КИЇВСЬКИЙ УНІВЕРСИТЕТ ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ

Кафедра міжнародного та приватного права

КВАЛІФІКАЦІЙНА РОБОТА

за темою:

«Кібероборона в міжнародному праві»

Виконав:
здобувач 2 курсу, групи ММ-21д
спеціальності 293 «Міжнародне право»
Морозов Анатолій Адольфович
(П.І.Б. здобувача)

Науковий керівник:
Пилипенко Володимир Пилипович
доктор юридичних наук, доцент, доцент
кафедри міжнародного та приватного права
(П.І.Б., науковий ступінь, вчене звання, посада)

Робота допущена до захисту в ЕК
«__» _____ 20____ р.

В.о. завідувача кафедри Чернега В.М.
доктор юридичних наук, професор
(П.І.Б., науковий ступінь, вчене звання, посада)

КИЇВ-2026

Анотація

Морозов А.А. Кібероборона в міжнародному праві

Кваліфікаційна робота складається зі вступу, трьох розділів (шести підрозділів), висновків, списку використаних джерел (144 найменування). Загальний обсяг роботи становить 106 сторінок комп'ютерного тексту.

Об'єктом дослідження є суспільні відносини, що виникають у сфері міжнародно-правового регулювання кібероборони та використання кіберпростору державами під час забезпечення міжнародної безпеки. Йдеться про комплекс правовідносин, пов'язаних із запобіганням, здійсненням та реагуванням на кібероперації, які можуть становити загрозу миру, безпеці або збройним конфліктам.

Предметом дослідження є норми міжнародного права, що регулюють кібероборону, включаючи положення Статуту ООН, принципи міжнародного гуманітарного права, доктринальні підходи, а також міжнародну та національну практику держав щодо кваліфікації та реагування на кіберзагрози.

Методологічну основу формують: діалектичний метод - для аналізу розвитку кібероборони як динамічного явища міжнародного права та виявлення суперечностей у його правовому регулюванні; історико-правовий метод - для вивчення еволюції підходів до регулювання кіберпростору та формування доктрини кібероборони; порівняльно-правовий метод - для зіставлення національних підходів різних держав до кібероборони та їх відповідності міжнародним стандартам; формально-юридичний метод - для тлумачення норм міжнародного права, що застосовуються до кібероперацій; системний метод - для дослідження кібероборони як елемента системи міжнародної безпеки та взаємозв'язку між її складовими; емпіричний метод - для аналізу

практичних кейсів кібероперацій та державної практики у сфері кібероборони.

У роботі проаналізовано поняття кібероборони у міжнародно-правовому розумінні, досліджено джерела міжнародного права у цій сфері, включаючи положення Статуту ООН, норми міжнародного гуманітарного права, міжнародні конвенції, судову практику та доктринальні джерела.

Особливу увагу приділено аналізу застосування норм jus ad bellum та jus in bello до кіберпростору та кібероперацій, зокрема питанням кваліфікації кібероперацій як застосування сили, збройного нападу або оборони відповідно до статей 2(4) та 51 Статуту ООН. Досліджено підходи до застосування міжнародного гуманітарного права у кіберпросторі, проблеми визначення об’єктів атаки та оцінки наслідків кібероперацій. Окремо було розглянуто принципи пропорційності, розрізнення, необхідності у межах кібероборонних операцій.

У роботі проаналізовано Талліннський посібник 2.0 та інші сучасні доктринальні підходи щодо міжнародно-правового регулювання кібероборони. Окрему увагу приділено практиці Естонської Республіки, Сполучених Штатів Америки та Держави Ізраїль у сфері кібероборони, відповідним моделям кіберзахисту, практичному досвіду проведення кібероперацій та впливу на формування міжнародних підходів у цій сфері.

Також досліджено сучасний досвід України у сфері кібероборони в умовах збройної агресії та гібридної війни. Обґрунтовано необхідність подальшого вдосконалення міжнародно-правових механізмів регулювання кіберпростору та доцільність створення Спеціального міжнародного трибуналу щодо злочину агресії проти України, який може сприяти формуванню міжнародної практики кваліфікації кібероперацій.

У результаті дослідження зроблено висновок про необхідність подальшої кодифікації міжнародно-правових норм у сфері кібероборони та розвитку міжнародного співробітництва у сфері кібербезпеки.

Ключові слова: кібероборона, кібернапад, кібератака, кіберпростір, кібероперації, кібербезпека, міжнародне право, міжнародне гуманітарне право, jus ad bellum, jus in bello, Статут ООН, Таллінський посібник, право Женеви, збройний напад, цифровий простір, кіберсередовище, міжнародна безпека.

Abstract

Morozov A. Cyber Defense in International Law

Qualifying work for the second (master's) level of higher education.

The qualifying work consists of an introduction, three chapters (six subsections), conclusions, and a list of references (144 titles). The total volume of the thesis contains 106 pages of computer text.

The object of the research is the social relations arising in the field of international legal regulation of cyber defense and the use of cyberspace by states in the process of ensuring international security. It concerns a complex of legal relations connected with the prevention, implementation, and response to cyber operations that may pose a threat to peace, security, or armed conflicts.

The subject of the research is the norms of international law regulating cyber defense, including the provisions of the UN Charter, the principles of international humanitarian law, doctrinal approaches, as well as international and national state practice regarding the qualification of and response to cyber threats.

The methodological basis of the research is formed by the following methods: the dialectical method — for analyzing the development of cyber defense as a dynamic phenomenon of international law and identifying contradictions in its legal regulation; the historical-legal method — for studying the evolution of approaches to cyberspace regulation and the formation of the doctrine of cyber defense; the comparative-legal method — for comparing national approaches of different states to cyber defense and their compliance with international standards; the formal-legal method — for interpreting the norms of international law applicable to cyber operations; the systemic