участь у підривній діяльності, псуючи веб-сайти, маніпулюючи інтернет-ресурсами, організовуючи атаки типу «відмова в обслуговуванні», вчиняючи крадіжки інформації, використовуючи пародії на веб-сайти та відкриваючи віртуальні сайти.84

Головна мета комп'ютерних активістів – впливати та змінювати політичні, соціальні чи релігійні ідеї. Слід сказати, що сьогодні кожна акція, яка закликає громадськість протестувати проти свободи слова, громадянських прав, релігійних прав та інших питань, у певний момент пов'язана з

комп’ютерними активістами. 85 Комп’ютерні активісти є відображенням громадянської непокори та запитувачів у кіберпросторі.

Хакери

Хакер — це той, хто використовує свої навички роботи з комп’ютерами та мережею, щоб вирішити будь-яку технічну проблему. Хакери, які зазвичай використовують свої навички у злочинній діяльності, прагнуть отримати несанкціонований доступ до систем або мереж. 86 Хакери, класифіковані за кольором капелюха відповідно до їхніх навичок, знань і намірів, поділяються на підкатегорії: чорні, білі та сірі капелюхи.

Чорні хакери - це люди, які використовують комп'ютерні системи та мережі для власних цілей та інтересів. Хакери, які знаходять і використовують вразливі місця в безпеці, здійснюють дії, які принесуть їм матеріальне або моральне задоволення. Ці хакери діють без поваги до законів, збоїв у системах і наслідків для жертв, і в цьому контексті вони вважаються найбільш зловмисним актором серед хакерів.87

Хакери білого капелюха — це люди, які піклуються про етику та мають високі моральні цінності та діють, щоб перешкодити хакерам чорного капелюха. Ці люди працюють над запобіганням можливим проблемам, усуваючи вразливі місця системи безпеки. Обов’язком хакерів із білим капелюхом є зміцнення існуючої системи шляхом тестування на проникнення, забезпечення безпеки системи та розробка методів перевірки користувачів. Зрештою, якщо проблема виявлена, власник системи або адміністратор може бути попереджений і може бути розглянуто можливість виправлення системи.88

Хакери «сірого капелюха» — це люди, які діють без зловмисництва хакерів із «чорним капелюхом», часто дотримуються стандартів хакерів «білого капелюха» і в основному працюють для захисту існуючої системи. Однак, коли ці люди виявляють проблему, яка суперечить їхнім цілям та інтересам, вони можуть працювати над її усуненням і перевищувати дозволені межі.89

На відміну від хет-хакерів, існує також підкатегорія, яка називається патріотичними хакерами. Хакери-патріоти — це незалежні особи, які прагнуть допомогти своїй національній державі в конфлікті чи війні в зовнішньому світі.90 Ці особи діють з тими ж цілями, що й інші хакери, але демонструють більш націоналістичну поведінку. Слід також зазначити, що вони більш різкі та спрямовані, ніж комп'ютерні активісти.91 Хакери можуть діяти в кіберпросторі з багатьма хорошими та поганими цілями, тому важливо визначити їхню роль у конкретному інциденті та вжити заходів проти них.

Кібертерористи

Кібертерористи - це дуже складна та провокаційна група кіберактерів, щодо яких точаться багато суперечок. Ці люди діють, щоб впливати на державу відповідно до політичних цілей чи ідеологій. Кібертерористи здійснюють дії, які створюють страх, паніку та плутанину серед населення, використовуючи комп'ютерні та мережеві технології в кіберпросторі.92

Кібертероризм є привабливим варіантом для сучасних терористів, якщо розглядати його разом із його анонімністю, потенціалом великої шкоди, психологічним впливом та увагою ЗМІ. 93 Враховуючи масштаби та інтенсивність актів кібертероризму, стає зрозуміло, що він може завдати більших руйнувань, ніж комп'ютерні активісти та хакери. Як і в традиційних концепціях тероризму, вбачається, що владі та суверенітету держави загрожує вибір публічно відомих, відкритих і широко поширених цілей. З цієї причини необхідно вжити необхідних заходів проти потенційно успішних атак і вжити заходів для запобігання кібертероризму.

Організовані кіберзлочинці

Кіберзлочинці - це люди, які використовують комп'ютерні та мережеві технології як інструменти або мішені при вчиненні злочинів. Ці люди завдають шкоди, атакуючи системи з метою поширення вірусів, викрадення інформації та з іншими зловмисними цілями. Таким чином, звичайні люди також стають інструментами для таких злочинів, як шахрайство та незаконні

ставки. Мережі кіберзлочинності, які працюють як організована група, складаються з лідера, який керує злочином, тих, хто планує кіберзлочини, і людей, які виконують ролі через ланцюжок командування та ефективно спілкуються. 94 Залежно від розміру та масштабів кіберзлочинності, ці злочини можуть вплинути на держави та міжнародні відносини. У цьому контексті міжнародне співробітництво в боротьбі з кіберзлочинністю забезпечується «Конвенцією Ради Європи про злочини, вчинені у віртуальному середовищі»95, учасницею якої є Туреччина.

Компанії

Компанії, що працюють у кіберпросторі, є керівництвами, які дотримуються правових норм і мають кіберекономічну владу. Ці компанії продовжують свою діяльність автономно, зазвичай на прохання держави, за державним контрактом або під захистом. Державні спецслужби також можуть використовувати корпоративні компанії як прикриття96

Більші та домінуючі на ринку компанії обслуговують технічну галузь добре організованими та навченими працівниками. Крім того, вона має повноваження та ресурси щодо технології, апаратного забезпечення та глобальної комунікаційної інфраструктури, щоб мати право голосу в кіберпросторі. 97 Стратегічне значення таких великих компаній у міжнародних відносинах незаперечне.

Агенти кібершпигунства

Шпигунство — це, по суті, отримання конфіденційних або чутливих даних без згоди власника інформації. Збройні сили держави, розвідувальні підрозділи, компанії, злочинні організації чи будь-які інші особи можуть здійснювати шпигунську діяльність. Дії, вжиті державами для отримання приватної та конфіденційної інформації, тісно пов'язані зі шпигунством. У кібершпигунстві агенти збирають дані та інформацію, використовуючи ресурси кіберпростору. Зібрані результати аналізуються, звітуються та доставляються особі чи установі, яка призначає. У цій ситуації обидві сторони мають економічні та політичні інтереси.98

Кібершпигуни, по суті, є різновидом хакерів. 99 Він обходить захист системи та досліджує комп’ютерні структури без авторизації. У цьому контексті несанкціонований доступ до системи є злочином у внутрішньому законодавстві багатьох держав. Однак, за деякими поглядами, кібершпигунство в сучасних умовах стало невід'ємною частиною економічної конкуренції. Крім того, таємний моніторинг кіберактивності та можливостей потенційних ворогів вважається необхідним для національної оборони.100

Кібер воїни/ополчення

Кібервоїни/міліції — це групи добровольців із можливостями кібератак, які об’єднуються для досягнення більшої мети, крім особистих. Люди, які діють через спільну комунікаційну мережу, приховуючи свою справжню особу, працюють, не будучи пов’язаними з жодною установою чи організацією та не отримуючи жодної фінансової вигоди. Ці воїни, які можуть бути тимчасовою або постійною групою, є гнучкою організацією. Вони не мають жодних договірних зобов'язань. Зрештою, кібервоїни відрізняються від інших організованих груп усіма цими особливостями.101

Кібервоїни можуть діяти, щоб захистити або атакувати комп'ютерні системи. Ці люди, які воюють за допомогою ресурсів кіберпростору, також є майстрами приховувати себе та свої сліди, коли справа доходить до виявлення. З цієї причини слід подбати про захист систем.

Завжди важливо визначити акторів, які діють у будь-якій сфері на міжнародній арені, і відносини між цими акторами. Поряд з державами, які відіграють вирішальну роль в управлінні, регулюванні та розвитку кіберпростору, існують також недержавні актори, які використовують свої повноваження незалежно. У поєднанні з наявністю багатьох учасників з різними цілями в кіберпросторі, анонімним характером кібер-дій і простим приховуванням особи можуть виникнути складні результати щодо відповідальності.

Як можна зрозуміти з багатьох різних визначень і пояснень, кіберпростір є основним поняттям у кіберпросторі. Хоча між визначеннями є

схожість, консенсусу ще не досягнуто. У цій площині, де інформацію можна контролювати за допомогою різних пристроїв, легше реалізувати протиправні дії. Однак кіберпростір має структуру, яка може похитнути національні та міжнародні відносини довіри як область, де можуть статися менш дорогі, раптові, анонімні та транскордонні атаки.102

Безпечне використання інформаційних і комунікаційних технологій стало основною потребою в усьому світі. Важливість Інтернету зросла, оскільки він став доступним для людей будь-якого віку, а процес, у якому кібератаки набувають значення, прискорився. Той факт, що Інтернет, який є основою кіберпростору, має інфраструктуру, яка виходить за межі суверенітету держав і не може бути фізично обмежена, хоча можна запобігти її використанню, призвів до того, що він став частиною міжнародних відносин. Імовірність того, що майже будь-що, що можна зробити через Інтернет, може мати наслідки за багато миль, викликає занепокоєння щодо безпеки та безпеки до крайності. 104 У цьому контексті кіберпростір розглядається як щось більше, ніж комп’ютери та цифрова інформація, і національні та міжнародні дослідження були прискорені для створення ефективних і потужних систем захисту від кібератак.

РОЗДІЛ 2
ВІДПОВІДНІ ФУНДАМЕНТАЛЬНІ НОРМИ МІЖНАРОДНОГО ПРАВА ТА КІБЕРАТАКИ

2.1.Правова природа суверенітету держав.

Міжнародне право стосується порядку, встановленого щодо тривалого існування держав. Держави, з іншого боку, побудовані на концепції суверенітету разом із правами та обов'язками, які є основою їх існування. 105 Суверенітет вважається одним із невід'ємних елементів держави, поряд з елементами країни та нації.

Існує багато дискусій щодо визначення та значення суверенітету. Той факт, що суверенітет, який переплітається з такими поняттями, як незалежність і повноваження, також є абстрактним і багатогранним поняттям, є центром цих дискусій. Незважаючи на те, що з цього приводу ведеться багато дискусій, суверенітет, по суті, є невід'ємною частиною міжнародного права та важливим інструментом політики.

Щоб зрозуміти значення та цінність суверенітету, необхідно враховувати історичний процес розвитку поняття суверенітету. По суті, суверенітет – це політичне поняття, яке виникло разом із подіями цього процесу. Оскільки в стародавній епосі не існувало іншого утворення, яке могло б конкурувати з могутністю держави, суверенітет і держава постають як взаємодоповнюючі вирази. Наприкінці Середньовіччя почалася боротьба з релігійно-феодальними силами, які загрожували існуванню держав, виникли дискусії щодо поняття суверенітету. 106

Жан Боден є першим мислителем, який пояснив суверенітет систематично й детально. 107 Відомий французький юрист у своїй праці під назвою «Шість книг про державу» вивів суверенітет від латинського слова «superanus», що означає «найвищий, вершинний», і назвав його «souveraineté». Визначення суверенітету Бодена використовувалося для

вираження абсолютної та постійної влади держави. Відповідно, суверенітет є абсолютним і не обмежується владою, функціями чи тривалістю. Будь-яке обмеження суверенітету суперечить природі суверенітету. Немає іншої сили, крім Бога, над владою, яка має суверенітет.108

Томас Гоббс — ще одна людина, яка відіграла важливу роль у розвитку концепції суверенітету. Свої погляди на суверенітет британський мислитель виклав у праці під назвою «Левіафан». Гоббс, який ототожнював суверенітет з державою, стверджував, що суверен має абсолютну, вищу, постійну та неподільну якість і що він не встановлює правил і зв'язаний цими правилами. Гоббс також підкреслював, що не може бути жодних обмежень або втручання в суверенітет, що випливає з інтересів підданих.109

Жан-Жак Руссо — мислитель, який розглядає суверенітет з демократичних позицій і вбачає в основі держави механізми прийняття народом рішень і обрання свого правителя. Свої погляди на народ і суверенітет женевський мислитель детально виклав у праці «Суспільний договір». На думку Руссо, існування держави залежить від її наділеності суверенітетом. Щоб існувала держава, повинна існувати абсолютна і суверенна влада, вільно обрана народом. Забезпечення цієї більшості, що називається загальною волею, означає, що суверенітет безумовно належить народу. У цьому відношенні суверенітет є невідчужуваним, нерепрезентативним, абсолютним і безпомилковим.110

Якості, пов’язані з проявом суверенітету, які є спільним знаменником усіх поглядів, можна підсумувати за такими заголовками:111

- Суверен повинен мати абсолютну владу у своєму суспільстві.

- Суверен повинен мати можливість діяти з абсолютною незалежністю.

- Суверен має бути особою міжнародного права з повною юридичною силою та владою.

Перші кроки щодо концепції суверенітету, яка набула значення в контексті міжнародного права, разом із дискусіями серед мислителів, з’явилися в результаті «Вестфальського миру» 1648 року. 112 Великі

руйнування сталися після Тридцятилітньої війни, яка почалася як релігійна боротьба між католиками та протестантами в Центральній Європі і тривала протягом тривалого часу. Врешті-решт мир було досягнуто завдяки Оснабрюкському та Мюнстерському договорам, підписаним у 1648 році, було закладено основу сучасної держави та встановлено новий міжнародний порядок, заснований на суверенній рівності держав. Багато подій щодо суверенітету було зафіксовано після Французької революції 1789 року та Першої та Другої світових воєн у 1900-х роках. Важливість суверенітету продовжує зростати з міжнародним співробітництвом і глобалізацією.113

Після народження сучасного міжнародного права різні вимоги різних держав, які впливатимуть на міжнародну спільноту, призвели до диференціації розуміння суверенітету. Кожна держава має суверенітет над своєю територією, а порушення територіального суверенітету суперечить міжнародному праву. У розумінні суверенітету в міжнародному праві прийнято, що держави авторитарні у своїх внутрішніх справах і рівні з іншими державами щодо суверенітету та незалежності у зовнішніх справах. Завдяки такому розмежуванню, яке називається внутрішнім суверенітетом і зовнішнім суверенітетом, держава не може втручатися у волю іншої держави та контролювати функціонування держави через авторитарні вимоги чи авторитарний тиск.114

Дискурс про суверенну рівність держав був висунутий у Вестфальський період, і з часом він отримав визнання в міжнародному праві та став одним із основних принципів. Наприкінці XVIII століття швейцарський філософ Еммеріх де Ваттель заявив, що всі держави є рівними в очах міжнародних прав, незалежно від того, великі вони чи малі, сильні чи слабкі. Зрештою, розуміння рівного суверенітету уможливило співіснування в міжнародній системі.115

Особливо після Віденського конгресу в 1815 році було проведено багато кодифікаційних досліджень на основі принципу суверенної рівності держав, і це було спрямовано на забезпечення міжнародного мирного середовища

різними правилами. Якщо спочатку державам з невеликою економікою та політичною вагою навіть не було можливості визначати свою долю, з часом з'явилися держави, які могли проголосити свою незалежність. Проблеми на практиці були подолані шляхом вивчення того, що сталося в історичному процесі. У цьому контексті Гаазькі конференції між 1899 і 1907 роками зайняли своє місце на сцені історії як поворотний пункт.116

На Гаазькій конференції, що відбулася 18 травня 1899 р., 26 держав зібралися разом і було домовлено, що всі держави, незалежно від їх розміру, повноважень і кількості делегатів, матимуть право одного голосу, а також були прийняті рішення з питань про порядку денного з дотриманням принципу рівності. Завдяки позитивній атмосфері першої конференції в 1907 році було проведено другу Гаазьку конференцію, на яку було надіслано запрошення 46 державам, у тому числі південноамериканським. Було вкотре наголошено, що кожен штат має рівні права голосу, і було домовлено, що всі важливі рішення будуть прийматися консенсусом. Однак така ситуація не відповідала сучасному світовому порядку, і деякі практики не могли бути втілені в життя. Щодо проекту щодо Постійної палати міжнародного правосуддя (USAD/PCIJ), то процес було відкладено через неспроможність держав досягти консенсусу щодо таких питань, як наявність суддів у суді та термін їх повноважень.117

Багато дебатів щодо суверенітету зросли та зберегли свою важливість на порядку денному після Першої світової війни. Зрештою, потреба створити платформу, де держави могли б рівноправно представляти себе, була гостро відчута, і була створена Ліга Націй. Принцип суверенної рівності не був чітко врегульований у Пакті Ліги Націй, але USAD, який планувалося створити в період Ліги Націй, було створено, і в судових рішеннях підкреслювалося, що суверенітет є фундаментальним принципом міжнародного права . 118 У цьому контексті такі рішення, як Bozkurt-Lotus119 і Wimbledon120, мають велике значення.

Пакт Бріана-Келлога121, який був підписаний за участю п’ятнадцяти держав 27 серпня 1928 року і набув чинності 25 липня 1929 року, закріпив принцип суверенної рівності держав і заборонив війну, щоб запобігти повторній світовій війні, але остаточної санкції не було передбачено. Хоча вважалося, що проблеми можна було б вирішити за допомогою Пакту, про який йдеться, відсутність будь-яких санкцій спростовувала цю можливість.122

Метою заснування Ліги Націй є організація сфер, які є ефективними в міжнародних відносинах, у спосіб, який буде вигідним для всіх держав, і забезпечити постійний міжнародний мир. З цієї причини, хоча просування на основі основних принципів здавалося доцільним з огляду на умови періоду, цього було недостатньо, і Ліга Націй була розпущена на своїй останній сесії 18 квітня 1946 року. Після Другої світової війни було створено Організацію Об’єднаних Націй (ООН) і прийнято нормативні акти для більш детального розгляду міжнародного права, і ці нормативні акти були підкріплені судовими рішеннями шляхом створення Міжнародного суду.123

У статті 2/1 Статуту Організації Об'єднаних Націй визнається суверенна рівність держав і втілюються основи концепцій невтручання у внутрішні справи та заборони втручання. 124 З цього приводу відповідне положення Статуту ООН містить речення «Організація заснована на принципі суверенної рівності всіх її членів».

У «Декларації про співпрацю та дружні відносини між державами»125 від 24.10.1970 р. під номером 2625(XXV), прийнятій Генеральною Асамблеєю ООН, принцип суверенної рівності держав було виражено детально126:

Усі держави користуються суверенною рівністю. Вони мають рівні права та обов’язки та є рівноправними членами міжнародного співтовариства, незалежно від своїх економічних, соціальних, політичних чи інших якісних відмінностей.

Суверенна рівність включає, зокрема, такі елементи:

(a) держави юридично рівні;

(b) кожна держава користується правами, притаманними повному суверенітету;

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

d) територіальна цілісність і політична незалежність держави є непорушними;

(e) кожна держава має право вільно обирати та розвивати власні політичні, соціальні, економічні та культурні системи;

(f) Кожна держава зобов'язана повністю і сумлінно виконувати свої міжнародні зобов'язання і жити в мирі з іншими державами.

У Рішенні щодо протоки Корфу127, одному з найбільш фундаментальних рішень щодо суверенітету, важливість суверенітету держав була підкреслена реченням: «Повага територіального суверенітету між незалежними державами є фундаментальною основою міжнародних відносин». 128

Фактична рівність між державами неможлива в нинішньому світовому порядку через різний розвиток і зміни. На забезпечення правової рівності функціонує принцип суверенної рівності держав. Отже, кожна держава, незалежно від її фактичної влади, може мати право голосу в міжнародному праві та мати права та обов’язки. 129 З усіх цих причин суверенітет і захист повноважень, що випливають із суверенітету, мають велике значення для міжнародного права.

Кіберпростір, на відміну від просторів, які регулюються певними нормами міжнародного права (земля, повітря, море та космос), є суперечливою та сучасною сферою, яка має різні наслідки в межах суверенітету. Постійні зміни в питаннях кібератак і захисту ускладнюють узгодження правил державами, а швидкість технологічного розвитку затримує процес кодифікації. 130 З цієї причини питання про те, як кіберпростір буде оцінюватися під егідою суверенітету, залишається актуальним і важливим.

Структура та унікальні характеристики кіберпростору, що виходить за рамки національних кордонів, можуть суперечити принципу суверенної рівності держав. Домінуюча позиція недержавних кіберакторів в інтернет-інфраструктурі та додатках спричиняє невизначеність у міжнародному правопорядку, оскільки може підірвати суверенітет держав у цій сфері. 131 Відповідно до заяв у рамках «Звіту про події в галузі інформації та телекомунікації в контексті міжнародної безпеки», підготовленого в 2013 році та оновленого в 2015 році Міжнародною групою експертів, яка проводить дослідження на цю тему до Генеральної Асамблеї ООН, очевидно, що основні норми міжнародного права будуть застосовуватися в кіберпросторі. Пояснення у Звіті, який також наголошує на суверенітеті та пов’язаних із суверенітетом нормах, є такими:132

Міжнародне право, і зокрема Статут Організації Об’єднаних Націй, є дійсним і необхідним для сприяння відкритому, безпечному, мирному, доступному середовищу інформаційних і комунікаційних технологій і підтримці миру і стабільності.

Державний суверенітет і міжнародні норми та принципи, які випливають із суверенітету, застосовуються до здійснення державою діяльності, пов’язаної з інформаційно-комунікаційними технологіями, та її юрисдикції над інфраструктурою на своїй території.

При використанні інформаційних і комунікаційних технологій держави повинні дотримуватися, серед інших принципів міжнародного права, таких питань, як державний суверенітет, суверенна рівність, мирне вирішення суперечок і невтручання у внутрішні справи інших держав. Існуючі зобов'язання за міжнародним правом також застосовуються до використання державою інформаційно-комунікаційних технологій. Держави повинні виконувати свої зобов’язання згідно з міжнародним правом щодо поваги та захисту прав людини та основних свобод.

Відповідно до Звіту, який не має обов’язкової сили, а є міждержавною угодою, запобігти загрозі технологічного розвитку міжнародному правопорядку було визнано можливим через міжнародний правопорядок.

Питання суверенітету більш детально розглядається в правилах 1-5 Талліннського керівництва. Для цілей посібника пояснюється, що рівні кіберпростору розглядаються в рамках принципу суверенітету. Відповідно, кібердіяльність може здійснюватися різними особами та організаціями через різні об’єкти в межах територіальних кордонів держав, у місцях, де вони можуть здійснювати повноваження, пов’язані з суверенітетом. Навіть якщо кібердіяльність перетинає більше ніж один кордон і відбувається в міжнародних водах, міжнародному повітряному просторі чи космосі, одна або кілька держав можуть здійснювати юрисдикцію. Той факт, що інфраструктура, яка забезпечує доступ до кіберпростору, розташована на суші, у повітрі чи на морі держави, не може тлумачитися як відмова від суверенітету даної держави. У цьому контексті держави також мають право накладати обмеження на кіберінфраструктуру та Інтернет відповідно до міжнародного права.133

Відповідно до Талліннського посібника, держави можуть здійснювати кібердіяльність у своїх міжнародних відносинах за умови, що вони дотримуються норм міжнародного права, які їх зобов’язують. Згідно зі статтею 2/1 Статуту ООН, держави є юридично суверенними та рівноправними. У контексті зовнішнього суверенітету держави здійснення кібердіяльності нарівні з іншими державами не є порушенням міжнародного права. Однак у зв'язку з цим особливу увагу слід звернути на заборони втручання та застосування сили, що призвело б до порушення суверенітету інших держав. Держава не повинна порушувати суверенітет іншої держави та повинна уникати кібер-дій у цій сфері. 134 Зрештою, можна сказати, що шпигунські дії держави в розвідувальних цілях у кіберсередовищі самі по собі не загрожуватимуть миру та безпеці в міжнародному співтоваристві, доки вони не завдають шкоди та не порушують суверенітет інших держав.

По суті, суверенітет у кіберпросторі є загальною концепцією, яка вступає в дію, коли кібер-дія відбувається до такого ступеня, що правила щодо втручання у внутрішні справи, втручання та застосування сили не можуть бути застосовані. У цьому контексті більш м’які кібер-дії, які порушують суверенітет держав, можуть вважатися деліктами в міжнародному праві.135

2.2.Принцип заборони втручання у внутрішні справи держави

Паралельно з розвитком міжнародного права щодо суверенітету відбулися різноманітні зміни в таких питаннях, як право держав на самовизначення, втручання у внутрішні справи та заборона втручання. На Гаазькій конференції, що відбулася в 1907 році, і в Пакті Бріана-Келлога було підкреслено, що акти війни і втручання є ворожими, але повністю превентивне регулювання не може бути зроблено. По суті, ефективний розвиток у цьому відношенні відбувся зі створенням ООН.136

Найбільш конкретним відображенням принципу суверенної рівності держав у міжнародному праві є принцип невтручання у внутрішні справи. Згідно зі статтею 2/7 Статуту ООН Організацією ООН прийнято принцип невтручання у внутрішні справи держав. Відповідно, як правило, Організація ООН не може втручатися у внутрішні справи держави, а держави-члени не можуть нести відповідальність за внутрішні справи іншої держави. Специфічним аспектом принципу невтручання у внутрішні справи є заборона втручання. Насправді, коли відбувається втручання у внутрішні справи держав, природним наслідком є порушення суверенітету та пов’язаних із суверенітетом прав відповідної держави. З цього приводу відповідне положення Статуту ООН викладено так:

Ніщо в цьому Договорі не дозволяє Організації Об'єднаних Націй втручатися в справи, які невід'ємно входять до національної юрисдикції держави, і не зобов'язує своїх членів передавати такі питання на процедуру

врегулювання відповідно до цього Договору, а також не дозволяє застосовувати примусових заходів, викладених у розділі VII.

У Декларації про співробітництво і дружні відносини між державами визнавався звичайний характер принципу невтручання і заборони втручання у внутрішні справи і підкреслювалася його обов'язковість для всіх держав. Крім того, зміст розглянутого принципу та заборони підсумовано таким чином:137

Жодна держава чи група держав не має права прямо чи опосередковано втручатися у внутрішні чи зовнішні справи з будь-яких причин. З цієї причини збройне чи будь-яке інше втручання або спроба загрози особистості держави або її політичним, економічним і культурним елементам суперечить міжнародному праву.

Території, де можуть відбуватися дії, які вважаються внутрішніми справами держав, називають національною юрисдикцією (заповідна зона, domaine rêservê). Національна юрисдикція відноситься до верхнього поняття з кордонами, включаючи сухопутні, повітряні та морські райони, на яких можуть здійснюватися міжнародні права та зобов’язання держав. Міжнародне співтовариство не має ні права, ні обов’язку втручатися проти дій, які відбуваються в межах національної юрисдикції.

Одним із важливих прикладів принципу невтручання у внутрішні справи та заборони втручання, з якими ми стикаємося на практиці, є Рішення у справі Нікарагуа, винесене Міжнародним Судом ООН у 1986 році. 138 У рішенні, про яке йдеться, було наголошено, що принцип невтручання у внутрішні справи та заборона втручання є частиною звичаєвого права, і було зазначено два основні елементи разом із змістом відповідного принципу та заборони. У цьому контексті застосування іншою державою методів примусу в питаннях, що випливають із суверенітету держави і в яких вона має право вільно вирішувати, порушує відповідні принципи та заборони. Питання, щодо яких держави можуть вільно вирішувати, виражаються у виборі політичних, економічних, соціальних і культурних систем і формулюванні

зовнішньої політики. 139 Держави, як правило, не можуть вчиняти жодних дій на території іншої держави. Однак межі принципу заборони втручання і невтручання у внутрішні справи держав можуть змінюватися, і згода держав може зробити дії в цій сфері законними. Тривають дискусії щодо дій, які вважаються міжнародними через їх характер, у рамках таких понять, як права людини, гуманітарне втручання та відповідальність за захист суспільства.140

Іншими важливими Резолюціями Генеральної Асамблеї ООН, які містять концепції принципу невтручання у внутрішні справи та заборони втручання, є «Рішення про відмову від втручання у внутрішні справи держав і захист їх незалежності та суверенітету» від 21.12.1965 р. і під номерами 2131(XX),141 і 36/103 від 9.12.1981 р. «Декларація про неприпустимість втручання та будь-яких видів втручання у внутрішні справи держав»142. Проте дискусії щодо принципу невтручання у внутрішні справи та заборони втручання ще можуть виникати паралельно з розвитком та змінами міжнародного права. Одним із важливих прикладів у цьому відношенні є кіберпростір.

Кібер-дії, які збільшують можливість дистанційного втручання у суверенітет держав, можуть проявлятися таким чином, що може порушувати принцип невтручання у внутрішні справи. Ця ситуація не розглядається як одне з питань, у яких держави можуть дозволити втручання іншої держави в рамках звичайного життя. Таким чином, у кіберпросторі, який робить концепцію національної юрисдикції відкритою для дискусії, виникає необхідність розвитку нової перспективи.

У Талліннському путівнику детально роз’яснено правила № 66 і 67, а також принцип невтручання у внутрішні справи та заборону втручання. Кіберпростір – це сфера, де втручання у внутрішні чи зовнішні справи стало легшим через глобалізацію та зростаючу залежність від інформаційних технологій. Однак заборона втручання та втручання у внутрішні справи, заснована на принципі суверенної рівності держав у міжнародному праві, є традиційною міжнародною нормою, яка також включає кіберпростір. Крім

того, держави, ООН, Міжнародний суд і багато міжнародних організацій також визнають звичаєвий статус даної норми. У цьому контексті держави не можуть втручатися у внутрішні чи зовнішні справи, у тому числі за допомогою кіберзасобів.143

У рамках Талліннського посібника приклад заміни електронних бюлетенів кібератаками та маніпулювання виборами наводиться як один із випадків, коли держава може втрутитися в іншу державу в контексті кіберпростору. Крім того, заборонено вдаватися до таких методів, як зміна внутрішнього законодавства держав щодо Інтернету, направлення їх на роззброєння в кіберпросторі та втручання в рішення щодо приєднання до міжнародних угод.144

Заборони, зазначені в Посібнику, діють лише у міждержавних відносинах. Це не стосується інших кіберакторів, які беруть участь у ворожих кібердіях проти держави. Проте, якщо дії недержавних кіберакторів можна приписати будь-якій державі, заборона на втручання буде порушена і виникне міжнародна відповідальність відповідної держави. Однак у міжнародних відносинах, які постійно розвиваються та все більше переплітаються з точки зору кіберпростору, важко провести чіткі межі щодо того, як буде реалізовуватися заборона на втручання та втручання у внутрішні справи. У цьому контексті оцінку слід проводити в рамках питань, які держава може вирішувати вільно, та втручання іншої держави за допомогою примусових методів.145

Згідно з Талліннським посібником, внутрішні справи держав виводяться в рамках концепції національної юрисдикції, яка по суті складається з питань, неврегульованих міжнародним правом. Коротко кажучи, питання, не врегульовані міжнародним правом, розглядаються в межах національної юрисдикції держав і захищені від втручання інших держав. Питання, які можуть входити до національної юрисдикції держави, можуть змінюватися з часом. Яке питання буде прийнято в кластері національної юрисдикції, залежить від практики та юридичних думок

держав. Як зазначено в Рішенні щодо Нікарагуа, примусові методи, спрямовані на обмеження або усунення повноважень держав у питаннях, що ґрунтуються на їхньому суверенітеті, порушують заборону втручання. Кібернетичні дії такого характеру також порушуватимуть принцип невтручання у внутрішні справи та заборону втручання. По суті, порушення, про яке йдеться, значною мірою знаходиться на тому ж рівні, що й інші питання, що належать до монополії держав.146

Талліннський путівник детально описав тему з різними прикладами для кращого розуміння порогу щодо національної юрисдикції, втручання у внутрішні справи, втручання та методів примусу в кіберпросторі. Наприклад, у державі А шляхом референдуму планується перехід від двох офіційних мов, якими користуються етнічні групи більшості та етнічних меншин, до однієї офіційної мови, якою користується більшість. Держава В, яка має спільні коріння з етнічною меншиною, здійснила атаки на важливі урядові веб-сайти, щоб стримати державу А, і вжила заходів для підтримки веб-сайтів обома мовами. У цьому прикладі втручання в мовну політику держави А через кіберпростір містить елементи питань, щодо яких держави можуть вільно вирішувати, і примусових методів, і є порушенням заборони втручання.147

В іншому прикладі розглядається держава Y, яка здійснює деструктивну кібердіяльність проти комерційних банків держави X. Держава Y під тиском, який вона чинила на державу X, вимагала видалення онлайн-контенту, який вона вважала образливим, на приватних веб-сайтах, пов’язаних з інфраструктурою держави X. Норми держав щодо онлайн-контенту підпадають під сферу національної юрисдикції, якщо вони не суперечать їхнім міжнародним зобов’язанням, і така кібер-діяльність також вважається такою, що суперечить забороні втручання.148

У міжнародній правовій системі держави можуть відмовитися від розгляду проблеми як національної юрисдикції через двосторонні або багатосторонні міжнародні угоди. Це також стосуватиметься будь-яких міжнародних угод щодо кібердіяльності. Однак не слід забувати, що ця

практика не буде дійсна для держав, які не є сторонами відповідної міжнародної угоди, і продовжуватимуть захищати свою національну юрисдикцію проти інших держав. 149 Зрештою, питання та методи примусу, щодо яких держави вирішуватимуть вільно, є відносними. Той факт, що кіберзагрози впливають на національну юрисдикцію, є достатнім для втручання держав у їх внутрішнє функціонування.150 Кожен спір із цих питань має оцінюватися відповідно до конкретних подій та умов.

Останнім питанням, яке регулює Талліннське керівництво щодо принципу невтручання у внутрішні справи та заборони втручання, є позиція Організації ООН у кібердіяльності. Відповідно, як і в статті 2/7 Статуту ООН, по суті визнається, що Організація ООН не повинна втручатися у справи, які підпадають під внутрішню юрисдикцію держав, включаючи кіберзасоби, як у статті VII Статуту ООН. Заходи, які можуть бути вжиті в рамках цього розділу, зарезервовані. Однак питання, що входять до сфери цілей Організації ООН, зазначених у статті 1 Статуту ООН, і зокрема питання, що стосуються міжнародного миру та безпеки, виключаються з цього правила. 152 Підводячи підсумок, можна сказати, що в межах своїх цілей Організація може втручатися в кібернетичні дії, які можуть загрожувати міжнародному миру та безпеці.

Відповідно до Керівництва, враховуючи взаємопов’язаний характер кіберінфраструктури та дій, зрозуміло, що кібердіяльність, яка здійснюється в одній державі, впливатиме на інші держави. Коли цей факт розглядається з точки зору міжнародного миру та безпеки, така діяльність стає чутливою до нагляду та контролю з боку Організації ООН. Насправді кібердіяльність має базову структуру, яка може впливати на економічні, соціальні, культурні та гуманітарні проблеми на міжнародній арені. В ООН можна запобігти більшим суперечкам, втручаючись у місцеві ситуації.153

Організація ООН не має права втручатися в питання, в яких держави мають суверенну владу, незалежно від того, чи використовуються примусові методи чи ні. Наприклад, вимога Організації ООН щодо прийняття

спеціального законодавства щодо кібердіяльності, яка здійснюється державами на їхній власній території та в суто локальних цілях, порушує принцип невтручання у внутрішні справи та заборону втручання. Однак не слід забувати, що з метою підтримки міжнародного миру та безпеки втручання в національну юрисдикцію держав може здійснюватися за рішенням, прийнятим Радою Безпеки ООН, у рамках Розділу VII Статуту ООН.154

Природа кібератак породжує нові інтерпретації, змішані з традиційними правилами. Зрештою, можна легко сказати, що політика та методи, яких дотримуються держави в цій сфері, мають бути спрямовані на дотримання міжнародного права. Інакше буде важко досягти консенсусу щодо складної структури кіберпростору, а різні програми можуть спричинити проблеми.

2.3.Принцип заборони застосування сили та право на самозахист

У міжнародному праві основні принципи права на застосування сили (jus ad bellum) і колізійні норми, яких необхідно дотримуватися при застосуванні сили (jus in bello), відрізняються там, де застосовуються різні правові норми. По суті, хоча наявність права на застосування сили не впливає на застосування норм колізійного права, необхідно почати з короткого торкання цієї відмінності в контексті нашої теми та зазначити, що зміст нашого дослідження буде продовжуватися конкретно в jus ad bellum.

Jus ad bellum стверджує, що держави повинні мати законні підстави для початку війни. Законні причини, як правило, базуються на етичних, правових і доказових підставах, таких як оборона, національна безпека та захист міжнародного миру. Для того, щоб визначити, чи дії були вчинені розумно і правомірно, необхідно провести оцінку конкретних подій. Jus in bello стосується принципів, яких слід дотримуватися після початку війни. По суті,

очікується, що військові дії, які відбуватимуться під час війни, будуть пропорційними, гуманними та захищатимуть цивільне населення.155

Застосування сили було проблемою для держав, де б не було людини. До моменту створення ООН і впровадження Статуту ООН застосування сили розглядалося як право держав за певних умов. «Справедлива війна» була прийнята як одна з найважливіших умов законного застосування сили.156

Справедлива війна вперше з'явилася в той період, коли християни вважали гріхом воювати і вбивати людей. Аврелій Августин, один із відомих мислителів того періоду, висловив цю концепцію в систематичний спосіб і зробив її застосовною. Після того, як християнство було прийнято Римською імперією та прийнято як імперська релігія, була встановлена система, за якої держави могли застосовувати силу лише для встановлення миру, беручи до уваги критерії того, що війна базувалася на справедливій причині, була благими намірами, і була оголошена легітимною владою.157

Концепція справедливої війни, яка трансформувалася та продовжила свою ефективність під час переходу від періоду природного права до сучасного періоду, використовувалася до 20-го століття, а застосування сили та самооборони розглядалися як природне право, надане суверенітетом , і з цієї причини різні війни відбувалися між державами в кожному столітті. Через неадекватність м'яких положень Ліги Націй, що обмежують повноваження щодо війни, почалася Перша світова війна, яка мала руйнівні наслідки для всіх держав. У зв’язку з цим було зрозуміло, що застосування сили державами не може розглядатися як право, і кодифікаційні дослідження почалися з Пакту Бріана-Келлога щодо заборони застосування сили в міжнародному праві, держави засуджували війни та було прийнято зобов’язання вирішувати суперечки мирним шляхом і не вдаватися до війни. 158 Перші дві статті Пакту були написані так:159

1. Високі Договірні Сторони офіційно заявляють від імені своїх націй, що вони відкидають і засуджують використання війни для вирішення

міжнародних суперечок і що вони перестали розглядати війну як інструмент національної політики у своїх відносинах одна з одною.

2. Високі Договірні Сторони погоджуються з тим, що всі суперечки або розбіжності, які можуть виникнути між ними, незалежно від їх характеру та джерела, за жодних обставин не будуть намагатися вирішити чи врегулювати інакше, ніж мирними засобами.

Остаточні та чіткі правила щодо застосування сили були прийняті з початком ери ООН. Виходячи з принципу суверенної рівності держав, застосування сили або загроза застосування сили заборонено відповідно до статті 2/4 Статуту ООН, і ця заборона зайняла своє місце в літературі як конкретне міжнародно-правове правило. Положення, про яке йдеться, було викладено так:

Члени Організації повинні утримуватися від застосування сили або погрози силою у своїх міжнародних відносинах проти територіальної цілісності чи політичної незалежності будь-якої іншої держави або будь-яким іншим способом, несумісним з цілями Організації Об'єднаних Націй.

Заборона застосування сили розвинулася з норм міжнародного звичаєвого права і стала обов'язковою нормою, і в цьому контексті вона стала обов'язковою для всіх держав. 160 Статут ООН зайняв своє місце на сцені історії як перший договір, який забороняв застосування сили як фундаментальну глобальну норму міжнародного права. 161 Як бачимо, одним із найважливіших зобов'язань, які зазначений договір покладає на держави-члени Організації ООН, є утримання від застосування сили та використання сили як загрози з метою забезпечення міжнародного миру та безпеки.

Слід зазначити, що положення статті 2/4 Статуту ООН забороняє лише акти застосування сили, вчинені державами або приписані державам. По суті, у випадках повстання, заворушення чи громадянської війни на території держави неможливо вважати, що це стосується заборони застосування сили, якщо не буде доведено конкретними та вагомими доказами вплив іншої

держави. 162 Визначення дій, які підпадають під дію заборони, та приписування їх державі має велике значення з точки зору можливості законної відповіді на атаки, про які йдеться.163

Існують різні дискусії про те, що заборонені Статутом ООН акти застосування сили включають не лише застосування збройної та військової сили, а й методи економічного та політичного тиску, які слід оцінювати в рамках цього положення. Очевидно, що положення забороняє використання збройної сили. 164 У цьому контексті важливо вивчити конкретний інцидент і оцінити, в чому поточна дія перевищує поріг застосування сили.

Із заборони застосування сили є два винятки. Ці винятки становлять заходи «самооборони», регламентовані Статутом ООН, і заходи «легітимного втручання», яких має вжити Рада Безпеки ООН у разі загрози або порушення міжнародного миру в рамках Розділу VII Статуту. Положення статті 51 Статуту ООН щодо самооборони таке:

Ніщо в цьому Статуті не завдає шкоди невід'ємному праву на індивідуальну або колективну самооборону, якщо член Організації Об'єднаних Націй є об'єктом збройного нападу, доки Рада Безпеки не вживе таких заходів, які необхідні для підтримки міжнародного миру та безпеки. Про дії, вжиті членами для здійснення цього права на самозахист, необхідно негайно повідомляти Раду Безпеки, і вони жодним чином не впливають на повноваження та обов’язки Ради Безпеки діяти в будь-який час, як це може вважатися необхідним для підтримки або відновлення міжнародного миру та безпеки відповідно до цього Статуту.

Хоча самозахист розглядається як природне право держав у межах сфери застосування цього положення, існують також деякі критерії, прийняті в міжнародному звичаєвому праві щодо здійснення цього права. Критерії, про які йдеться, виражені як наявність збройного нападу, терміновість, необхідність, пропорційність та повідомлення про вжиті заходи Раді Безпеки ООН.165 Повідомлення Раді Безпеки не є істотною умовою. Це пояснюється як процедура в статті 51 Статуту ООН і приймається як процедурна умова.

Невиконання умови не скасовує існування права на необхідний захист. По суті, суть права на самозахист також базується на міжнародному звичаєвому праві та суверенітеті держав. Тому, на відміну від винятків щодо примусових військових заходів у Розділі VII Статуту ООН, відповідна держава не підлягає санкціонуванню Ради Безпеки. Однак було б доцільніше негайно повідомити Раду про заходи, вжиті державами в цьому контексті. Якщо Рада Безпеки втручається і приймає рішення після повідомлення, право на самозахист припиняється.166

Якщо коротко торкнутися умов пропорційності, необхідності та терміновості, то слід сказати, що для конкретного випадку важливо оцінити характер ситуації, яка породжує заходи самооборони. Немає чіткого визначення для цих умов, прийнятих державами, які пережили Каролінський інцидент. Конкретизувати умови допомагають заяви, зроблені в рамках поглядів Вебстера, тодішнього держсекретаря США. Основним елементом умови пропорційності є те, що втручання здійснюється в тій мірі, в якій поточна атака усунена. В умовах необхідності та терміновості загроза набула такого розміру, що є раптовою, непереборною та не може бути усунена іншим способом, і останнім засобом для захисту держави є самооборона.167

Тягар надання доказів дотримання умови збройного нападу належить державі, яка бажає скористатися своїм правом на самозахист. Невиконання тягаря подання доказів, яке також наголошується в Рішенні щодо Нікарагуа, також впливає на умову необхідності та втрачає основу для здійснення права на самозахист відповідно до міжнародного права. 168. Самозахист, спрямований на відбиття нападу, не повинен перетворюватися на дії, що перевищують цю мету, або не повинен мати на меті покарання.

Хоча у змісті Статуту ООН немає концептуального визначення збройного нападу, який є найважливішою умовою права на самозахист, було проведено багато міжнародних досліджень і розроблено судову практику з рішеннями Міжнародного суду. Тут ми натрапляємо на «Рішення про визначення нападу» від 14.12.1974 р. під номером 3314(XXIX)169 та

положення ст.3, в якому дії, які можна вважати нападами, зараховуються до зразкових відповідно до ст. 4. У той же час відповідне положення, що пояснює акти агресії, які слід розглядати в рамках заборони в статті 2/4 Статуту ООН, викладено так:

Будь-які з наступних актів, незважаючи на оголошення війни, вважаються актом агресії з урахуванням і відповідно до положень статті 2:

(a) вторгнення або напад збройних сил держави на іншу державу та будь-яка військова окупація або анексія території цієї держави або її частини із застосуванням сили в результаті такого вторгнення або нападу, незважаючи на тимчасовий характер;

b) збройні сили держави бомблять територію іншої держави або застосовують будь-яку зброю проти території іншої держави;

c) блокада портів або узбережжя однієї держави збройними силами іншої держави;

d) збройні сили однієї держави атакують сухопутні, військово-морські чи повітряні сили або військово-морський чи повітряний флот іншої держави;

e) використання збройних сил держави проти держави, яка прийняла їх на свою територію за договором, всупереч умовам, зазначеним у договорі, або їх продовження присутності в країні після закінчення терміну дії договору;

(f) держава передає свою територію іншій державі та дозволяє цій іншій державі використовувати територію для здійснення актів агресії проти третьої держави;

(g) Направлення державою або від її імені озброєної банди, групи, нерегулярного підрозділу чи найманців для вчинення вищезазначених дій проти іншої держави або суттєва участь у таких діях.

Рішення щодо Нікарагуа 1986 року є першим прецедентним рішенням Міжнародного суду, яке містить детальні пояснення щодо застосування сили, самооборони та понять, що входять до них. Визначення в Рішенні у справі

Нікарагуа, яке робило різні оцінки для того, щоб вважати акт застосування сили збройним нападом, є таким:170

- Збройний напад має вужче значення, ніж застосування сили та погроза застосування сили, регламентоване статтею 2/4 Статуту ООН.

- Держави, які застосовують силу або погрожують застосувати силу, суперечать статті 2/4 Статуту ООН, але для того, щоб дія кваліфікувалася як збройний напад, вона повинна бути «масштабною, інтенсивною та мати серйозний ефект». Можлива одиночна або колективна атака.

- Транскордонні переміщення, які можна вважати незначними з точки зору їх інтенсивності та наслідків і які не здійснюються державами, можуть розглядатися лише як «прикордонні інциденти», а не як збройні напади. У цьому випадку держави можуть вдатися до контрзаходів, які не передбачають застосування сили, навіть якщо вони не можуть скористатися своїм правом на самозахист.

У Рішенні щодо Нікарагуа було зроблено посилання на визначення рішення про напад, а пояснення, що відображають звичаєве право, були зроблені в рамках статті 3/g у визначенні рішення про напад. У цьому контексті було зазначено, що право на самозахист може виникнути, якщо збройний напад виходить за межі невеликих прикордонних інцидентів і перетворюється на регулярні сили, які загрожують державі, і вказується на відмінність між прямим і непрямим збройним нападом: 171

- Для того, щоб дія вважалася прямим збройним нападом, виконавцем має бути «держава».

- Держави можуть здійснювати збройні напади опосередковано, використовуючи нерегулярні сили, які не пов'язані з ними безпосередньо. Для того, щоб дія була в межах непрямого збройного нападу, має бути встановлено, що відповідна держава бере істотну участь у діях, і конкретний інцидент має бути оцінений, а дія повинна бути приписана державі. Якщо обвинувачення неможливе, твердження про те, що потерпіла держава

використовує своє право на самозахист, може стати суперечливим, незалежно від інтенсивності дії.

Паралельно з рішенням щодо Нікарагуа Міжнародний суд також пояснив умови права на самозахист у своєму рішенні щодо «Збройної діяльності в Демократичній Республіці Конго». Водночас він підкреслив, що заборона застосування сили є одним із наріжних каменів Статуту ООН, і заявив, що право на самозахист може вважатися дійсним у міжнародному праві, якщо воно використовується обмежено положенням статті 51 Статуту ООН.172

Після висновків Міжнародного суду в Рішенні щодо Нікарагуа таблиця, створена Джеймсом Гріном, класифікуюча порогові значення втручання, застосування сили та збройного нападу, прийняті Судом, є важливою в ході нашого дослідження. Таким чином, відображення існуючих правил на практиці та те, як держави діятимуть у цьому випадку, стане конкретним. Насамкінець коротко торкнемося використання примусових і непримусових засобів протидії в діях, які не перевищують поріг збройного нападу.

У міжнародному праві є два типи контрзаходів, доступних державам, які не є винятком самооборони. Ці заходи називаються «нанесення збитків та дипломатичні заходи». Нанесення збитків – це коли держава бере участь у ворожих і завдаючих шкоди діях проти іншої держави, використовуючи незаконні засоби, а держава, яка піддається цій ситуації, відповідає протиправними діями. Основними прикладами таких заходів є ембарго, мирна блокада та бойкот. Дипломатичні наслідки, на відміну від нанесення збитків, є методом вираження невдоволення законним і легітимним способом. Прикладами таких заходів є розрив дипломатичних відносин, депортація іноземців або обмеження їхніх прав, економічні обмеження або обмеження на подорожі.173 Дипломатичні заходи можна застосовувати проти дій, які не перевищують межі збройного нападу, але завдають шкоди інтересам держав. Крім того, якщо виникає ситуація, яка порушує права держав, на перший план можуть вийти як відшкодування збитків, так і методи помсти. Таким

чином зміцнюються кроки до підтримки міжнародного миру та безпеки, а проблеми та суперечки вирішуються до того, як війна виходить на перший план.

Іншими важливими положеннями щодо визначення межі між військовим і невоєнним застосуванням сили є спільні статті 2 і 3 Женевських конвенцій 1949 року174. Ці положення, які відображають зусилля щодо регулювання правил, яких має дотримуватися міжнародне співтовариство, забезпечують гуманне поводження. Основні принципи міжнародного гуманітарного права виражаються як дискримінація, пропорційність, належна обачність, військова необхідність і відсутність непотрібних страждань.175 Проте від воюючих сторін вимагається діяти відповідно до певних критеріїв у рамках принципу пропорційності. Ці критерії можна виразити як достатню мету, інтенсивність і тривалість.176 Таким чином, законність застосування сили та безперервність війни обмежені, увага зосереджена на оборонних цілях і запобігає надмірному застосуванню сили.

З якого моменту збройний напад можна вважати збройним конфліктом і застосовуватимуться норми колізійного права, слід оцінювати з урахуванням відображення зазначених критеріїв у конкретній ситуації. Слід зазначити, що застосування надмірної сили суперечить міжнародному гуманітарному праву та може поставити на порядок денний військові злочини.

Оскільки в міжнародному праві немає спеціального регулювання щодо кіберпростору та кібератак, існують різні дискусії щодо того, як застосовуватимуться існуючі правила. З цієї причини також необхідно переглянути основні принципи та правила щодо заборони застосування сили та самозахисту. Незважаючи на те, що Талліннський путівник не є обов’язковим, він все ще зберігає свою відмінність як єдина міжнародна робота, яка детально пояснює це питання та дає вказівки державам.

У правилах № 68-75 Посібника кібератаки розглядаються в рамках заборони застосування сили та самозахисту. Відповідно, кібератаки, які становлять загрозу територіальній цілісності чи політичній незалежності

будь-якої держави, рівнозначні застосуванню сили або несумісні з цілями ООН, вважаються протиправними. Однак було також наголошено, що дії, які не порушують заборону на застосування сили, можуть порушувати основні положення щодо суверенітету, втручання та втручання у внутрішні справи.177

Згідно з Правилом № 69 Талліннського керівництва, яке також посилається на висновки Рішення щодо Нікарагуа, кібератака означає застосування сили, якщо вона «порівняна з іншою некібератакою, яку можна інтерпретувати як застосування сили» з точки зору масштабу інтенсивності та ефектів». У зв'язку з цим було зазначено, що психологічна кібердіяльність, яка здійснюється з метою підриву довіри громадян держави до уряду та не завдає фізичної шкоди, не порушуватиме заборону застосування сили. В іншому прикладі було зазначено, що ця дія держави, яка лише надавала фінансову підтримку комп'ютерним активістам, які здійснювали кібердіяльність у рамках повстанців, не є порушенням заборони на застосування сили.178

Згідно з довідником, застосування сили не обов'язково має здійснюватися із застосуванням військових чи інших збройних сил. З цієї причини держави, які забезпечують необхідне навчання та забезпечують шкідливе програмне забезпечення для організованої озброєної групи для здійснення кібердіяльності, слід вважати такими, що застосували силу та порушили заборону. Однак не слід забувати, що міжнародна відповідальність виникне, коли це питання буде покладено на відповідну державу.179

Талліннське керівництво передбачає певні критерії, які слід використовувати в рамках заборони на застосування сили щодо кібератак. 180 Відповідні критерії можна підсумувати таким чином:181

- Серйозність: значний вплив за обсягом, тривалістю, інтенсивністю та результатами.

- Терміновість: тривалість шкідливого впливу, який буде відчутний і зменшиться, викликає тривогу.

- Безпосередність: існує прямий і тісний зв'язок між проблемами, які викликають дію, і результатом.

- Вторгнення: прагнення проникнути в кібермережу в цільовій країні.

- Вимірність: поява конкретних подій, які можна виміряти та визначити.

- Військовий характер: проведення дій за допомогою військових або збройних організованих сил.

- Участь держави: існує тісний і чіткий зв'язок між державою та кібернетичними діями, що відбуваються.

- Можлива легітимність: вчинені дії належать до категорії застосування сили з її інструментами та якостями.

Одним із найважливіших питань і проблем, які виникають після оцінки кібератаки в рамках застосування сили, є характер кібератак як збройних нападів і паралельне право на самозахист. У зв’язку з цим важливо визначити характер кібератаки чи атак у конкретному випадку та умови самозахисту. На цьому етапі необхідно провести оцінку за дуже чутливою шкалою, беручи до уваги необхідність підтримки міжнародного миру та безпеки.

У Рішенні щодо Нікарагуа збройний напад оцінювався на основі шкали інтенсивності та критеріїв впливу. У Талліннському посібнику пояснюється природа кібератак як збройних нападів, знову посилаючись на відповідне рішення. Відповідно, держава, яка є об’єктом кіберактивності, що досягає рівня кібератаки, може скористатися невід’ємним правом на самозахист. Розмір збройної атаки кіберактивності залежить від масштабу інтенсивності та тяжкості її наслідків.182

Згідно з Посібником, право на застосування сили в контексті самозахисту охоплює напади, здійснені з використанням засобів і методів у кіберпросторі, а також кінетичні атаки в зовнішньому світі. Насправді деякі кіберактивності можуть бути такими за розміром і серйозністю, що можна класифікувати як збройний напад. Відповідно до «Консультативного висновку МКС щодо законності загрози або застосування ядерної зброї» від 08.07.1996 р.183 вибір засобів нападу не має значення при визначенні

характеру збройного нападу. Така ситуація зустрічається і в практиці держав, і загальновизнано, що спрацьовує право на самозахист. Незалежно від використовуваного інструменту та методу можуть виникнути наслідки, пов’язані з серйозними стражданнями або смертю. Можна легко сказати, що таке міркування також буде справедливим для кіберактивності.184

Іншим фундаментальним елементом збройних нападів є їх транскордонний характер. Транскордонні дії під час кібератак розглядаються як дії, що здійснюються державою проти іншої держави або коли держави керують зовнішніми акторами від свого імені. Однак існують дискусії про те, що недержавні суб’єкти здійснюють транскордонну дію самостійно, і про право на самозахист, яке виникає з цієї причини. Більшість Міжнародної експертної групи, яка підготувала Посібник, визнає, що право на самозахист виникне проти кібератак, здійснених терористичними чи повстанськими групами та, зрештою, недержавними суб’єктами, посилаючись на «атаки 11 вересня»185. як приклад. Невизначеність і дебати щодо організаційного виміру недержавних акторів, географічних обмежень та індивідуальних дій під час кібератак все ще тривають.186

Відповідно до Керівництва, здійснення права на необхідний захист залежить від наявності умов необхідності, пропорційності, негайності та терміновості. Безсумнівно, обґрунтоване визначення того, що збройний напад стався або має відбутися, є основною основою самозахисту. У кібератаках, паралельно з традиційними збройними атаками, наявність збройної атаки має визначатися такими критеріями, як масштаб шкоди, завданої дією, характер і стан пошкодженої цілі та наявність політичних факторів. Напади на державні установи, організації, об'єкти, техніку та персонал визнаються збройними нападами за наявності інших умов і права на необхідну оборону. Характеристики конкретної справи є важливими для визначення всіх відповідних питань.187

Необхідність самозахисту при кібератаках дійсна у випадках, коли примусових або непримусових заходів протидії недостатньо. У випадках,

коли альтернативні варіанти не працюють, можна віддати перевагу пропорційному застосуванню сили. Вимога пропорційності обмежує масштаб, обсяг, тривалість та інтенсивність оборонних заходів. Оборонні заходи не обов'язково мають бути такого ж характеру, як напад. Тому на традиційні збройні атаки можна відповісти кібератакою або вжити інших заходів обережності. Успішний захист на рівні, який відбиває поточну атаку, буде еквівалентом принципу пропорційності.188

В умовах негайності та терміновості виражаються ситуації, в яких сталася кібератака або її настання є певним і не можна запобігти. Підготовчі заходи або вороже ставлення до кібератак не вимагають самозахисту. Коли напад стає неминучим і незворотним, вдаються до самозахисту. Якщо кібератака залишається непоміченою та не може бути виявлена, слід очікувати, що відбудеться інцидент, який виправдав би вжиття заходів.189

Під час кібератак слід ретельно враховувати принцип суверенітету в процесі застосування заходів самозахисту та переходу до оборони. Якщо держава жертви вимагає та погоджується, можуть бути вжиті заходи колективної самооборони, обмежені обсягом запиту. Зрештою, про заходи індивідуальної або колективної самооборони необхідно повідомляти Раду Безпеки ООН. Цей обов’язок не є істотною умовою, відсутність повідомлення не порушує права на самозахист. Однак не слід забувати, що ООН може втручатися в події для підтримки міжнародного миру та безпеки. 190 Зрештою, якщо кібератаки переступають поріг збройних нападів і стають взаємною та фактичною суперечкою між державами, застосування міжнародного гуманітарного права та права збройних конфліктів може стати предметом дискусії.

2.4. Міжнародна відповідальність держав та імплементація

Відповідальність стосується відшкодування збитків, що виникли внаслідок невиконання особами, які є суб'єктами правопорядку, своїх

зобов'язань. Скрізь, де є закон, будуть згадані права, обов’язки, а отже, і відповідальність. Міжнародна відповідальність може виникати і для держав через їх протиправні дії. З іншої точки зору, нові правові відносини, створені діями, які порушують права та обов’язки, існуючі в міжнародному праві, називаються міжнародною відповідальністю.191 Метою є відновлення балансу в цих правовідносинах між сторонами, які завдають шкоди, і жертвами.

Принципи щодо міжнародної відповідальності прийняті як міжнародні звичаєві норми і є обов'язковими для всіх держав. З моменту заснування ООН виникло бажання прийняти обов’язкове положення про міжнародну відповідальність, і врешті-решт у 2001 році Комісія міжнародного права, яка працює у сфері розвитку та кодифікації міжнародного права в рамках ООН, підготувала проект який включає 59 статей «Про відповідальність держав за дії, що суперечать міжнародному праву». 182 Законопроект включає існуючі звичайні норми та запроваджує деякі нові стандарти.193

Для того, щоб виникла міжнародна відповідальність держави, мають бути дотримані умови протиправних дій, шкоди, причинного зв’язку та приписування. Як правило, дії, що суперечать міжнародному праву, відбуваються у сферах, де існують міжнародні зобов'язання, але особливі випадки відповідальності також можуть бути передбачені міжнародними угодами. Зрештою, згідно зі статтею 38 Статуту МС можна легко сказати, що міжнародна відповідальність настане для держав у разі порушення міжнародних угод, загальних принципів права, звичаїв і традицій. По суті, видно, що в рішеннях щодо протоки Корфу та Нікарагуа є багатоаспектні порушення.194 У цьому контексті перша стаття проекту була написана з реченням «Кожна дія держави, що суперечить міжнародному праву, призводить до міжнародної відповідальності».

В умовах шкоди та причинного зв'язку фігурує ст.31. Відповідно, будь-яка матеріальна та моральна шкода, завдана несправедливим актом, підпадає під дію міжнародного права. Відшкодувати шкоду зобов'язана

держава, яка завдала шкоди. Власне, на відміну від матеріальної шкоди, враховується, що моральна шкода також вплине на репутацію держави і може призвести до порушення суверенітету в цьому контексті. 195 Дане положення викладено так:

Держава, відповідальна за дії, що суперечать міжнародному праву, повинна відшкодувати всю завдану ним шкоду.

Обсяг шкоди - це вся матеріальна і моральна шкода, завдана діянням, що суперечить міжнародному праву.

Порушення міжнародних зобов'язань може статися через невиконання того, що слід робити, або виконання того, що не слід робити. Однак очевидно, що міжнародна відповідальність виникне, якщо дії чи бездіяльність, про які йде мова, будуть приписані державам. Ця ситуація виражена в статті 2 проекту таким чином:

Коли існує поведінка, яка включає дію чи бездіяльність, умови, необхідні для того, щоб держава діяла всупереч міжнародному праву, є такими:

(a) це може бути віднесено до держави відповідно до міжнародного права, і

(b) це є порушенням міжнародного зобов'язання держави.

Ці дві умови повинні бути присутніми в сукупності в конкретному випадку. Інакше міжнародна відповідальність держав не настане.

У той час як відповідальність держави в діяльності державних органів може бути визначена безсумнівно і чітко, це неможливо для ідентифікації осіб та установ, які діють за вказівками держави. Претензія щодо відповідальності держав, звичайно, є серйозною, і в усталеній юриспруденції прийнято, що сторона, яка стверджує таку відповідальність, повинна довести це «чіткими, переконливими та переконливими доказами». 196 У межах нашого дослідження це подвійне розрізнення та приписування протиправного діяння державі мають велике значення.

У статтях 4-11 законопроекту містяться положення, що роз’яснюють відповідальність держави за дії державних органів, а також за дії осіб і установ, підпорядкованих державі. Підсумовуючи відповідні положення, держави несуть відповідальність за всі дії, що суперечать міжнародному праву, у яких використовується державна влада. Проте, якщо в діяльності приватних осіб є наказ, розпорядження та пропозиції держави, відповідні держави можуть нести відповідальність за ці дії. Міжнародна відповідальність також поширюватиметься на дії, які держави приймають як свою власну поведінку, а збитки потребуватимуть відшкодування. У випадку груп повстання та повстання, відповідальність не виникає, якщо держави не порушують свій обов’язок піклуватися. Порушення обов'язку піклування ґрунтується на використанні та нагляді за власним суверенітетом держав у спосіб, який запобігає завданню шкоди іншим державам. Це питання, з яким ми стикаємося в рамках загальних принципів права, також було підкреслено в Рішенні щодо протоки Корфу.197

Якщо умови, пов’язані з діями, про які йде мова, будуть доведені державою, яка зазнала прямої чи непрямої шкоди внаслідок будь-яких дій, дія припиняється та розпочинається процес компенсації. У зв’язку з цим, згода держави-жертви, самозахист, контрзаходи, які є законними або пропорційними збитковим діям, форс-мажорні обставини та практика крайньої необхідності зберігаються.198

Міжнародна відповідальність і приписування в кіберпросторі є важливими в процесі визначення особи та місцезнаходження особи-злочинця, яка вчинила кібер-дії. Власне, ця детермінація відіграє роль у визначенні відповіді на дію та адресата. Однак через анонімну, багаторівневу та швидку структуру кіберпростору стає важко виявити вищий інтелект, що стоїть за кібердіями.199

Беручи до уваги проект, підготовлений Комісією міжнародного права, і звичайні норми в цих рамках, питання та проблеми щодо діяльності в кіберпросторі, що призводить до міжнародної відповідальності, виходять на

перший план. Коли Талліннське керівництво розглядається разом із відповідними правилами, робиться висновок, що кібератаки мають відбутися в одній із трьох ситуацій, щоб їх можна було оцінити в рамках міжнародної відповідальності. Ситуації, про які йдеться, виражені таким чином:200

– Кібератаку здійснюють державні органи.

– Кібератака відбувається внаслідок недбалості чи незнання держави та порушення обов’язку обережності.

- Кібератака здійснюється недержавними суб'єктами за наказом, керівництвом або контролем держави.

У правилах 14-19 Талліннського керівництва питання міжнародної відповідальності детально розглядається. Відповідно, держава нестиме міжнародну відповідальність за «пов’язані з кібернетичною діяльністю дії», які становлять порушення зобов’язань, які вона має згідно з міжнародним правом. Термін пов’язані з кібер-діяльністю включає кібер-діяльність, яку здійснюють самі держави або в якій вони беруть участь, а також виділення кібер-інфраструктури для зловмисного використання іншою державою, недбалість щодо кібер-інфраструктури або надання програмного та апаратного забезпечення для кібердіяльності. 201

Міжнародний суд підтверджує характер міжнародної відповідальності у багатьох своїх рішеннях і пояснює, що порушення зобов’язань і приписування є важливими елементами міжнародної відповідальності. Зобов'язання, про які йде мова, можуть випливати з міжнародних угод, загальних принципів права та звичаєвих норм. У цьому контексті держави, крім зобов’язань одна перед одною, мають також зобов’язання перед міжнародним співтовариством. Хоча фізична шкода чи намір завдати шкоди не є істотними елементами в процесі визначення міжнародної відповідальності, вони можуть бути важливими в конкретному випадку. 202

Згідно з довідником, міжнародна відповідальність, що виникає внаслідок діяння, що суперечить міжнародному праву, також дійсна для збройних конфліктів, а також порушення норм, що регулюють мирний час.

Основні норми, такі як суверенітет, заборона застосування сили, принцип невтручання у внутрішні справи та заборона втручання, які стосуються обох підкатегорій, виділяються як основні норми, які можуть бути порушені. У цьому контексті обов'язки, які вимагають позитивних дій, також покладаються на держави. Наприклад, використання кіберпростору комп’ютерними активістами, терористичними організаціями та іншими групами та функціонування механізмів контролю, нагляду та запобіжних заходів у національному законодавстві для кібердіяльності розглядається як обов’язок держав відповідно до міжнародного права.203

Дії, здійснені в кіберпросторі, не підлягають міжнародному праву, якщо вони не порушують норми, які повинні застосовуватися в міжнародному праві. Міжнародна відповідальність не настане за питання, які прямо дозволені державам або які не регулюються міжнародним правом.204 Насправді, як чітко зазначено в Рішенні у справі Бозкурта-Лотоса, у питаннях, які не регулюються міжнародним правом, Авторитет держави розглядається як істотний завдяки принципу суверенітету. Наприклад, шпигунські дії держави в розвідувальних цілях у кіберсередовищі не загрожують миру та безпеці міжнародної спільноти, якщо вони не завдають шкоди. Якщо держави перевищують свою юрисдикцію в розвідці, збройних силах, внутрішній безпеці та інших питаннях і беруть участь у діях, які порушують міжнародне право, виникатиме міжнародна відповідальність. Ситуація, про яку йде мова, прийнята в нормах міжнародного звичайного права як заборона державам завдавати шкоди іншій державі своєю діяльністю у їхніх власних країнах, і в цьому контексті держави повинні проявляти належну обачність.205

Немає географічних обмежень для вчинення дій проти міжнародного права в кіберпросторі. Держави можуть вчиняти дії, про які йде мова, на своїй власній території, на території держави, яка завдасть шкоди, на території третьої держави, у відкритому морі, у міжнародному повітряному просторі або в космосі.206

Нарешті, якщо кібердіяльність відбувається в рамках згоди, самозахисту, контрзаходів, необхідності, форс-мажорних обставин чи необхідності, то протиправності немає. Ці ситуації з’являються як підстави законності в міжнародному праві.207 У цих випадках, як відображення принципу суверенітету, відповідна держава приймає рішення щодо свого внутрішнього функціонування та може вдаватися до різних методів з міркувань законності.

Кібератаки, здійснені державними органами або внаслідок порушення обов'язку обережності.

У рамках Проекту та Талліннського керівництва щодо відповідальності держав за дії, що суперечать міжнародному праву, кібердіяльність, що здійснюється державними органами або особами чи організаціями, уповноваженими здійснювати публічну владу, може бути приписана державам. Вираз, про який йде мова, є досить широким; кожна особа, установа чи організація під егідою держави, під наглядом держави, уповноважена національним законодавством, незалежно від її функції чи місця в країні, розглядається в цій сфері, і кожна вчинена дія, навіть здійснена з перевищенням повноважень, може призвести до міжнародної відповідальності держави.208

Кваліфікаційні елементи державної влади відносяться до основних функцій влади. Іншими словами, дії, за допомогою яких чинний уряд здійснює свої повноваження, такі як ведення зовнішніх справ, збір податків і використання правоохоронних органів, є відображенням державної влади. Однак існування державної влади не є певним у кожній дії. Що стосується кожного конкретного інциденту, необхідно оцінити повноваження держави, її мету, минулі практики та, зрештою, критерії відповідальності.

Держави можуть звертатися до приватних або добровільних організацій у випадках, коли вони не мають необхідного технічного обладнання або не хочуть здійснювати діяльність зі своїми власними установами в питаннях, які повинні здійснюватися як державна діяльність. У цьому випадку, коли

відбувається дія, що суперечить міжнародному праву, міжнародна відповідальність держави може виникнути, якщо ця дія приписується державі. У зв'язку з цим кібератаки можна навести як приклад приписування державі міжнародно-незаконних дій, здійснених компанією, яка займається кіберзахистом військових мереж, визначених урядом. Однак, згідно з Tallinn Guide, якщо компанія використовує методи протидії кібератакам для усунення зловмисних кібератак проти державних мереж, перевищуючи свої повноваження, цілком можливо, що держава не буде нести відповідальності за ці дії. Власне, відповідно до мети товариства та наданих повноважень необхідно і достатньо здійснювати лише захист. В іншому прикладі, якщо та сама компанія надає послуги з інформаційної безпеки для приватних установ у державі, проблеми, які виникають у цій службі через перевищення повноважень, не будуть відповідати державі. 209 Істотними умовами приписки є те, що повноваження надаються державою державним інституціям і що приватні особи та організації не вживають жодних дій, які перевищують межі відповідних повноважень.

Ознаки державної влади в діянні, що суперечить міжнародному праву, повинні бути доведені державою-жертвою. Традиційно використання танків і військових кораблів є достатнім і вагомим показником обвинувачення, оскільки воно може здійснюватися лише державою. Подібного засобу для дій і атак у кіберпросторі немає. По суті, недержавні кіберактори можуть захопити привілеї та повноваження, які має уряд у кіберпросторі, і використовувати кіберінфраструктуру або спрямувати її на кіберінфраструктуру держави. Хоча така ситуація створила б проблеми для держав на практиці, здається, що цього недостатньо для виникнення відповідальності. Однак надійні та перевірені розвіддані, які вказують на те, що держави відіграють провідну роль у цій ситуації, можуть змінити хід подій.210

Відповідно до посібника, якщо держава передає підлеглий їй орган у розпорядження іншої держави, кібердіяльність, яку здійснює цей орган за

наказом другої держави, може бути приписана другій державі, і міжнародна відповідальність буде під питанням. . Однак перша держава повинна виконати свій обов'язок турботи у формі відкликання та призупинення діяльності. Інакше перша держава може нести відповідальність за міжнародне порушення, яке відбудеться. Однак, якщо орган не діє відповідно до вказівок першої держави і продовжує свої дії, це правило не застосовуватиметься.211

Кібератаки недержавних суб’єктів

Як правило, кібердіяльність приватних осіб, груп і організацій не призводить до міжнародної відповідальності держав. Однак, згідно з проектом і Талліннським керівництвом, підготовленим Комісією міжнародного права, кібердіяльність, яку здійснюють недержавні суб’єкти, може бути приписана державам, якщо вона здійснюється за наказом, керівництвом чи контролем держави, або в питаннях, які сама держава приймає і приймає за своє. Відображення цих критеріїв у реальних відносинах може відрізнятися залежно від конкретної події. По суті, у міжнародному праві кожна подія залежить від власних фактів.212

Діяльність згідно з вказівками держави, як правило, еквівалентна діям приватних осіб та організацій, що працюють у рамках державної влади. Різниця в цьому відношенні виникає через елемент правового дозволу. Одним із найбільш типових прикладів на цю тему є те, що під час зловмисних кібердій проти інфраструктури держави держава заохочує недержавних суб’єктів втрутитися в кризу, і ці суб’єкти діють добровільно, щоб допомогти державі. Подібним чином, запитувані дії суб’єктів, яких просять здійснити певні форми кібератак для підтримки традиційної військової діяльності держави, також можуть бути віднесені до держав, і в цьому контексті міжнародна відповідальність може вийти на перший план.213

Поведінка недержавних акторів у межах командування, керівництва та контролю повинна оцінюватися разом із концепціями серйозної участі та ефективного контролю держави, як зазначено в Рішенні щодо Нікарагуа. Під

час здійснення конкретної кіберактивності, якщо дія недержавних акторів є невід'ємною частиною діяльності, що визначає процес і результат, і якщо ця дія підтримується самою державою, вона повинна бути приписана державі. Як приклад ефективного контролю, якщо держава розміщує вразливі місця в програмному забезпеченні, що використовується на комп'ютерах іншої держави за допомогою недержавних суб'єктів, і наказує використати ці вразливості за допомогою кібердій, держава, яка контролює поведінку суб'єктів, буде нести відповідальність.214

Дії, вжиті недержавними суб'єктами, які перевищують свої повноваження або є незалежними від дій держави, не можуть бути приписані державам, і міжнародна відповідальність у цьому контексті не виникає. Однак при цілісному підході, якщо буде визначено, що відповідна дія має важливий характер для досягнення мети, яку хоче досягти держава, приписування державі знову стане можливим. У зв'язку з цим як приклад можна навести підтримку зловмисного програмного забезпечення державою недержавним особам на території іншої держави та спричинення плутанини.215

Зрештою, слід взяти до уваги, що держави можуть бути притягнуті до відповідальності за всі свої дії, такі як усвідомлення дій, що суперечать міжнародному праву, допомога державам і недержавним суб'єктам у вчиненні цих дій, активне втручання в дії або примус до таких дій. Якщо буде доведено чіткими та переконливими доказами, що кібератака, яка перевищує поріг застосування сили і є принаймні такою ж ефективною, як і збройний напад, спонсорується державою, може виникнути питання про порушення заборони на застосування сили. 216 Однак через анонімний характер кібератак під час процесу атрибуції можуть виникнути різні проблеми. 217

Більшість кібердій складається з постійних і неавторизованих входів в систему, навіть якщо вони не спричиняють достатньо великих і всеосяжних проблем, щоб порушити заборону на застосування сили. При розгляді в контексті інтервенції та суверенітету у внутрішні справи іншої держави стає

важливим фактом те, що міжнародне право також застосовуватиметься до кібер-діяльності та що міжнародна відповідальність виникатиме, якщо будуть дотримані необхідні умови.218

РОЗДІЛ 3
ОСНОВНІ ПРИКЛАДИ ДЕРЖАВНИХ ЗАСТОСУВАНЬ У КІБЕРПРОСТОРІ

3.1.Кібератаки які, порушували принципи суверенітету, та заборони втручання

Кібератаки займають важливе місце серед сучасних і технологічних тактик атак завдяки своїй силі залякування та примусу. Особливо розвинені держави, які інвестують у технології, беруть активну роль у кіберпросторі та формують дискусії про природу кібератак на міжнародній арені. Враховуючи різні характеристики кібератак, зрозуміло, що міжнародний мир може бути порушений через кібератаки проти держав, проблеми можуть виникнути в економіці країни та соціальних структурах, і, зрештою, кібератаки можуть становити загрозу в усіх аспектах.

Загалом, базові послуги, такі як електроенергія, природний газ, вода та Інтернет, які забезпечують безперервність держав і які вони повинні надавати своїм громадянам, розглядаються в межах суверенітету в міжнародному праві, а втручання іншої держави в ці зони не вважаються доречними. Однак зловмисні атаки, спрямовані на зрив військових служб, що використовуються для захисту кордонів і суверенітету, ліквідацію ядерних центрів, виведення з ладу військового обладнання та створення проблем у повітряному або морському сполученні, можуть розглядатися в межах заборони на застосування сили. Міжнародні дебати викликають кібератаки, які в кінцевому підсумку призводять до саботажу багатьох людей, у тому числі держав, і завдають великої шкоди.219

Стає все більш важливим, щоб кібератаки, які використовуються державами для дестабілізації інших держав, паралізували системи захисту або порушили роботу державних послуг, оцінювалися з точки зору відповідності фундаментальним принципам міжнародного права. Необхідно

прояснити тему різними прикладами, щоб оцінити природу концепцій заборони застосування сили та втручання, які діють у міжнародному праві та завжди зберігають свою важливість у кібератаках. У цьому контексті було б корисно оцінити кібератаки, які, як стверджують, здійснюються державами проти інших держав у всьому світі в рамках прикладів. Кібератаки, пов'язані з державами, будуть розглянуті в рамках нашої теми в історичному порядку, з урахуванням їх інтенсивності та наслідків. Оцінюючи конкретні події, ми виходимо з огляду на основну інформацію, яка міститься в темі нашої дипломної роботи.

Перша кібератака та дебати щодо міжнародного права: Естонія (2007)

Естонія є країною, яка в різні періоди своєї історії зазнавала окупації та переслідувань з боку Росії та Німеччини. Під час Другої світової війни Естонія спочатку була окупована Радянським Союзом і потрапила під контроль Німеччини через різні події під час війни. Наприкінці війни Радянський Союз знову вторгся до Естонії, і Естонія стала частиною Радянського Союзу до кінця холодної війни.220

Після закінчення холодної війни та розпаду Радянського Союзу багато держав проголосили свою незалежність. Естонія також посіла своє місце на сцені історії як одна з держав, що проголосили свою незалежність. Однак, на відміну від багатьох держав, які вийшли з Радянського Союзу, Естонія відмовилася надати громадянство російській меншині, з якою вони жили. Ця меншина становить приблизно 40% населення країни. 221 Хоча уряд Естонії продовжував цю політику в рамках мети захисту національної ідентичності країни та інтересів безпеки, ця ситуація спричинила проблеми у відносинах між Естонією та Росією. Нездатність російської меншини отримати громадянство чи неналежний захист прав меншини призвели до дипломатичної напруги та політичних розбіжностей. Напруга у відносинах між Естонією та Росією в різні періоди набувала різних вимірів і продовжувала породжувати дебати в міжнародних відносинах.

З початку 2000-х Естонія надає великого значення інвестиціям в інфраструктуру Інтернету. Завдяки цим інвестиціям у поєднанні з високоосвіченим населенням і технологічною спадщиною вона створила систему, яка включає зв'язок, телекомунікації, програмне забезпечення та мережеві технології, яку називають найпередовішим у Європі «електронним урядом». Ця система проклала шлях для багатьох технологічних інновацій, які підтримуватимуть розвиток держав. Технологічна інфраструктура Естонії та використання Інтернету сприяли появі та розвитку таких інноваційних проектів. Це зробило Естонію цифровим лідером і технологічним центром. Відносно розвинена система електронного урядування Естонії стала прикладом для інших держав і надихнула на цифрову трансформацію.222

Причиною кібератак проти Естонії стало рішення уряду Естонії демонтувати пам'ятник, відому як «Бронзовий солдат», який був побудований за часів Радянського Союзу. Статуя «Бронзовий солдат» багато років стояла в центрі Таллінна і символізувала звільнення Естонії від нацистської окупації. Уряд хотів прибрати статую, про яку йдеться, з центру міста та перенести її в менш помітне місце. Це рішення було сприйнято як провокацію серед російської меншини Естонії та викликало протести.

Зловмисні кіберхакери, або кібервоїни, рішення про демогтаж пам'ятника використали як можливість і здійснили атаки на об'єкти критичної інфраструктури естонського уряду. Ці атаки відбувалися у формі DDoS-атак, спрямованих на блокування онлайн-сервісів президента, парламенту, політичних партій, інтернет-провайдерів і банків, і завдали великої шкоди, націлившись на інфраструктурні системи. Захопивши приблизно один мільйон комп'ютерів із 75 різних країн, було створено структурну мережу під назвою «Ботнет» і створено інтенсивний інтернет-трафік через комп'ютери-зомбі. Проблеми виникли в технологічному структуруванні стану в результаті колапсу цільових систем, які не витримали інтенсивності. Кібератаки, про які йдеться, сильно вплинули на Естонію та спричинили перебої в роботі інтернет-служб країни.

223 Кібератаки тривали протягом трьох тижнів між 26 квітня та 19 травня 2007 року, і значна частина державних служб Естонії була вражена та стала непридатною. Хоча уряд Естонії вирішив заблокувати доступ до національної мережі Інтернет країни з-за меж країни під час атак, атаки тривали, але були зменшені до розумного та допустимого рівня. 224 В результаті цих атак уряд Естонії зазнав великих фінансових втрат і був змушений витратити велику кількість ресурсів, еквівалентну співвідношенню п’ятсот до одного, щоб ліквідувати наслідки атаки.225

Хоча державні установи Естонії, інтернет-провайдери та банки протистояли атакам, вживаючи заходів обережності під час процесу, було помічено, що уряд Естонії звернувся за допомогою до країн-членів НАТО. На тлі атак на перший план вийшли події на ґрунті «кіберпростору» як нової лінії напруженості між Росією та НАТО та почалися дискусії в контексті міжнародного права. Під час процесу заступник генерального секретаря НАТО посол Сорін Дукару заявив, що Естонія відіграє важливу роль у формуванні політики кібербезпеки в НАТО. Він також наголосив на масштабах загрози, оскільки пізніше Росія здійснила подібні напади на Грузію, Україну та Крим. З цієї причини країни НАТО направили до Таллінна експертів з кібербезпеки та допомогли із системами захисту. НАТО зосередила свою роботу в цій сфері, перемістивши Об’єднаний центр передового досвіду кіберзахисту до Естонії в серпні 2008 року. Через цей центр були створені концепції та основи кіберзахисту НАТО, а також почали проводитися міжнародні кібернавчання. 226 Однак було зазначено, що особи зловмисників неможливо встановити через їх анонімність. Однак прес-секретар Кремля Дмитро Пєсков також заявив, що ці атаки не мають жодного зв’язку з Росією.227

У результаті відомо, що Росія вважала за краще заперечувати звинувачення в тому, що атака була здійснена Росією, і що не вдалося надати остаточних доказів того, хто здійснив таку масовану атаку. Виявлення таких кібератак і ідентифікація зловмисників часто є складним процесом. Потрібна

співпраця та обмін інформацією між країною, де стався напад, та іншими країнами. Крім того, стає важливим підвищити обізнаність про кібербезпеку для посилення заходів безпеки та захисту від кібератак.

Естонські урядовці зафіксували ці події як кібератаку проти них з боку Росії. За словами співробітників естонської розвідки, Росія, схоже, має необхідні інструменти та ресурси для здійснення таких атак. Однак, згідно з заявою естонської держави, було встановлено, що під час масштабних DDoS-атак на російськомовних платформах соціальних медіа та веб-сайтах велася пропаганда про те, що патріотично налаштовані росіяни повинні підтримувати ці кібератаки. З іншого боку, було зазначено, що існують різні ознаки того, що російський уряд того періоду організував або принаймні підтримував ці напади. У цьому контексті було зазначено, що IP-адреси більшості комп'ютерів, залучених до атаки, походять з Росії, що значна частина людей, які беруть участь у цих атаках, мають досвід кібератак, і що результати підтверджують твердження, що напади на Естонію були здійснені Росією спланово та організовано.228

Кібератаки на Естонію детально обговорювали вчені, які продовжують свої дослідження в галузі міжнародного права. За словами Шмітта, згадані атаки мали значний вплив на роботу уряду та державних послуг. Крім того, економічна діяльність і операції уряду були миттєво вражені, і в результаті громадяни не мали доступу до державних коштів та інших переваг. Ці атаки спрямовані не лише на економічний та політичний тиск на державу, а й на навмисне порушення адміністративно-економічного функціонування. Відповідно до поглядів, висловлених у Талліннському довіднику та довідниках, у яких Шмітт оцінював цю тему, напади на Естонію не перевищують поріг збройного нападу. З цієї причини неможливо визначити події, про які йдеться, як застосування сили або оцінити їх у контексті заборони застосування сили. Однак факт втручання в суверенітет Естонії є безсумнівним.229

Так само щодо того, чи напади на Естонію є застосуванням сили, Цагуріс вважає, що напад був обмеженим, його шкідливий вплив був на контрольованому рівні, а окупаційний характер нападів був тимчасовим. Він вважає, що економічні та фінансові наслідки мають тимчасовий вплив, а не руйнівні. Незважаючи на все це, Цагуріас підкреслив, що напади, про які йдеться, мали характер міжнародного тиску з метою змусити уряд Естонії відмовитися від свого рішення, і тому оцінив напади як заборону втручання та порушення державного суверенітету.230

Деякі різні автори вважають, що існуючі норми слід тлумачити розширено. З цієї точки зору, замість того, щоб досліджувати кінетичні наслідки кібератак, слід зазначити, що ці атаки є прямим нападом на існування держави та її право на подальше існування, і слід підкреслити широкі наслідки атаки. У прикладі Естонії стверджується, що потік інформації заблокований, на відміну від потоку конкретних послуг і процесів, і наголошується, що сьогодні потік інформації є життєво важливим для фізичного та матеріального добробуту суспільства та стати більш важливим, ніж у минулому.231

У будь-якому випадку, ці події, через їх вплив і масштаби, були оцінені в контексті суверенітету, принципу невтручання у внутрішні справи та заборони втручання, і зайняли своє місце в історії як перша кібератака, яка почала дискусії з цього питання. 232 Кібератаки, про які йдеться, стали важливим поворотним моментом для Естонії, щоб переглянути свої можливості кіберзахисту та підвищити обізнаність міжнародної спільноти щодо кібербезпеки. Після подій Естонія взяла на себе лідерську роль у сфері кібербезпеки на міжнародній арені. Розпочато спільні кроки для проведення досліджень захисту від кібератак і стратегій кіберзахисту в міжнародному праві. Вважається, що з часом дискусії зійдуться до спільного знаменника, і кібератаки будуть усунені таким чином, щоб не завдавати шкоди державам, у контексті таких основних понять, як суверенітет держав у міжнародному праві, заборона застосування сили та втручання.

Гібридний характер кібератак: грузино-російські проблеми (2008)

У 2008 році внаслідок кризи у Південній Осетії та Абхазії між Росією та Грузією сталися військові конфлікти та кібератаки. У той час як Збройні сили Росії продовжували звичайні методи у військовій операції проти Грузії, вони також здійснювали інтенсивні атаки в кіберпросторі. Таким чином він мав на меті отримати перевагу над Грузією, розділивши увагу свого ворога на дві різні сфери. Ці події розглядаються як один із важливих поворотних пунктів з точки зору кібербезпеки та міжнародних відносин.233

Після розпаду Радянського Союзу Абхазія та Південна Осетія продовжили своє існування як автономні області. Проте влітку 2008 року національні провокації в Грузії вийшли на перший план, і грузинські ЗСУ почали операцію проти Південної Осетії. Метою цих операцій є захист територіальної цілісності країни та забезпечення суверенітету Грузії в регіоні. Проте наступними днями Збройні сили Росії втрутилися та увійшли на територію Грузії, розпочали серію окупаційних дій проти Грузії, а ситуація ще більше ускладнилася з кібератаками. Вважається, що на основі цієї напруги діють ідеологічні та геополітичні фактори. Зокрема, кроки, які Грузія вживає для покращення своїх політичних відносин із країнами Західного блоку та НАТО, а також сприйняття Росією того, що присутність країни-члена НАТО в її сусідній географічній зоні є загрозою її суверенітету, є одним із головних елементів проблеми. .234

Кібератаки, здійснені російськими кібератакорами, доцільніше було б проаналізувати, розділивши їх на два основні мотиви: створення міжнародної громадської думки та послаблення уряду Грузії, щоб показати хід подій. Першою метою було завдати шкоди іміджу Грузії та представити її роль як рятівника, поширюючи на міжнародній арені пропаганду про те, що грузинський уряд Росії проводить політику пригнічення меншин. У цьому контексті було помічено, що Росія намагається позиціонувати себе в позитивному ключі, наголошуючи на твердженнях про порушення прав меншин у Грузії. Метою Росії є захистити себе в контексті міжнародного

права як рятівника та гравця, що поважає права людини. Було створено величезний трафік Інтернету та неправдивої інформації, щоб змусити громадськість вважати цю інформацію правдивою.235

Наприклад, примітна пропагандистська діяльність, яка порівнює Саакашвілі, одного з колишніх лідерів Грузії, з лідером нацистів Адольфом Гітлером. Проте можна також вважати пропагандистську діяльність, про яку йде мова, великою мірою відображенням свободи слова. Свобода вираження поглядів на міжнародній арені є важливим елементом вільного вираження різних поглядів і думок. Незважаючи на те, що така пропаганда та риторика можуть викликати різну реакцію в міжнародному співтоваристві, їх потрібно ретельно оцінювати, щоб захистити свободу слова. 236 Важливо, щоб такі дії, які відбуваються в кіберпросторі, не обмежували свободу вираження поглядів у цифровому просторі та не завдавали шкоди демократичним цінностям. Однак не слід забувати, що також важливо, щоб ці ситуації залишалися в рамках правових і етичних кордонів і не втручалися у внутрішні справи інших країн.

З іншого боку, діяльність російських кіберхакерів, спрямована на послаблення уряду Грузії, постає як друга мета. Ці дії були спрямовані на дестабілізацію політичної та соціальної структури в Грузії. Кібератаки Росії на Грузію мають на меті паралізувати та вивести з ладу уряд за допомогою DDoS-атак на важливі інфраструктури країни, подібно до прикладу Естонії. Згідно зі звітом, підготовленим Міжнародною комісією з встановлення фактів щодо конфлікту в Грузії, найважливішими з цих кібератак є такі:237

– 20 липня сайт президента Саакашвілі був закритий на 24 години.

- 7 серпня багато серверів і інтернет-трафіку в Грузії було вилучено і поставлено під зовнішній контроль.

– 8 серпня почалася масштабна кібератака, джерело атак встановити не вдалося. За деякими даними, ці операції приписують організації під назвою «Російська бізнес-мережа». У цьому процесі урядові веб-сайти Грузії стали непридатними для використання в США, Великобританії та Європі. Крім

того, вважалося, що доступ через турецький AS9121 TTNet Server COMSTAR був заблокований.

- 9 серпня веб-сайт Міністерства закордонних справ Грузії було зламано кіберзловмисниками та опубліковано провокаційний контент. Водночас сайти МВС, Міністерства оборони та прогрузинської Тимчасової адміністрації Південної Осетії також зазнали інших кібератак. Протягом цього періоду Національний банк Грузії та сайти преси/ЗМІ зазнали DDoS-атак і стали непрацездатними.

– 12 серпня сайт президента Саакашвілі та популярний грузинський телеканал «Руставі» були передані «Тюліп Системс». Також було атаковано Tulip Systems.

– 12-13 серпня сайт Міністерства оборони зазнав масштабної кібератаки та двічі ставав недоступним.

Ці кібератаки показують, що існує спроба серйозно послабити грузинський уряд шляхом впливу на інфраструктуру країни. Такі атаки привертають увагу міжнародної спільноти щодо кібербезпеки та підкреслюють, що держави повинні посилити заходи, які вони вживатимуть у кіберсфері. Кібератаки стали зброєю, яка може мати значні наслідки в міжнародних відносинах, і важливо вживати ефективних заходів проти такої діяльності.

Після перевірки атак і проведення необхідних розслідувань було встановлено, що сайти, використані в атаках, були відкриті через Росію та Туреччину за допомогою кредитних карток, що працюють у США, і що непотрібні електронні листи були надіслані, щоб паралізувати систему. Ці знахідки чітко показують, що напад було здійснено в складній і багатогранній структурі.238

Між кібератаками на Грузію та подіями в Естонії є певна схожість. Російські сайти «StopGeorgia.ru» і «Zakep.ru» були виявлені організаторами атак, а інструкції щодо атаки та інструменти атаки були спрямовані з цих платформ. Поряд з DDoS-атаками також використовувалися такі методи, як

програми-вимагачі та соціальна інженерія. У цьому контексті розуміється, що атаки були здійснені організованою структурою і що було зовнішнє втручання, і вважається, що це також підтримували російські спецслужби.239

У науковій літературі та на міжнародній арені кібератаки порівнюють із «туманом війни». Згідно з цією концепцією, кібератаки здійснюються з метою підтримки та відволікання інших військових операцій і поєднують чинники невизначеності, хаосу, безладу, обману, введення в оману та пропаганди. Ця ситуація показує складність кібератак і те, що вони повинні розглядатися як частина військових частин через їх характер.240

Передбачувані кібератаки Росії проти Грузії виглядають як складні та сплановані дії, спрямовані на цифрову інфраструктуру, але також спрямовані на підтримку військових операцій і відволікання ворога. Очевидно, що такі кібератаки можуть мати наслідки на рівні сучасного застосування сили, тому з часом вони будуть відігравати більш важливу роль, і в міжнародному співтоваристві слід вживати необхідних заходів проти таких дій.

Порівняння того, що сталося у випадку з Грузією, з тактикою, використаною в рамках операції в Іраку 2003 року, спільно здійсненої США та Великою Британією, допоможе краще оцінити позицію кібератак у гібридних атаках. Коротко кажучи, під час операції в Іраку в 2003 році США проникли в системи військового зв'язку Іраку, і деякі повідомлення, підготовлені Пентагоном, були відправлені іракським офіцерам. У відповідних повідомленнях було зазначено, що США напали на Ірак великою силою і що їхньою метою було забезпечити звільнення іракського народу від Саддама Хусейна та його двох синів. 241 У зв’язку з цим кібератаки надають можливість прямого втручання у військові системи зв’язку як частину сучасної війни та мають силу впливати на сприйняття ворогом. У той час як кібератаки можуть скеровувати традиційні атаки, вони також можуть спричиняти психологічні наслідки. Це свідчить про те, що війна виграється не лише у фізичному полі, а й у кібернетичному полі, і що важливо також

отримати психологічну перевагу. Сьогодні кібератаки та кібербезпека стають важливою складовою стратегій держав.

Нарешті, для нашої теми буде необхідно і корисно дослідити, як напруга між Росією і Грузією оцінюється в міжнародному праві в рамках аналізу Шмітта. З огляду на аналіз Шмітта, кібератаки на Грузію можна розглядати як проблему з важливим правовим і політичним виміром. Враховуючи інтенсивність та наслідки атак, виявляється, що тривале закриття державних установ, особливо припинення медіа та банківської діяльності на тривалий період часу, завдає серйозної шкоди. Крім того, вважається, що було порушено суверенітет, один із фундаментальних принципів міжнародного права.

Суверенітет включає повноваження визначати внутрішню та зовнішню стратегію держави та втручатися проти різних факторів. Вплив кібератак на Грузію порушив принцип суверенітету, оскільки становив загрозу внутрішнім справам та економіці держави. Оскільки одним із найважливіших обов'язків держави є забезпечення безпеки та добробуту громадян, такий напад завадив державі виконувати свої основні функції та викликав хвилювання серед громадян. З цієї причини очевидно, що принцип суверенітету було порушено, і його слід оцінювати окремо в рамках права міжнародної відповідальності.

Кібератаки відбулися миттєво і швидко, завдавши прямої шкоди Грузії. Крім того, той факт, що ці атаки збіглися з початком російсько-грузинської війни, підтверджує твердження, що вони були здійснені Російською Федерацією або групами, якими вона особисто керувала, навіть якщо Росія заперечує свою відповідальність за ці атаки. Крім того, згідно з висновками Міжнародної комісії з розслідування конфлікту в Грузії, не слід забувати про причетність російських спецслужб до цих нападів.242

Незважаючи на те, що однією з головних цілей атаки було вивести з ладу медіа та банки Грузії, той факт, що населення країни періодично обмежувало доступ до Інтернету, призводив до того, що Грузія постраждала від цих атак менше, ніж приклад Естонії. 243 З цієї причини відображення

нападів у міжнародному праві були м’якшими порівняно з основними прикладами та розглядалися як один із етапів підготовки традиційних нападів серед актів застосування сили. Навіть якщо вважати, що події, про які йдеться, не відповідають інтенсивності та рівню застосування сили, слід підкреслити, що, якщо їх оцінювати разом із традиційними методами, вони мають характер порушення принципу невтручання у внутрішні справи. 244

Найважливішою особливістю кібератак проти Грузії є те, що це перша в історії акція в кіберпросторі, яка зіграла допоміжну роль у гарячому конфлікті. Хоча ця ситуація вважається піонерським прикладом використання кібератак як частини сучасних гібридних атак, також зазначено, що напруга між Грузією та Росією увійшла в історію як перший випадок, коли кібератаки були використані до початку збройного конфлікту. 245

Зрештою, кібератаки все більше набувають значення як попередньої частини традиційних військових операцій, а також окремих, викликаючи більше дискусій про міжнародне право та кібербезпеку. Слід зазначити, що визначити межі кібератак досить складно. Необхідно подумати про те, як міжнародна спільнота відреагує на такі події, які представляють нові аспекти сучасної війни, і як запобігти кібератакам.

Кібератаки з метою примусу: трикутник США-Sony-Північна Корея (2014)

У 2014 році кібератаки проти американської компанії Sony Pictures Entertainment мали світовий резонанс і були на порядку денному міжнародної громадськості. Через те, що технологічний гігант Sony не вжив ефективних заходів проти цих атак, його комп’ютерні системи були конфісковані, а також стався витік конфіденційних документів і електронних листів, що належали компанії. Ця ситуація була зафіксована як серйозний збій у кібербезпеці.

Цікаво, що напруга і початок проблем постають як у кіно. Остання кінематографічна культура США включає в себе фільми, які мають на меті представити критичний погляд на США та штати, які далекі від культури США загалом, і загалом відображають деяке цинічне ставлення до штатів

глядачам через кіно. Кібератаки на Sony виникли через комедійний фільм під назвою «Інтерв'ю», який був підготовлений про Кім Чен Ина, який прийшов до влади після смерті лідера Північної Кореї Кім Чен Іра.246

Фільм був представлений на YouTube та подібних соціальних мережах 11 червня 2014 року. Сюжет фільму: ведучий ток-шоу, завербований ЦРУ, їде до Північної Кореї під приводом взяти інтерв'ю у нового північнокорейського лідера та вбиває його. На цей фільм відреагувала Північна Корея, оскільки він був націлений на особистість Кім Чен Ина як політика та глави держави, і уряд Північної Кореї вимагав припинити виробництво цього фільму. Власне кажучи, фільм, про який йде мова, був розцінений Північною Кореєю як напад на них як на «державу» та був негайно й суворо засуджений на міжнародному рівні. 247 Проте приблизно через два тижні після презентації фільму представник Північної Кореї в ООН Джа Сон Нам написав листа Генеральному секретарю ООН Пан Гі Муну. Заяви в листі такі:248

Дозвіл суверенній державі створювати та розповсюджувати такий фільм про вбивство чинного президента розглядається як акт війни, а також як явне спонсорування тероризму. Влада США має негайно вжити відповідних заходів, інакше вони будуть нести повну відповідальність за заохочення та підтримку тероризму.

За тиждень до Дня подяки в США керівники Sony отримали електронний лист із політичними вимогами, надісланими групою під назвою «God'sApstls». Через кілька днів було встановлено, що комп'ютери співробітників Sony зазнали кібератак. Ця атака виявила вразливість кібербезпеки компанії Sony і була також зареєстрована як акт організованої злочинності. Співробітники виявили на своїх комп'ютерах тривожні зображення, повідомлення з погрозами та деякі посилання. Посилання виявилися списками деяких файлів, нібито взятих із даних компанії Sony. Це чітко продемонструвало, що атака не обмежувалася завданням шкоди в кіберпросторі, але також була внутрішньою діяльністю з вилучення даних.

Хакери з чорного капелюха, які називають себе «охоронцями миру (GoP's)», заволоділи конфіденційним, чутливим і нібито захищеним вмістом Sony.249

Атака також виявила вразливі місця в кібербезпеці Sony. Що стосується внутрішньої безпеки, компанія призначила Кевіна Мандіа, досвідченого експерта з кібербезпеки, розслідувати цей інцидент. Мандія описав напад як надзвичайно спланований та організований злочин. Було стверджено, що Sony та подібні компанії не були готові до атаки такого масштабу.250

У заявах Федерального бюро розслідувань (ФБР) після нападу є заяви про те, що події, що відбулися, не є терористичним актом, але є інформація, що процес показу фільму негативно вплинув і був зірваний. 251 Виходячи з цього, здається, що це перша кібератака, яка змінює бізнес-плани великої компанії шляхом тиску та залякування.

У заявах офіційних осіб Північної Кореї щодо подій зазначено, що вони не несуть відповідальності чи впливу щодо кібератаки. Однак у прес-релізі ФБР від 19 грудня 2014 року наголошується, що в черговий раз підтверджено, що атака Північної Кореї на Sony є однією з найглибших кіберзагроз національній безпеці Сполучених Штатів. Важливі розділи заяви ФБР такі:252

У результаті нашого розслідування та в тісній співпраці з іншими департаментами та агентствами уряду США ФБР тепер має достатньо інформації, щоб зробити висновок, що уряд Північної Кореї несе відповідальність за ці дії. Хоча необхідність захисту конфіденційних джерел і методів не дозволяє нам ділитися всією цією інформацією, наш висновок частково базується на наступному:

Технічний аналіз зловмисного програмного забезпечення для видалення даних, використаного в цій атаці, виявив зв’язки з іншим зловмисним програмним забезпеченням, про яке, як відомо ФБР, раніше розробили північнокорейські гравці. Наприклад, є подібності в певних рядках коду, алгоритмах шифрування, методах видалення даних і скомпрометованих мережах.

ФБР також помітило значне збігання між інфраструктурою, використаною в цій атаці, та іншою зловмисною кіберактивністю, яку уряд США раніше безпосередньо пов’язував з Північною Кореєю. Наприклад, ФБР виявило, що різні адреси Інтернет-протоколу (IP), пов’язані з відомою інфраструктурою Північної Кореї, обмінювалися даними з IP-адресами, жорстко закодованими в зловмисне програмне забезпечення для стирання даних, використане в цій атаці.

Крім того, інструменти, використані в атаці на Sony Pictures Entertainment, схожі на кібератаку, нібито здійснену Північною Кореєю проти південнокорейських банків і ЗМІ в березні минулого року.

Незалежне дослідження, проведене американськими компаніями з кібербезпеки, також дійшло висновку, що атаку здійснив уряд Північної Кореї. Однак розуміється, що ці результати не ґрунтуються на конкретних і остаточних доказах, а ґрунтуються на загальних висновках, тому не видається можливим приписати їх Північній Кореї. 253 Паралельно з розвитком подій, того ж дня тодішній президент США Барак Обама оголосив, що атаку здійснила Північна Корея та завдала великої шкоди, і сказав: «Ми відповімо на це. Він поставив крапку в ситуації своєю заявою: «Ми відповімо на це тим же, і ми зробимо це в час, який ми виберемо самі, у місці, яке ми виберемо, і в спосіб, який ми виберемо». 254 Угруповання під назвою GoP, яке згадувалося в кібератаках, було негайно розпущено в цьому процесі.

Після напруженості та кібератак між двома державами Sony та ключові люди, які працюють у Sony, почали хвилюватися щодо суперечливого фільму. Зокрема, виконавчий директор Sony Corporation Кадзуо Хіраї висловив ці занепокоєння в електронному листі, який він надіслав вищому керівництву Sony до виходу фільму. У заявах Хіраї явно відчувався дискомфорт, який відчував фільм. У результаті нових подій у фільмі були внесені значні зміни, а вміст, який можна було б вважати провокаційним, як-от сцена смерті Кім Чен Ина, було видалено з фільму. 255 Остаточно було вирішено, що фільм вийде в прокат 25 грудня 2014 року.

Хоча компанія вирішила випустити фільм, примітно, що кібератаки та загрози не мали продовження. Однак цю ситуацію можна інтерпретувати як ознаку того, що дії, здійснені зловмисниками, досягли бажаного результату. Ці дії є одним із рідкісних прикладів в історії використання державою кібератак як елементу тиску в міжнародному праві. Той факт, що уряд США виявив бажання відкрито та публічно захищати інтереси своїх приватних компаній, яскраво свідчить про важливість цієї події.256

З іншої точки зору, той факт, що не було представлено жодних доказів, які б конкретно підтверджували відповідальність і керівну роль Північної Кореї, показує серйозність інциденту. Насправді Мартін Вільямс, який працює в Північнокорейському технічному відділі та вивчає технології, заявив, що у заявах ФБР є невідповідності, і що, враховуючи логіку засобів і методів кібератак, які використовує Північна Корея, «вони ніколи не застосовували такі методи», і оцінив можливість того, що атаки були пов’язані з урядом Північної Кореї, підтвердивши це різними аргументами. 257

Шмітт провів детальну оцінку зловмисної кібердіяльності проти Sony відповідно до положень статей 2 і 51 Статуту ООН і звичаєвого міжнародного права. У цьому контексті висновки Шмітта можна підсумувати таким чином:258

- Зміст кібератак проти Sony в основному полягав у погрозах співробітникам, розкритті конфіденційної інформації та знищенні даних, у деяких випадках втрата даних навіть перешкоджала належному перезавантаженню комп’ютерів. Незважаючи на це, кібератаки на Sony не є «застосуванням сили», яке досягає рівня «збройного нападу». Хоча такі наслідки були надзвичайно руйнівними та дорогими, вони не були помічені на рівні, який експерти вважали б збройним нападом.

- Деякі точки зору відкидають думку про те, що право на самозахист також охоплює напади недержавних суб'єктів. Хоча роль Північної Кореї в подіях Sony ставиться під сумнів, ця дискусія не має значення. Насправді

атаки, про які йде мова, здійснюються хакерами з чорним капелюхом і їх не можна охарактеризувати як збройні атаки.

- Незважаючи на те, що поріг для застосування сили залишається неясним, погляди міжнародної спільноти щодо нападів на Sony здебільшого зосереджені на забороні втручання та порушенні принципу суверенітету. Коротко кажучи, вважається, що операція проти Sony не є незаконним «втручанням» проти США. Порушення діяльності приватної компанії не є однією з дій, які призводять до несанкціонованого проникнення в юрисдикцію іншої держави і, отже, до порушення заборони втручання. Ситуація, з якою зіткнулася Sony, надзвичайно далека від сфери заборони втручання.

– У нинішній ситуації опис подій Sony як порушення суверенітету США виглядає набагато більш обґрунтованим аргументом. Щоб порушення суверенітету відбулося, дія має бути приписувана державі. Якщо буде доведено, що група Вартових миру, яка здійснила атаку, діяла під впливом і керівництвом Північної Кореї, або якщо це буде особисто прийнято відповідною державою, відповідальність може бути покладена на Північну Корею і може бути обговорено питання про порушення Північною Кореєю принципу суверенітету. В даному випадку неважливо, що Sony є приватною компанією. Тому що кіберінфраструктура, про яку йде мова, розташована на території США і діє в межах суверенітету США.

- Хоча консенсусу з цього питання ще не досягнуто, видається розумним характеризувати кібероперацію, яка передбачає маніпулювання державою кіберінфраструктурою на території іншої держави або введення шкідливого програмного забезпечення в тамтешні системи, як порушення суверенітету цієї держави. . У цьому випадку, якщо можна приписати кібератаку на Sony Північній Кореї, Північна Корея порушила б суверенітет США. Крім того, ситуація, про яку йдеться, буде оцінена в рамках міжнародного законодавства про відповідальність і викличе внесення санкцій і контрзаходів до порядку денного в рамках «дій, що суперечать

міжнародному праву». Якщо напади не можуть бути юридично приписані Північній Кореї, санкції та контрзаходи можуть бути на порядку денному для Північної Кореї через порушення її обов’язку дбати про те, щоб дії в межах її національних кордонів не завдавали шкоди іншим державам.

Неспроможність довести відповідальність Північної Кореї за конкретний інцидент призвела до дискусій з різних точок зору щодо того, як такі атаки слід розглядати в міжнародних відносинах. Хоча атаку називають іншим прикладом, який змінює бізнес-плани Sony, вона не порушує заборону втручання, оскільки жертва не є державою. Проте, якщо вдасться приписати напад Північній Кореї, на перший план можуть вийти дискусії щодо порушення принципу суверенітету.

Зрештою, слід зазначити, що міжнародне право визнає широкий спектр можливих варіантів реагування на зловмисні кібероперації. Держави повинні керувати своїми діями, враховуючи ці можливості, і уникати поведінки, яка може порушити мир міжнародної спільноти. Насправді всі дії, що суперечать міжнародному праву, які можуть бути приписані державам, матимуть наслідки в міжнародному праві. Крім того, не слід забувати, що з точки зору згаданих дій, правові заходи можуть бути вжиті в межах внутрішнього законодавства, коли вступає в дію юрисдикція. Ті, хто причетний до кібератак, ризикуватимуть бути притягнуті до відповідальності за законодавством держави-жертви, звинувачені в хакерстві, економічному шпигунстві та інших злочинах.

3.2.Кібератаки у сфері заборони застосування сили та самозахисту

Підтримка кібератак: сирійсько-ізраїльська операція «Орчард» (2007)

У 2007 році Сирія в таємній співпраці з Північною Кореєю працювала над будівництвом ядерного об'єкта, який викликав би занепокоєння держави Ізраїль. Цей об’єкт відомий як Аль-Кібар і розташований у регіоні Дейр-ель-Зур у Сирії. Існують серйозні звинувачення, що цей об’єкт може

мати потужність для виробництва ядерної зброї. Основною основою звинувачень є секретні документи, отримані ізраїльською розвідувальною службою Моссад. Ці документи, отримані за допомогою вдосконаленого програмного забезпечення для кібершпигунства під назвою «Троянський кінь» з ноутбука сирійського урядовця, показують, що об’єкт класифікується як «дуже чутливий». Крім того, висновки щодо виробництва ядерної зброї також були ідентифіковані за фотографіями та планами будівництва в отриманих даних.259

У вересні цей об'єкт під назвою Аль-Кібар вибухнув і був повністю зруйнований бомбардуванням, коли він ще будувався. Існують вагомі ознаки того, що цей вибух був нападом, здійсненим безпосередньо ізраїльськими ВПС. Перед тим, як здійснити атаку на ймовірний ядерний об'єкт, стверджується, що Ізраїль наблизився до регіону Тель-Аб'яд, розташованого поблизу турецько-сирійського кордону, і здійснив електронну атаку. Вважається, що ця атака була здійснена за допомогою керованої ракети. Зазначається, що згадана атака тимчасово вивела з ладу сирійську радіолокаційну систему, що не дозволило літакам ізраїльських ВПС виявити їх вхід у повітряний простір Сирії. 260 Ці методи, з якими ми часто стикаємося під час кібератак, використовуються для нейтралізації систем захисту та відіграють активну роль у цьому процесі.

Хоча Сирія заперечувала атаку, фотографії, які з’явилися після атаки, показали, що це був реактор з графітовим охолодженням, тобто секретна ядерна структура. Зрозуміло, що цей реактор майже ідентичний реактору Йонбен, який використовується для виробництва плутонію в Північній Кореї. 261 Хоча спочатку Ізраїль заперечував, що атаку здійснив сам, деякі отримані дані показують, що операція була здійснена за допомогою потужної технології глушіння. 262

Незважаючи на те, що це викликало значний вплив і обурення в сирійській громадськості, жодної детальної заяви з цього приводу держави не зробили. Цей інцидент ще більше посилив політичну напругу та

занепокоєння безпекою в регіоні. Були міжнародні дискусії та спекуляції щодо прозорості ядерної програми Сирії, а ізраїльсько-сирійські відносини стали напруженими. Той факт, що не було зроблено жодних офіційних заяв про те, з якою саме метою був побудований секретний об'єкт і наскільки він розвинений, викликав дискусії.

Зрештою, майже через 11 років після нападу, 21 березня 2018 року, міністр оборони Ізраїлю Авігдор Ліберман офіційно взяв на себе відповідальність за цю операцію. Окрім сумних і ганебних заяв міністра Лібармана, було також наголошено, що сміливу позицію ізраїльського уряду та успішну операцію зі знищення ядерного реактора в Сирії не слід сприймати легковажно, і що він ніколи не дозволить ядерну зброю країнам, які загрожують існуванню Ізраїлю . 263 Однак слід підкреслити, що цю ситуацію потрібно буде оцінювати разом із поняттями застосування сили та самозахисту. На нашу думку, конкретний інцидент є яскравим прикладом порушення заборони на застосування сили, а оскільки минуло багато часу, критерій часової близькості між нападом і реалізацією права на необхідну оборону буде не буде виконано, і держава-жертва не матиме права на самозахист. Однак не слід ігнорувати, що такі ситуації можуть зашкодити дипломатичним відносинам і спричинити проблеми в міжнародному співтоваристві.

Orchard та подібні кібератаки надзвичайно важливі для оцінок у міжнародному праві. У цій операції Ізраїль використовував комбінацію традиційних і кібератак. Операція, про яку йдеться, є одним із перших прикладів того, що кібератаки, здійснені державами, можуть мати фізично руйнівні наслідки. У рамках підходу Ізраїлю до стратегічної безпеки кібератаки використовувалися, щоб перешкодити таким країнам, як Сирія та Іран, отримати ядерну зброю, а також захистити національну безпеку.

Операція Orchard також показала, що кібератаки забезпечують стратегічну перевагу для держав. Кібератаки можуть підвищити ефективність фізичних атак шляхом послаблення захисних механізмів, а в деяких випадках

можуть навіть повністю запобігти фізичним атакам. Це свідчить про те, що кібератаки є важливим інструментом досягнення державами своїх стратегічних цілей та забезпечення національної безпеки. Тому в майбутньому можливості кібератак можуть відігравати центральну роль у військових стратегіях держав.

Обговорення фізичної шкоди під час кібератак: Stuxnet (2014)

Іран постав перед нами зі своїми ініціативами в ядерних дослідженнях від минулого до сьогодення. У 2010 році ядерні об’єкти в Натанзі, Іран, зазнали кібератаки за допомогою високоефективного вірусу Stuxnet, і хоча Іран спочатку заперечував напад, він заявив, що він зазнав серйозної фізичної шкоди. 264 Вірус, про який йде мова, був визнаний поворотним пунктом для атак на комп’ютерні мережі в контексті основних принципів міжнародного права та викликав багато дискусій, які все ще залишаються важливими.

На першому етапі Stuxnet було відкрито в червні 2010 року Сергієм Уласенем, який працював аналітиком в антивірусній компанії під назвою «VirusBlokAda» в Мінську, Білорусь. 265 Згодом стало відомо, що Stuxnet виявила німецька компанія Siemens під час сканування промислової системи управління, і клієнти були попереджені, заявивши, що центральна система контролю та збору даних (SCADA) уразлива до цього вірусу. Цей вірус, здатний контролювати всю систему, на яку він націлений, може скористатися вразливістю безпеки операційних систем Windows, передавши його через невелику портативну пам’ять, а також може використовуватися для шпигунства та саботажу шляхом поширення в локальних обчислювальних мереж.266

У конкретному випадку вірус Stuxnet діяв як засіб контролю та надання даних у програмному забезпеченні, на яке він націлений, наприклад, у системі SCADA на ядерному об’єкті, і як тільки він був інтегрований у систему, він став дистанційно керованим за допомогою зв’язку з віддаленим сервером. На першому етапі вірус діяв, ховаючись, не починаючи зловмисної діяльності, таємно записував звичайні транзакції під час свого робочого

циклу та дотримувався політики поширення, виглядаючи легітимним у системі та на комп’ютерах, підключених до локальної мережі. 267 Через встановлення програмного забезпечення під назвою «людина посередині» в цільовій системі зв’язок між машиною та контролером було перервано, головний комп’ютер не міг виявити цю помилку та проблему зв’язку, тому пошкодження не можна було помітити на першому етапі . За оцінками, в результаті цієї атаки постраждали тридцять тисяч комп'ютерів. Крім того, повідомлялося, що щонайменше дві тисячі ядерних боєголовок стали непридатними через зміну параметрів тиску.268

Можна легко сказати, що Stuxnet, який суттєво відрізняється від інших зразків шкідливого програмного забезпечення, що використовується в кіберпросторі, і працює на безпрецедентному рівні з точки зору технічної складності та інтеграції, виділяється в деяких важливих аспектах. Особливості, які відрізняють Stuxnet від інших за своєю якістю, такі:269

- Відсутність помилок: Stuxnet привернув увагу як програмне забезпечення, яке майже не має помилок, які зазвичай зустрічаються в програмному забезпеченні для атак. Дивно, але на відміну від іншого програмного забезпечення для кібератак, у кодах Stuxnet не було виявлено жодних помилок.

- Уразливість нульового дня: Stuxnet відрізнявся здатністю поширюватися в системі за допомогою вразливостей нульового дня. Було визначено, що зловмисник або зловмисники, які використовують Stuxnet, використовують нову вразливість, яка раніше не була виявлена, а не використовують раніше відомі вразливості в цільовій системі. Атаки з використанням методу нульового дня є одними з рідкісних типів атак, які невідомі експертам з кібербезпеки та розробникам програмного забезпечення, і тому вразливі до заходів захисту.

- Методи ухилення від вірусів: виявлено, що Stuxnet має низку методів ухилення від вірусів, призначених для обману програмного забезпечення захисту комп’ютера та брандмауерів. Таким чином Stuxnet не можна було

виявити, поки він поширювався в системі, що давало зловмисникам час для досягнення своїх цілей.

З усіх цих причин зазначається, що напад на Іран тривалий час не вдавалося виявити і не могли бути вжиті необхідні запобіжні заходи. Власне кажучи, після того, як вплив Stuxnet на порядок денний зменшився, було оголошено, що атака почалася в 2009 році і що ситуація була відома лише в 2010 році. 270 Ці функції Stuxnet створили серйозний виклик для експертів з кібербезпеки та показали, що кібератаки стають дедалі складнішими та зосередженими на великих цілях.

Згідно з різними припущеннями, які поширюються в суспільстві, і звітами, представленими ЗМІ, стверджується, що атака Stuxnet була розроблена та використана в рамках спільної операції між спецслужбами США та Ізраїлю під назвою «Олімпійські ігри». Однак, оскільки жодна держава офіційно не взяла на себе наслідки та відповідальність за атаку, Іран не мав права відповідати на міжнародній арені. Stuxnet, який демонструє потенціал розвитку можливостей кібератак і вважається рідкісним прикладом загрози міжнародній безпеці через завдання фізичної шкоди, розглядається як поворотний момент у цьому відношенні.271

Відкриття різних варіантів Stuxnet також підвищило ймовірність того, що ефекти та наслідки кібератак можуть бути більшими, ніж вважалося. Наприклад, вважається, що вірус Duqu, виявлений у 2011 році та оброблений за допомогою подібної групи кодів, як Stuxnet, був розроблений командою, яка написала Stuxnet, або був успішною версією нового програмування, виконаного через Stuxnet. Однак відомо, що метою Duqu є збір розвідувальних даних від різних організацій, таких як виробники промислових систем управління, і використання цих даних для критичної інфраструктури. Аналогічно, вірус «Flame», інша версія Stuxnet і Duqu, був виявлений дослідниками в 2012 році. Flame описано як складний вірус, схожий за дизайном на Stuxnet і Duqu, але використовується в більш спеціалізованих цілеспрямованих атаках. ЗМІ повідомляють, що зловмисне

програмне забезпечення Stuxnet, Duqu і Flame було розроблено АНБ для проведення Олімпійських ігор.272

Кібератака Stuxnet чітко відрізняється від інших прикладів своєю здатністю завдати прямої фізичної шкоди та наміром завдати шкоди, яка матиме руйнівні наслідки в реальному світі, а не в кіберпросторі. Цей вірус використовувався спеціально для запобігання діяльності Ірану зі збагачення урану та порушив значну частину ядерної інфраструктури Ірану, негативно керуючи можливостями його системи. Після нападу іранські офіційні особи визнали, що тисячі ядерних центрифуг були пошкоджені. Однак у громадськості склалося враження, що завдано більше збитків, ніж офіційно.273

Вважається, що Stuxnet в основному здійснювався з метою перешкоджати ядерній діяльності Ірану протягом кількох років. Виявляється, що в результаті цієї атаки роботи на атомних енергетичних об’єктах в Бушері, Іран, також були затримані. Однак це не змінило планів Ірану щодо ядерної розробки, навпаки, його прихильність стала сильнішою. Іран не припинив своє виробництво збагаченого урану, а також не уклав угоди чи не співпрацював з іншою державою.274

Ще один результат щодо Stuxnet полягає в тому, що він показує, що бажаного результату можна досягти за короткий час з меншими витратами та впливом. Очевидно, що вартість звичайного застосування сили буде набагато вищою, ніж ціна кібератаки. Крім того, не слід ігнорувати, що військове втручання потенційно може спричинити набагато більші проблеми, ніж поточні проблеми.

Зі стратегічної точки зору Stuxnet показує, що межі між кіберзлочинністю та діями держави стираються. Держави можуть отримати вигоду від особисто вчинених кіберзлочинів і технологічних розробок у кіберпросторі. Фактично, у випадках, коли здатність держав використовувати технології кібератак є слабкою, можливі нові можливості, такі як залучення недержавних акторів і проведення операцій з кібератак.275

Історично Stuxnet вважається першою атакою, якій вдалося досягти фізичних результатів у результаті кібератаки, і з цієї причини існують оцінки, що в цьому інциденті було перевищено поріг застосування сили в міжнародному праві. Наприклад, Різ Нгуєн стверджує, що шкода, завдана Ірану цими нападами, мала подібний ефект до руйнування частково побудованих реакторів у Багдаді та Сирії в результаті авіаударів, здійснених Ізраїлем між 1987 і 2007 роками.276

Було б корисно завершити питання оцінкою розвитку подій після Stuxnet у контексті міжнародного права. Для того, щоб кібератаку вважали застосуванням сили, необхідно буде оцінити, чи ця сила відповідає застосуванню військової сили фізичного характеру, як обговорювалося під час подій в Естонії. Схоже, що атаки Stuxnet спрямовані на те, щоб фізично знищити або повністю знищити ціль за межами кіберпростору. У цьому контексті необхідно обговорити питання про те, чи мала місце дія, що суперечить забороні застосування сили, яка регулюється статтею 2/4 Статуту ООН. За словами Уолтера Гарі Шарпа, кібератака з руйнівними наслідками була здійснена безпосередньо на інфраструктуру Ірану.277

Домінуючою точкою зору в літературі з міжнародного права вважається те, що Stuxnet був явно руйнівною атакою і що наслідки цієї атаки спричинили подібні результати до збройної ракети чи бомби, і що всі основні принципи, такі як суверенітет, принцип не оцінюється втручання у внутрішні справи, заборона втручання та застосування сили. Однак слід підкреслити, що жодна держава, в тому числі держава-жертва Іран, не бачить у цій ситуації порушення суверенітету. Хоча важливість націлювання на ядерні системи Ірану юридично зрозуміла, одна з причин такої ситуації полягає в тому, що система не повністю уражена, і Іран хоче стримати поточну напругу або відповісти іншими методами з політичних причин. Однак, враховуючи серйозність і наслідки атаки, стає зрозуміло, що Stuxnet мав значні наслідки, і його необхідно оцінити відповідно до застосовних норм міжнародного права.

Правильніше було б оцінювати політичні та стратегічні кроки держав і юридичні факти окремо один від одного.278

Франсуа Делерю резюмував зв’язок між традиційними атаками та Stuxnet таким чином, наголошуючи на деяких важливих моментах:279

Кібероперації можна розглядати як діяльність, яка спричиняє руйнування, пошкодження, поранення або втрату людського життя, але такі атаки повинні мати певний ступінь тяжкості, щоб вважатися збройним нападом. Можливі сценарії підтримують думку про те, що фізичні наслідки кібероперації повинні перевищувати певний поріг тяжкості, щоб оцінити її вплив. Наприклад, коли досліджується інцидент зі Stuxnet, можна стверджувати, що наслідки цієї атаки як перевищили поріг насильства, так і залишилися нижче. У цьому контексті можливо, що Stuxnet можна вважати застосуванням сили, беручи до уваги лише її вплив, але не збройний напад. Однак той факт, що цей напад був спрямований на ядерний об’єкт, посилює можливість більш глибокого розгляду та оцінки його як збройного нападу з точки зору його наслідків.

Tallinn Guide представляє дискусію про те, чи слід вважати такі інциденти збройними нападами. Stuxnet вплинув на багато центрифуг, спричинивши фізичні пошкодження. Деякі члени Міжнародної групи експертів поділяють думку, що ця атака досягла порогу збройного нападу. Оскільки Stuxnet на сьогоднішній день є єдиною загальновідомою кібероперацією, яка мала серйозні наслідки, наразі неможливо прийняти більшість кібероперацій як збройні атаки. Однак не можна виключити можливість того, що кібероперація, яка може мати серйозні наслідки в майбутньому, буде вважатися збройним нападом.

У міжнародному праві роль кібератак у підтримці традиційних методів обговорювалася та визнавалася протягом тривалого часу. Завдяки Stuxnet ці дискусії розрослися та набули іншого виміру. Було зрозуміло, що існує потреба в більшій співпраці та консенсусі щодо кібератак, щоб забезпечити мир і безпеку міжнародної спільноти. По суті, стало зрозуміло, що необхідно

вжити конкретних національних і міжнародних заходів проти кібератаки, яка може завдати серйозної фізичної шкоди, і Stuxnet став важливим поворотним моментом з точки зору права.

Триваючі кібератаки: конфлікт між Україною та Росією (2014 р. – теперішній час)

Збройний конфлікт між Україною та Росією мають давню історію внаслідок історичних, політичних та географічних факторів. Після розпаду Радянського Союзу в 1991 році Україна проголосила свою незалежність і була визнана міжнародним співтовариством як незалежна держава. Проте цей процес незалежності став болісним через присутність російської меншини в таких регіонах, як східна Україна та Крим, етнічну подібність, економічний і політичний тиск та інші причини. З початку 2000-х років Україна зробила кроки для зміцнення своїх відносин з Європейським Союзом і НАТО, посиливши напругу між нею та Росією. Останніми роками ця напруга набула нових вимірів, особливо з використанням сучасних технологій, таких як кібератаки.

У листопаді 2013 року в Україні виникли проблеми через тих, хто був незадоволений підходом до управління, політикою уряду та економічним становищем проросійського лідера України Віктора Януковича. Проблеми наростали і переросли в кризу, і група людей розпочала акцію протесту на Майдані Незалежності у столиці Києві. 280 Протестувальники, які назвали себе «Євромайданом», завоювали місце у світовому порядку денному завдяки ефективній роботі в соціальних мережах і зуміли зібрати на Майдан близько 300 тисяч протестувальників.

З наслідком протестів інтенсивність і гострота кризи зросла, і в 2014 році, коли протестували 25 000 людей, спецпідрозділ «Беркут», відомий як проросійський, спричинив смерть понад 100 людей. Зрештою, 22 лютого 2014 року Янукович та його уряд пішли у відставку, протестувальники захопили громадські будівлі, а Янукович покинув країну та сховався в Росії. Було

створено тимчасовий уряд, головою якого було призначено Олександра Турчинова. Однак Росія заявила, що не визнає даний тимчасовий уряд.281

Від минулого до сьогодення Росія прагнула зберегти політичний контроль над державами, які проголосили незалежність, навіть якщо Радянський Союз розпадеться. З цієї причини вона використала протести Євромайдану на свою користь і перетворила кризу на військову та стратегічну можливість. Конфлікти, що почалися в різних регіонах України, втягнули країну в громадянську війну. 27-28 лютого 2014 року російські військові скупчилися на кордоні з Кримом, а батальйон спеціального призначення «Спецназ», спрямований у регіон, разом з проросійським підрозділом Криму проводив бойові дії з метою взяття під контроль державних установ. У столиці Криму Сімферополі приспустили український прапор і підняли російський. Прем'єр-міністром того періоду було призначено Сергія Аксьонова.282

16 березня 2014 року відбувся невизнаний Україною та іншими західними державами референдум, на якому 97% голосів «за» проголосили незалежність Криму. Одразу після цього лідери Росії та Криму зустрілися в Москві, столиці Росії, і підписали міжнародну угоду про приєднання Криму до Росії. Таким чином анексія Криму була офіційно реалізована і Крим фактично перейшов під владу Росії. Українці та кримські татари, які проживали в регіоні, змушені були мігрувати. 283 27 березня 2014 року Генеральна Асамблея ООН публічно оголосила про визнання недійсним референдуму в Криму. 284 США, Велика Британія, Франція, Німеччина, Італія, Польща, Канада, Японія, Нідерланди, Південна Корея, Грузія, Молдова, Туреччина, Австралія та Європейський Союз звинувачують Росію в порушенні суверенітету України та втручанні у внутрішні справи України. 285

Анексія Криму ще більше загострила напругу між Росією та Україною та вивела її в новий вимір. Через велику кількість російського населення в Донецькій і Луганській областях на сході України посилилися сепаратистські

рухи, і в квітні 2014 року на референдумах про незалежність було проголошено Донецьку і Луганську народні республіки. Згодом для об'єднання цих двох утворень було створено конфедеративну Новоросію під назвою Донбас. Росія явно продовжувала посилювати своє фактичне домінування на сході України. Ця ініціатива була переважно не визнана міжнародним співтовариством і вважалася загрозою територіальній цілісності України.286

У липні 2014 року малайзійський Boeing 777 MH17 був збитий східноукраїнськими військовими, які проводили сепаратистську політику, під час польоту над Донецькою та Луганською областями, серед 298 осіб, які перебували на борту, ніхто не вижив. Цей інцидент, який стався із застосуванням зброї російського виробництва, мав великий резонанс у міжнародному співтоваристві, але винних встановити не вдалося. Зрештою, ця криза, яка почалася з локальних проблем і наростала, стала загрозою міжнародному миру та безпеці та почалися гарячі конфлікти.287

Напруженість і військові конфлікти на Донбасі серйозно похитнули суверенітет України, і на порядок денний винесено угоду, в якій буде прийнято створення автономій у Донецькій і Луганській областях і буде досягнуто припинення вогню. Після цього 5 вересня 2014 року та 12 лютого 2015 року були підписані Мінські протоколи за участю України, Донецька, Луганська, Росії, Франції та Німеччини, а також представників Організації з безпеки та співробітництва в Європі (ОБСЄ). Мінські протоколи є першим позитивним кроком двох держав для забезпечення стабільності у східному регіоні України. Незважаючи на це, хоча збройні конфлікти на деякий час припинилися, політичні розбіжності тривали.289

Українсько-російська криза від початку до сьогодні тривала різними військовими та гарячими конфліктами, а також систематичними операціями, що проводяться за підтримки кібератак. Росія розташувала свої кібератаки на підтримку інших своїх стратегій з метою пропаганди проти України, спотворення інформації та порушення комунікаційних мереж і систем. У той

же час вона зробила зони конфлікту невидимими, прикриваючи свої військові операції кібератаками.

Росія здійснювала шпигунську діяльність шляхом кібератак проти України, а також використовувала різне програмне забезпечення, яке пошкоджувало інфраструктурні системи. Вперше він проник в державні системи України в 2010 році, використовуючи вірус, відомий як «Snake/Turla/Uroboros». Snake, який може легко обійти сканування вірусів і програми безпеки, відіграє активну роль завдяки своїй здатності читати й аналізувати всі види даних на комп'ютері та надсилати їх назовні. Таким чином Росія мала доступ до стратегій і планів України і завжди була на крок попереду.290

Під час протестів на Євромайдані та анексії Криму такі шкідливі програми, як MiniDuke, NetTraveler і RedOctober, також пошкодили українські системи. Багато шкоди Україні завдали спецпідрозділи «Беркут» і кіберугруповання, які вважаються афілійованими з «Беркутом» або діють самостійно. 291 Групи, про які йдеться, робили недоступними державні веб-сайти, блокували телефони українських урядовців, виводили з ладу медіа-сайти та українські веб-сайти підтримки, припиняли зв'язок через Інтернет, вилучали та публікували конфіденційні персональні дані, викрадали великі суми грошей із банків за допомогою цифрових переказів, і в кінцевому підсумку порушили цільове сприйняття військових систем.292

Події між Україною та Росією не обмежилися цим, у 2015 та 2016 роках були відключення електроенергії, які торкнулися більшості людей, які проживають в Україні. Особливо в період до відключення електроенергії в Україні проукраїнські активісти здійснювали фізичні напади на підстанції, що постачають електроенергію в Крим, і в результаті цієї ситуації близько двох мільйонів кримчан тимчасово залишилися без світла. 23 грудня 2015 року організовані та обережні кібератаки, які, очевидно, проводилися проти українських енергетичних компаній протягом 6 місяців, дали результат і призвели до того, що в Івано-Франківській області на заході України понад

700 000 людей залишилися без світла на години. Ці атаки вивели з ладу багато трансформаторів, заблокували кол-центри та видалили важливі файли комп'ютерів, зробивши систему непрацездатною. Ці події чітко продемонстрували потенціал використання кіберзброї як сучасного інструменту ведення війни та послужили сильним попередженням.293

Через рік, 17 грудня 2016 року, українська енергомережа піддалася ще одній масштабній кібератаці, в результаті якої було знеструмлено приблизно 225 тис. користувачів. Атака, схожа на атаку 2015 року, втратила наслідки за кілька годин, коли працівники вийшли на підстанції та вручну вимкнули вимикачі. Зловмисне програмне забезпечення, яке використовувалося в атаці, отримало назву «CrashOverride», і було визначено, що воно призначене для порушення фізичних промислових процесів. CrashOverride описано як друге зловмисне програмне забезпечення, яке вражає промислові системи з точки зору його природи та розміру, після Stuxnet. 294 Зрештою, було чітко продемонстровано, що кібератаки стають дедалі важливішими та можуть вплинути на умови життя.

Кібератаки, які продовжували збільшуватися в 2015 і 2016 роках і набули іншого значення завдяки кібергрупам, підтримуваним державами з фону, висунули на перший план багато проблем, що стосуються міжнародних відносин та економіки, а також правових питань. Група кіберхакерів, відома як «Fancy Bear» і, як вважають, особисто підтримувана Росією, атакувала сервери США, а інша група, «Sandworm», здійснила серію кібератак на державні структури України та компанії приватного сектора. . У 2017 році ситуація стала ще жахливішою з «NotPetya», однією з найруйнівніших атак в історії технологій, яка спричинила глобальні наслідки.295

Через кібератаку NotPetya, розпочату з серверів Linkos Group, української компанії-розробника програмного забезпечення, зловмисне програмне забезпечення поширилося по всьому світу, близько 8000 комп'ютерних мереж, сотні тисяч користувачів і 65 країн за кілька годин через обліковий додаток, який використовується в міжнародних транзакціях.

NotPetya, тип програми-вимагача, який з’явився протягом кількох місяців, може спонтанно переміщатися в системі та шифрувати системні файли, не вимагаючи жодного дозволу. Таким чином, сервери Windows стають недоступними, і користувачі не можуть користуватися своїми комп'ютерами. Це програмне забезпечення, націлене спеціально на Україну, здійснило 75% своїх атак проти України, і багато організацій, включаючи державні банки, енергетичні компанії, Інтернет, медіа та комунікаційні мережі, зазнали серйозної шкоди. У СБУ стверджували, що за NotPetya стоїть Росія, але Росія не відреагувала на цю заяву. Вважається, що глобальна шкода, завдана програмним забезпеченням, яке спричиняє великі економічні катастрофи за дуже короткий час, перевищує 10 мільярдів доларів.296

З 2018 року Україна зрозуміла всю серйозність ситуації та почала розвивати кібербезпеку, щоб захистити державні інституції, виділяючи бюджетні кошти. Інвестиції та підтримку були надані українським проектам у сфері кібербезпеки, особливо з боку США. Події продемонстрували важливість міжнародної співпраці та ще раз продемонстрували, що потрібно більше працювати над кібератаками.297

У 2021 році президент Росії Володимир Путін не погодився на зустріч із президентом України Володимиром Зеленським і звинуватив Україну в русофобії, завівши процес у політичний глухий кут, з якого неможливо вийти. Прохання України про безпекову підтримку з боку НАТО, США та Європейського Союзу не сприйняли Росією, і криза поступово наростала. 298 24 лютого 2022 року Росія офіційно почала війну між двома державами збройним нападом під назвою «Військова спецоперація», нехтуючи Мінськими протоколами. Атака, про яку йдеться, була визнана неприйнятною та відкинута ООН і багатьма державами-членами, включаючи Туреччину. 299 У цій війні, яка діє й сьогодні, політика виснаження через кібератаки продовжує посилюватися. На зміну традиційним військовим діям і війнам приходить інформаційна війна.

Завершити нашу тему варто оцінкою того, що сталося між Україною та Росією в рамках кібератак і міжнародного права. Російський лідер Путін і російський уряд базують усі свої нападки на Україну на кількох основних аргументах, позбавлених реальності. Ці заголовки можна підсумувати таким чином:300

– Україна для Росії – проблема збройної агресії.

– Україна вчиняє геноцид на Донбасі.

– В Україні «новий нацистський» режим.

– Україна в історичній перспективі завжди була частиною Росії.

Ці заяви не були сприйняті та засуджені на міжнародній арені. Міжнародне право чітко визначає, що кожна держава є суверенною і має право на самовизначення. З цієї причини втручання в національні рішення та внутрішнє функціонування України є несправедливим і незаконним.

Враховуючи тиск під час виборів 2014 року, атаки на енергетичні системи у 2015 році та інциденти NotPetya у 2017 році, кіберпроблеми викликали багато занепокоєнь і призвели до багатьох дискусій у міжнародному праві. Хоча поріг для розгляду кібератак як застосування сили ще не повністю зрозумілий, стало важливим чітко та зрозуміло представити порушення понять порушення суверенітету та заборони втручання та детально оцінити цю ситуацію.

За словами Шмітта, багато держав не розглядають кібератаки як акт застосування сили, якщо вони не завдають фізичної шкоди чи збитку. Якщо оцінювати відповідальність за кібератаки, то широко визнається, що згадані кібератаки відбулися через Росію або підтримувані Росією кібергрупи, але питання конкретного приписування залишається суперечливим. Враховуючи критерії інтенсивності та впливу на першому етапі, видається можливим, що заборона втручання може бути порушена, а не застосована сила. Однак перед обличчям збройних атак не слід ігнорувати опорну структуру кібератак. Подібну логіку можна встановити для права на самозахист. Зрештою, щоб говорити про все це, не слід забувати, що атаки, про які йдеться, мають бути

конкретно приписані Росії. Заборона застосування сили є принципом міжнародного права, який поширюється лише на держави. З цієї причини кібератаки, здійснені недержавними акторами, не матимуть наслідків на міжнародній арені, навіть якщо вони порушують національне законодавство. Проблеми, про які йде мова, продовжують залишатися загадковими та невизначеними через природу кіберпростору.301

Зрештою, якщо припустити, що поточна ситуація відповідає умовам обвинувачення, і коли оцінити всі дії проти України разом, можна стверджувати, що поріг застосування сили перевищено і з'явилося право на самозахист. Кібератаками, які вона особисто проводить і підтримує, Росія показала громадськості, що вона експерт у цій галузі та може становити міжнародну загрозу. Росія, яка постійно вдосконалює себе в кіберстратегіях, здійснювала кібератаки лише у випадку з Естонією, і використовувала кібератаки для підтримки військових дій у випадку з Грузією. У випадку з Україною вона застосувала кібератаки в середовищі гібридної війни та втягнула Україну в громадянську війну, анексувавши Крим, який був її стратегічною ціллю, і повернула процес собі на користь. По суті, позиція Криму в транспортуванні нафти і природного газу та економічних відносинах в європейському регіоні має беззаперечну цінність.

Вороже ставлення та дії Росії мають різні наслідки для міжнародного права в багатьох аспектах. З 2014 року до сьогодні Росія порушила багато фундаментальних принципів, знехтувала суверенітетом держави, порушила заборону на втручання та перевищила поріг застосування сили. Проте з 2022 року вона розпочала атаку шляхом прямої військової операції, і зараз цей процес переріс в окрему ситуацію, коли мають застосовуватися норми міжнародного гуманітарного права та права збройних конфліктів. Важливо нагадати, що всі держави є суб'єктами міжнародного права, і ці правила будуть застосовуватися й надалі у світлі конкретних подій.

ВИСНОВКИ

Суверенітет постає як поняття, яке було предметом різноманітних дискусій з моменту його появи до сьогодні та залишається на порядку денному. Суверенітет може бути порушений діями, вжитими державами або приписуваними їм. Однак існує ймовірність того, що недержавні актори та особисті дії також можуть завдати шкоди суверенітету. Хоча здійснення юрисдикції проти недержавних суб’єктів та окремих осіб є одним із найважливіших прав держав, норми міжнародного права також повинні поважатися. Кіберпростір, кібербезпека та кібератаки є однією з нових тем для обговорення цього питання.

Кібератаки є новою вразливістю безпеки, яка може загрожувати суверенітету держав і викликати проблеми в міжнародному праві. Кібератаки можуть здійснюватися багатьма методами та акторами в межах кіберпростору, і держави стикаються з загрозою через анонімні та транскордонні технології. Поки держави не підпорядковують цю сферу обов'язковим нормам у рамках звичайних міжнародних правил і угод, існуючі правила повинні застосовуватися до конкретних подій. Тут на перший план виходять питання втручання у внутрішні справи та заборони застосування сили.

Той факт, що кіберзагрози досягають рівня кібератак, є першим кроком дій, які можуть спричинити серйозні проблеми з технологічним розвитком. Для того, щоб держави використовували свої повноваження проти кіберзагроз, достатньо, щоб особа або особи, які діють у кіберпросторі, перебували в межах національної юрисдикції відповідної держави. У деяких випадках можуть існувати загрози, які виходять за межі юрисдикції, і стає важливим застосовувати норми міжнародного права. У цьому випадку важлива природа кібератак, правила і принципи, які вони порушують, і кожен конкретний інцидент потрібно оцінювати окремо.

У рамках положень статей 2/1, 2/4 і 2/7 Статуту ООН підкреслюється принцип суверенної рівності держав, забороняється застосування сили або загроза силою, а також принцип невтручання у внутрішні справи держав. Одним із винятків із застосування сили є право на самооборону, закріплене в статті 51 Статуту ООН.

Оцінка кібератак у рамках суверенітету, принципу невтручання у внутрішні справи, заборони втручання, заборони застосування сили та права на самооборону вперше була винесена на порядок денний у Талліннському посібнику. . У цьому контексті, якщо буде доведено вагомі докази того, що кібератака була здійснена державами та перевищено поріг збройних сил, заборона на застосування сили буде порушена. Залежно від тяжкості нападу та того, чи відповідає він критеріям Шмітта, право атакованої держави на самозахист також може вийти на перший план.

Переважна точка зору в міжнародному праві полягає в тому, що відповідно до положення статті 2/4 Статуту ООН і звичаю дії «застосування сили» мають нижчий поріг, ніж дії «збройного нападу». Усі збройні напади є застосуванням сили, але навпаки не буде. Згідно з висновками Міжнародної групи експертів у рамках Талліннського посібника, неможливо провести чітке розмежування щодо порушення відповідних фундаментальних принципів у кіберпросторі, і важливою стала оцінка конкретних подій.

Відповідно до Міжнародної групи експертів, яка підготувала Талліннський посібник, було одностайно погоджено, що перевищення порогу збройного нападу може бути достатнім для кібероперацій, особливо у випадках, коли вони завдають серйозних травм або фізичної шкоди. Деякі члени групи пішли далі, зосередившись на серйозності заподіяної шкоди, а не на її характері.

Можна описати кібероперації, які призводять до економічного колапсу держави і не є достатньо серйозними, шкідливими чи руйнівними, як збройний напад. У цьому контексті, якщо кібератаки завдають шкоди, еквівалентної іншому акту застосування сили, заборона на застосування сили

буде порушена, і держави можуть вдатися до примусових контрзаходів. Якщо кібератака відповідає умовам збройного нападу, для ліквідації атаки може бути використано право на самозахист. У цьому випадку держави матимуть право відповісти традиційними або кіберметодами, дотримуючись принципу пропорційності права на самозахист.

Держави, як правило, не здійснюють відкрито кібератаки та намагаються приховати джерело атак за допомогою недержавних суб'єктів чи технічних засобів. Тому для того, щоб діяльність держав щодо кібератак оцінювалася в рамках заборони на застосування сили, має бути доведено, що атака була здійснена прямо чи опосередковано цією державою. Не слід забувати, що через анонімний характер кібератак процес приписування атаки державі пов'язаний з різними труднощами.

Слід зазначити, що державам може знадобитися багато часу для досягнення консенсусу при збереженні балансу сил на міжнародній арені та спільних інтересів світу. У цьому процесі слід розвивати практику, пов'язану з кіберпростором, відповідно до національних норм і основних норм міжнародного права, а також слід запобігати великомасштабним руйнуванням. Власне кажучи, не слід забувати, що якщо поріг збройного нападу щодо заборони застосування сили взаємно перевищено державами, норми міжнародного гуманітарного права та права збройних конфліктів можуть знайти застосування.

Як видно з прикладів, які траплялися в минулому і які все ще є ефективними сьогодні, кібератаки можуть завдати великих руйнувань, якщо вони підкріплені стратегічними ідеями. Щоб уникнути більших проблем у майбутньому, у міжнародному праві мають бути встановлені правила стримування щодо сфери кіберпростору та вжиті необхідні заходи для забезпечення дотримання державами цих правил. Слід підкреслити, що міжнародне співробітництво є наріжним каменем, який зберігає застосовність міжнародного права. Якщо держави не зроблять реальних кроків для співпраці, міжнародне право втрачає свою силу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 12 Ağustos 1949 Tarihli Cenevre Sözleşmeleri ve Ek Protokolleri, (Yayına Hazırlayanlar: Melike Batur Yamaner, A. Emre Öktem, Bleda Kurtdarcan, Mehmet C. Uzun), Galatasaray Üniversitesi Yayınları, İstanbul, 2008.
2. Ada, Mehmet ve Hüseyin Çakır. "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, Cilt:5, Sayı:2, 2017, ss. 632-656.
3. Ahronheim, Anna. "Liberman: Squabbling over credit for strike on Syrian reactor an 'embarrassment'", The Jerusalem Post, https://www.jpost.com/Israel-News/Liberman-praises-Israels-strike-on-Syrian-reactor-Livni-recalls-events-546640 (02.07.2023).
4. Akın, Murat ve Şeref Sağıroğlu. "Gelişmiş Sürekli Tehditler", Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, Cilt:10, Sayı:1, 2017, ss. 1-10.
5. Akman, Toygar. Sibernetik "Dünü Bugünü Yarını", Kaknüs Yayınları, İstanbul, 2003.
6. Anand, R. P.. "Sovereign Equality of States in International Law", International Studies, Cilt:8, Sayı:3, 1966, ss. 213-241.
7. Andress, Jason ve Steve Winterfeld. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Second Edition, Elsevier Inc., 2014.
8. Arasan, Murat Can. Uluslararası Hukukta Devletlerin Egemen Eşitliği İlkesi, (Yayınlanmamış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2017.
9. Ataş, İsmail. Otonom Silah Sistemlerinin ve Siber Saldırıların Uluslararası İnsancıl Hukukun Temel Prensiplerine Uygunluğu, Adalet Yayınevi, Ankara, 2023.
10. Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi. RG 09.08.2014, Sayı:29083.
11. Bağcı, Hasan. "Sosyal Mühendislik ve Denetim", Denetişim, Sayı:1, 2009, ss. 42-51.

12. Bal, Ali. Devletin Uluslararası Sorumluluğunun Doğması, (Yayınlanmamış Yüksek Lisans Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, 2006.
13. Balık, Gürcan. "Anayasa'da "Milletlerarası Hukukun Meşru Saydığı Haller" Sorunu", Uluslararası İlişkiler Dergisi, Cilt:12, Sayı:47, 2015, ss. 47-71.
14. Bass, Warren. A Surprise Out of Zion?, RAND Corporation, Santa Monica, 2015.
15. Benedikt, Michael. "Cyberspace: Some Proposals", Cyberspace: First Steps, Ed. Michael Benedikt, 3. Baskı, MIT Press, London, 1992, ss. 119-224.
16. Beriş, H. Emrah. "Egemenlik Kavramının Tarihsel Gelişimi ve Geleceği Üzerine Bir Değerlendirme", Ankara Üniversitesi SBF Dergisi, Cilt:63, Sayı:1, 2008, ss. 55-80.
17. Bıçakcı, Salih. "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", Uluslararası İlişkiler, Cilt:10, Sayı:40, 2014, ss. 101-130.
18. Bıçakçı, Salih. "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", Uluslararası İlişkiler, Cilt:9, Sayı:34, 2012, ss. 205-226.
19. Bilen, Abdulkadir. Akıllı Yöntemler ile Siber Saldırı Tespit Sistemi Geliştirilmesi, (Yayınlanmamış Yüksek Lisans Tezi), Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ, 2021.
20. Birleşmiş Milletler Andlaşması. RG 24.08.1945, Sayı:6092.
21. Bodin, Jean. On Sovereignty: Four chapters from The Six Books of the Commonwealth, Ed. ve Çev. Julian H. Franklin, Cambridge University Press, United Kingdom, 1992.
22. Bolat, Can. Siber Saldırılara Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2020.
23. Buchan, Russell. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", Journal of Conflict & Security Law, Cilt:17, Sayı:2, 2012, s. 211-227.

24. Buyuran, Abdullah Ahmet. Devlet Başarısızlığı, Egemen Eşitlik ve Uluslararası Hukukta Müdahale, (Yayınlanmamış Doktora Tezi), Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, İstanbul, 2023.
25. Carr, Jeffrey. Inside Cyber Warfare: Mapping the Cyber Underworld, O'Reilly Media, 2012.
26. Cerf, Vinton G. ve Robert E. Kahn. "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Cilt:22, Sayı:5, 1974, ss. 637-648.
27. Choucri, Nazli. Cyberpolitics in International Relations, MIT Press, London, 2012.
28. Cin, Gökhan ve Hasan Hüseyin Tekin. "Rusya'nın Hibrit Savaş Kapasitesinin Kırım ve Donbas Vakaları Üzerinden Analizi", Güvenlik Stratejileri Dergisi, Cilt:17, Sayı:37, 2021, ss. 203-246.
29. Civelek, Mustafa Emre. İnternet Çağı Dinamikleri, Beta Yayıncılık, İstanbul, 2009.
30. Clark, David D. ve Susan Landau. "Untangling Attribution", Harvard National Security Journal, Cilt:2, Sayı:2, 2011, ss. 323-352.
31. Clark, David. "Characterizing Cyberspace: Past, Present and Future", MIT CSAIL, Version 1.2, 2010.
32. Clarke, Richard A. ve Robert K. Kanke. Siber Savaş (Cyber War), Çev. Murat Erduran, İstanbul Kültür Üniversitesi Yayınları, 2011.
33. Coburn, Andrew, Éireann Leverett ve Gordon Woo. Solving Cyber Risk: Protecting Your Company and Society, Wiley, New Jersey, 2019.
34. Cohen-Almagor, Raphael. "Internet History", International Journal of Technoethics, Cilt:2, Sayı:2, 2011, ss. 45-64.
35. Collins, Sean ve Stephen McCombie. "Stuxnet: The Emergence of A New Cyber Weapon and Its Implications", Journal of Policing, Intelligence and Counter Terrorism, Cilt:7, Sayı:1, 2012, ss. 80-91.

36. Çakmak, Cenap. Uluslararası Hukuk: Giriş, Teori ve Uygulama, Ekin Yayınevi, Bursa, 2014.
37. Çelik, Soner ve Barış Çeliktaş. "Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar", Cyberpolitik Journal, Cilt:3, Sayı:5, 2018, ss. 105-132.
38. Çelik, Şener. "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1, 2013, ss. 137-175.
39. Çırak, Bekir ve Abdülkadir Yörük. "Mekatronik Biliminin Öncüsü İsmail El - Cezeri", Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı:4, 2015, ss. 175-194.
40. Çifci, Hasan. Her Yönüyle Siber Savaş, 2. Basım, TÜBİTAK Yayınları, Ankara, 2017.
41. Çölgeçen, Mutlu. Siber Savaş: Kıyametin İlk Halkası, Arşiv Kitapları, Ankara, 2002.
42. Darıcılı, A. Burak. "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi", U. Ü. Sosyal Bilimler Enstitüsü Dergisi, Cilt:7, Sayı:2, 2014, ss. 1-16.
43. Delerue, François. Cyber Operations and International Law, Cambridge University Press, United Kingdom, 2020.
44. DeSimone, Antonio ve Nicholas Horton. Sony's Nightmare Before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace, The Johns Hopkins University Applied Physics Laboratory LLC, Laurel, 2017.
45. Dinstein, Yoram. War, Aggression and Self-Defence, 4. Baskı, Cambridge University Press, United Kingdom, 2005.
46. DOD Dictionary of Military and Associated Terms.
47. Dörr, Oliver ve Kirsten Schmalenbach (Ed.). Vienna Convention on the Law of Treaties: A Commentary, 2. Baskı, Springer, Germany, 2018.

48. Durmaz, Didem. “İnsancıl Hukukun Orantılılık İlkesi Çerçevesinde Tali Hasar Doktrinine Genel Bir Bakış”, Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, Cilt:10, Sayı:20, 2022, ss. 213-238.
49. Emir, Buğrahan. Uluslararası İlişkilerin Kuramsal Çerçevesi ve Siber Güvenlik Kavramının Analizi, (Yayınlanmamış Yüksek Lisans Tezi), Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Trabzon, 2020.
50. Endicott, Timothy. “The Logic of Freedom and Power”, The Philosophy of International Law, Ed. Samantha Besson ve John Tasioulas, Oxford University Press, Oxford, 2010, ss. 245-260.
51. Erdem, Tolga. 21. Yüzyılda Uluslararası İlişkilerde Yeni Güç Rekabet Sahası: Siber Uzay, (Yayınlanmamış Doktora Tezi), Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Edirne, 2020.
52. Ereker, Fulya A.. “İlkçağlardan Günümüze Haklı Savaş Kavramı, Uluslararası İlişkiler Dergisi, Cilt:1, Sayı:3, 2004, ss. 1-36.
53. Eren, M. Yusuf. “Uluslararası Hukukta Savaşa Varmayan Kuvvet Kullanma Yolları”, İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt:3, Sayı:2, 2012, ss. 229-259.
54. Erkiner, Hakkı Hakan. “Rusya-Ukrayna Savaşı Dairesinde Uluslararası Hukuk Meseleleri”, Uluslararası Akdeniz Hukuku Kongresi 2022: Akdeniz Üniversitesi Hukuk Fakültesi’nin Kuruluşunun 30. Yılı Anısına, Adalet Yayınevi, Ankara, 2022, ss. 347-398.
55. FBI National Press Office. Update on Sony Investigation, 2014, https://www.fbi.gov/news/press-releases/update-on-sony-investigation (08.09.2023).
56. Garber, Lee. “Melissa Virus Creates a New Type of Threat”, Computer, Cilt:32, Sayı:6, 1999, ss. 16-19.
57. Geers, Kenneth. “Russian Introduction: Cyber War in Perspective”, Cyber War in Perspective: Russian Aggression against Ukraine, Ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn, 2015, ss. 13-18.
58. Geray, Haluk. İletişim ve Teknoloji, Ütopya Yayınları, Ankara, 2002.

59. Gibson, William. Burning Chrome, Yeniden Baskı, HarperCollins Publishers, Scotland, 2003.
60. Gibson, William. Neuromancer, Elektronik Baskı, ACE Books by ACE Publishing Group – Penguin Putnam Inc., Newyork, 2003.
61. Goodman, Marc. Future Crimes, Penguin Random House, London, Great Britain, 2015.
62. Graham, James Richard Howard ve Ryan Olson (Ed.). Cyber Security Essentials, CRC Press, 2011.
63. Green, James. The International Court of Justice and Self-Defence in International Law, Hart Publishing, Oregon, 2009, s. 61.
64. Gündüz, Aslan. Milletlerarası Hukuk, Ed. Reşat Volkan Günel, 11. Baskı, Savaş Yayınevi, Ankara, 2021.
65. Güneş, Mustafa ve Ahmet Alabacak. "Bilgisayar Virüsleri", D.E.Ü. İ.İ.B.F. Dergisi, Cilt:11, Sayı:2, 1996, ss. 239-248.
66. Güntay, Vahit. "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", Güvenlik Stratejileri Dergisi, Cilt:14, Sayı:27, 2018, ss. 79-113.
67. Güreşci, Ramazan. "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi", Savunma Bilimleri Dergisi, Cilt:18, Sayı:1, 2019, ss. 75-98.
68. Güven, Ferit. Siber Saldırılar ve Türk Kamu Yönetiminin Çözümleri, (Yayınlanmamış Doktora Tezi), Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, 2022.
69. Haggard, Stephan ve Jon R. Lindsay. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace", Asia Pacific Issues, Sayı:117, 2015, ss. 1-8.
70. Hearn, Kay, Patricia A. H. Williams ve Rachel J. Mahncke. "International Relations and Cyber Attacks: Official and Unofficial Discourse", 11th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 2010, ss. 7-12.

71. Hemsley, Kevin ve Ronald Fisher. “A History of Cyber Incidents and Threats Involving Industrial Control Systems”, 12. International Conference on Critical Infrastructure Protection (ICCIP), 2018, ss. 215-242.
72. Herzog, Stephen. “Ten Years After the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity”, Georgetown Journal of International Affairs, Cilt:18, Sayı:3, 2017, ss. 67-78.
73. Hobbes, Thomas. Leviathan, Çev. Semih Lim, 6. Baskı, Yapı Kredi Yayınları, İstanbul, 2007.
74. Hollis, Duncan B.. “An e-SOS for Cyberspace”, Harvard International Law Journal, Cilt:52, Sayı:2, 2011, ss. 373-432.
75. Independent International Fact-Finding Mission on the Conflict in Georgia, Report, Volume II, 2009, https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf (03.09.2023).
76. International Committee of the Red Cross. International Humanitarian Law: Answers to your Questions, ICRC Press, Switzerland, 2023.
77. International Committee of the Red Cross. The Geneva Conventions of 12 August 1949, https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf (03.02.2024).
78. International Law Commision. Responsibility of States for Internationally Wrongful Acts, A/56/49, 2001, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (11.01.2022).
79. Jaitner, Margarita Levin. “Russian Information Warfare: Lessons from Ukraine”, Cyber War in Perspective: Russian Aggression against Ukraine, Ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn, 2015, ss. 87-94.
80. Jensen, Eric Talbot. “The Tallinn Manual 2.0: Highlights and Insights”, Georgetown Journal of International Law, Cilt:48, 2017, ss. 735-778.

81. Kafadar, Muhammed Fatih. “Uluslararası Hukukta Devletlerin Sorumluluğu Bağlamında Siber Saldırıların Atfedilebilirliği Meselesi”, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Sayı:2, 2020, ss. 1027-1054.
82. Kanburoğlu, Ömer Lütfi. “Önleyici Harekât Stratejileri ve ABD”, 2012, http://www.kanburoglu.com/makale153.htm (05.01.2022).
83. Kara, Mahruze. Siber Saldırılar – Siber Savaşlar ve Etkileri, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013.
84. Karagiannis, Emmanuel. “The 2008 Russian-Georgian War via the Lens of Offensive Realism”, European Security, Cilt:22, 2013, ss. 74-93.
85. Keleştemur, Saim Atalay. Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Gedik Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018.
86. Kılınç, Doğan. “Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt:14, Sayı:2, 2010, ss. 407-454.
87. Klimburg, Alexander. “Mobilising Cyber Power”, Survival, Cilt:53, Sayı:1, 2011, ss.41-60.
88. Knapp, Eric D. ve Joel Thomas Langill. Industrial Network Security, Second Edition, Elsevier Inc., Waltham, 2015.
89. Kocabay, Hüseyin. Uluslararası Hukukta Kuvvet Kullanımı, (Yayınlanmamış Yüksek Lisans Tezi), Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü, Bolu, 2014.
90. Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva ve Jenny Oberholtzer. Lessons from Russia’s Operations in Crimea and Eastern Ukraine, RAND Corporation, California, 2017.
91. Korhan, Sevda. “Siber Uzayda Aktör - Güç İlişkisi”, Cyberpolitik Journal, Cilt:2, Sayı:4, 2018, ss. 75-103 (Aktör - Güç İlişkisi).

92. Korhan, Sevda. Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri, (Yayınlanmamış Yüksek Lisans Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018 (Parametreler).
93. Krishna-Hensel, Sai Felicia. "Preface", Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, Ed. Myriam Dunn Cavelty, Victor Mauer ve Sai Felicia Krishna-Hensel, Ashgate Publishing, 2007, ss. ix-xiv.
94. Lakomy, Miron. "The Significance of Cyberspace in Canadian Security Policy", Central European Journal of International and Security Studies, Cilt:7, Sayı:2, 2013, ss. 102-119.
95. League of Nations. General Treaty for Renunciation of War as an Instrument of National Policy, 1929, https://treaties.un.org/doc/Publication/UNTS/LON/Volume%2094/v94.pdf (12.10.2023).
96. Léonet, Louis. Contextual Cyber Securitisation: A Case Study of Russian Cyberattacks against Ukraine, (Yayınlanmamış Yüksek Lisans Tezi), Leiden Üniversitesi, Hollanda.
97. Li, Sheng. "When Does Internet Denial Trigger the Right of Armed Self-Defense?", Yale Journal of International Law, Sayı:38, 2013, ss. 179-216.
98. Libicki, Martin C.. Cyberdeterrence and Cyberwar, RAND Corporation, Santa Monica, 2009.
99. Mandel, Robert. Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks, Georgetown University Press, Washington, 2017.
100. Mares, Miroslav ve Veronika Netolicka. "Georgia 2008: Conflict Dynamics in the Cyber Domain, Strategic Analysis, Cilt:44, 2020, ss. 224-240.

101. Markoff, John. “A Silent Attack but Not a Subtle One”, The New York Times, 2010, https://www.nytimes.com/2010/09/27/technology/27virus.html (28.12.2022).
102. Medvedev, Sergei A.. Offense–Defense Theory Analysis of Russian Cyber Capability, Calhoun: The Naval Postgraduate School (NPS) Institutional Archive, California, 2015.
103. Moynihan, Harriet. “The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention”, Chatham House, 2019, ss. 1-60.
104. Mumcu, Şinasi Özgür. “Barış Zamanı Siber Operasyonların Egemenlik İlkesi Bakımından Hukuki Rejimi”, Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi, Cilt:16, Sayı:201-202, 2021, ss. 995-1012.
105. Nguyen, Reese. “Navigating Jus Ad Bellum in the Age of Cyber Warfare”, California Law Review, Cilt:101, Sayı:4, 2013, ss. 1079-1130.
106. Nourian, Arash ve Stuart Madnick. “A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet”, IEEE Transactions on Dependable and Secure Computing, Cilt:15, Sayı:1, 2018, ss. 2-13.
107. Orallı, Levent Ersin. “Uluslararası Hukukta Ve BM Sisteminde Askeri Müdahale Olgusu”, Tesam Akademi Dergisi, Cilt:1, Sayı:1, 2014, ss. 102-127.
108. OSCE. Комплекс мер по выполнению Минских соглашений, Minsk, 2015, https://www.osce.org/ru/cio/140221 (12.10.2023).
109. OSCE. Протокол о результатах консультаций Трехсторонней контактной группы, Минск, 5 сентября 2014 г., Minsk, 2014, https://www.osce.org/ru/home/123258 (12.10.2023).
110. Ottis, Rain. “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, Reading: Academic Publishing Limited, 2008, ss. 163-168.

111. Ottis, Rain. “Proactive Defense Tactics Against On-Line Cyber Militia”, Proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010), 2010, ss. 233-237.
112. Owolabi, Kudirat Magaji W.. “The Principle of The Common Heritage of Mankind”, Nnamdi Azikiwe University Journal of International Law and Jurisprudence, Cilt:4, 2013, ss. 51-56.
113. Öğün, Mehmet Nesip ve Adem Kaya. “Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler”, Güvenlik Stratejileri Dergisi, Y. 9, Sayı:18, 2013, ss. 145-181.
114. Özman, M. Aydoğan. “Devletlerin Egemenliği ve Milletlerarası Teşekküller”, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt:21, Sayı:1, 1964, ss. 53-121.
115. Pazarcı, Hüseyin. Uluslararası Hukuk, 15. Baskı, Turhan Kitabevi, Ankara, 2016.
116. Polat, Doğan Şafak. “Nato’nun Yeni Operasyon Alanı: Siber Uzay”, Güvenlik Bilimleri Dergisi, UGK Özel Sayısı, 2020, ss. 135-158.
117. Richet, Jean-Loup. Cybersecurity Policies and Strategies for Cyberwarfare Prevention, Information Science Reference, Pennsylvania, 2015.
118. Roscini, Marco. “Cyber Operations as a Use of Force”, Research Handbook on International Law and Cyberspace, Ed. Nicholas Tsagourias and Russell Buchan, Edward Elgar Publishing, United Kingdom, 2015, ss. 233-254.
119. Rousseau, Jean-Jacques. Toplum Sözleşmesi, Çev. Vedat Günyol, 9. Basım, Türkiye İş Bankası Kültür Yayınları, İstanbul, 2012.
120. Schmitt, Michael N. ve Liis Vihul. “Respect for Sovereignty in Cyberspace”, Texas Law Review, Cilt:95, Sayı:7, 2017, ss. 1639-1671.
121. Schmitt, Michael N.. “Russian Cyber Operations And Ukraine: The Legal Framework”, Lieber Institute West Point, 2022,

https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/ (09.10.2023).

122. Schmitt, Michael N.. “The Law of Cyber Warfare: Quo vadis?”, Stanford Law & Policy Review, Sayı:25, 2014, ss. 269-300.

123. Schmitt, Michael N.. Computer Network Attack and The Use of Force in International Law: Thoughts on A Normative Framework, Research Publication 1 Information Series, Institute for Information Technology Applications, USAF Academy, Colorado, 1999.

124. Schmitt, Michael. “International Law and Cyber Attacks: Sony v. North Korea”, Just Security, 2014, https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (08.09.2023).

125. Sertçelik, Aşır. “Siber Olaylar Ekseninde Siber Güvenliği Anlamak”, Medeniyet Araştırmaları Dergisi, Cilt:2, Sayı:3, 2015, ss. 25-42.

126. Shanghai Cooperation Organization. Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, 2009.

127. Shanghai Cooperation Organization. Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, ANNEX 1 to the Agreement on Cooperation in the

128. Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization, ss. 9-10, 2009. (ANNEX 1).

129. Sharp, Walter Gary. “The Past, Present, and Future of Cybersecurity”, Journal Of National Security Law & Policy, Cilt:4, Sayı:13, 2010, ss. 13-26.

130. Shaw, Malcolm N.. International Law, 8. Baskı, Cambridge University Press, United Kingdom, 2017.

131. Sigholm, Johan. “Non-State Actors in Cyberspace Operations”, Journal of Military Studies, Cilt:4, Sayı:1, 2016, ss. 1-37.

132. Slevin, James. The Internet and Society, Polity Press, Oxford, 2000.
133. Springer, Paul J.. Encyclopedia of Cyber Warfare, ABC-CLIO, California, 2017.
134. Steed, Brian L.. Piercing the Fog of War: Recognizing Change on the Battlefield: Lessons from Military History 216 BC through Today, Zenith Press, Mineneapolis, 2009.
135. Stinissen, Jan. "A Legal Framework for Cyber Operations in Ukraine", Cyber War in Perspective: Russian Aggression against Ukraine, Ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn, 2015, ss. 123-134.
136. Sullivan, Clare. "The 2014 Sony Hack and the Role of International Law", Journal of National Security Law & Policy, Sayı:8, 2016, ss. 437-468.
137. Sur, Melda. Uluslararası Hukukun Esasları, 15. Baskı, Beta Yayıncılık, İstanbul, 2021.
138. Süleymanova Rafael, Günay. A Comparative Analysis of Major Russian Cyber Attacks in the Post-Cold War Era, (Yayınlanmamış Yüksek Lisans Tezi), Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul, 2022.
139. Şafak, Erdi. "Uluslararası Hukukta Değişen Güvenlik Algısı Ve Saldırı Suçu Bağlamında Siber Saldırılar", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt:28, Sayı:1, 2020, ss. 127-160.
140. T. C. Dışişleri Bakanlığı. Şanhay İşbirliği Örgütü (ŞİÖ), https://www.mfa.gov.tr/sanghay-isbirligi-orgutu.tr.mfa, (02.12.2021).
141. T.C. Dışişleri Bakanlığı. 24 Şubat 2022, Rusya Federasyonu Tarafından Ukrayna'ya Yönelik Başlatılan Askeri Operasyon Hk., 62 Numaralı Resmî Açıklama, Ankara, 2022.
142. T.C. Ulaştırma ve Altyapı Bakanlığı. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, Ankara, 2020.
143. Tabansky, Lior ve Isaac Ben Israel. Cybersecurity in Israel, Springer, Switzerland, 2015.

144. Taşdemir, Fatma. “Uluslararası Anarşiye Giden Yol: Uluslararası Hukuk Açısından Önleyici Meşru Müdafaa Hakkı”, Uluslararası Hukuk ve Politika Dergisi, Cilt:2, Sayı:5, 2006, ss. 75-89.

145. Tezcan, Durmuş. “Bozkurt-Lotus Davasının Uluslararası Hukuktaki Önemi ve Yeri, Çağdaş Türkiye Tarihi Araştırmaları Dergisi, Cilt:2, Sayı:4, 1994, ss. 267-274.

146. The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Ed. Michael N. Schmitt ve Liis Vihul, 2. Baskı, Cambridge University Press, 2017 (Tallinn Kılavuzu).

147. The United States Army’s. Cyberspace Operations Concept Capability Plan 2016- 2028, United States, 2010.

148. Thornburgh, Tim. “Social Engineering: The “Dark Art””, 1st Annual Conference on Information Security Curriculum Development, 2004, ss. 133-135.

149. Tikk, Eneken, Kadri Kaska ve Liis Vihul. International Cyber Incidents: Legal Considerations, Cooperative Cyber Defense Centre of Excellence, Tallinn, 2010.

150. Tokdaş, Abdullah. Siber Güvenlik ve Uluslararası İlişkiler, (Yayınlanmamış Yüksek Lisans Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018.

151. Trautman, Lawrence J. ve Peter C. Ormerod. “Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things”, University of Miami Law Review, Cilt:72, Sayı:3, 2018, ss. 761-826.

152. Tsagourias, Nicolas. “The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II - The Use of Force”, Yearbook of International Humanitarian Law, Ed. Terry D Gill, Cilt:15, 2014, ss. 19-43.

153. Uluslararası Adalet Divanı, Kongo Demokratik Cumhuriyeti'ndeki Silahlı Faaliyetler Davası, 2005, https://www.icj-cij.org/public/files/case-related/116/116-20051219-JUD-01-00-EN.pdf (03.12.2023).

154. Uluslararası Adalet Divanı, Nükleer Silah Tehdidinin veya Kullanımının Yasallığı Hakkında Danışma Görüşü, 1996, https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (10.01.2022).

155. Uluslararası Adalet Divanı. Korfu Boğazı Davası, 1949, (Korfu Boğazı Kararı)https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf (05.01.2022).

156. Uluslararası Adalet Divanı. Nikaragua'ya Karşı Askeri ve Bölgesel Faaliyetler Davası, 1986, (Nikaragua Kararı), https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (31.12.2021).

157. United Nations General Assembly Security Council. Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations addressed to the Secretary-General, A/68/934–S/2014/451, 2014.

158. United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 2015, s. 12, https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf (11.01.2022).

159. United Nations General Assembly. Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 2625(XXV), 1970, https://digitallibrary.un.org/record/202170/files/A_RES_2625%28XXV%29-EN.pdf (31.12.2021).

160. United Nations General Assembly. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, 2131(XX), 1965, https://digitallibrary.un.org/record/203886/files/A_RES_2131%28XX%29-EN.pdf (31.12.2021).

161. United Nations General Assembly. Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, 36/103, 1981, https://digitallibrary.un.org/record/27066/files/A_RES_36_103-EN.pdf (31.12.2021).

162. United Nations General Assembly. Definition of Aggression, 3314(XXIX), 1974, https://digitallibrary.un.org/record/190983/files/A_RES_3314%28XXIX%29-EN.pdf (05.01.2022).

163. United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 2013, s. 8, https://digitallibrary.un.org/record/753055/files/A_68_98-EN.pdf (31.12.2021).

164. United Nations General Assembly. Territorial integrity of Ukraine, 68/262, 2014, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/455/17/PDF/N1345517.pdf?OpenElement (03.10.2023).

165. United Nations. Summaries of Judgments, Advisory Opinions and Orders of the Permanent Court of International Justice, 2012, (USAD Kararları), https://legal.un.org/PCIJsummaries/documents/english/PCIJ_FinalText.pdf (03.12.2023).

166. United Nations. United Nations Charter, https://www.un.org/en/about-us/un-charter/full-text (03.12.2023).

167. Uzun, Elif. “Haklı Savaş Düşüncesinin Batılı Kökleri: İlk Çağlardan Yirminci Yüzyıla Jus Ad Bellum Kavramı”, Uluslararası Hukuk ve Politika Dergisi, Cilt:6, Sayı:21, 2010, ss. 19-33.
168. Weimann, Gabriel. “Cyberterrorism: How Real is the Threat?” United States Institute of Peace, Special Report 119, 2004, ss. 1-12.
169. Whyte, Christopher ve Brian Mazanec. Understanding Cyber Warfare: Politics, Policy and Strategy, Routledge, New York, 2018.
170. Wiener, Norbert. Cybernetics or Control and Communication in the Animal and Machine, 2. Baskı, MIT Press, London, 2019.
171. Williams, Martyn. “Analysis: Why North Korea might not be to blame for the Sony Pictures hack”, The Guardian, https://www.theguardian.com/world/2014/dec/02/-sp-north-korea-hack-sony (08.09.2023).
172. Wilson, Clay. “Cyber Crime”, Cyberpower and National Security, (Ed. Franklin D. Kramer, Stuart H. Starr ve Larry Wentz), National Defense University Press, Washington, 2009, ss. 415-437.
173. Yaşın, Abdullah. “Ebul-İz’in Bilime Katkıları”, Bilim Düşünce ve Sanatta Cizre (Uluslararası Bilim Düşünce ve Sanatta Cizre Sempozyumu Bildirileri), 2012, ss. 201-204.
174. Yayla, Mehmet. “Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı”, Hacettepe Hukuk Fakültesi Dergisi, Cilt:4, Sayı:2, 2014, ss. 181-200.
175. Yayla, Mehmet. “Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma”, Türkiye Barolar Birliği Dergisi, Sayı:107, 2013, ss. 199-220.
176. Yazıcı, Merve. “İlk Modern Siber-Atak: Estonya, TUİÇ Akademi, 2015, https://www.tuicakademi.org/ilk-modern-siber-atak-estonya (27.12.2022).
177. Yener, Yavuz. “8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış”, SiberBülten, 2014, https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis (27.12.2022).

178. Yılmaz, Yağmur Ekim. “Milletlerarası Hukukta Kuvvet Kullanma Yasağı Kapsamında Rusya’nın Ukrayna’ya Müdahalesi”, Uluslararası İlişkiler ve Diplomasi Dergisi, Cilt:5, Sayı:2, 2022, ss. 58-80.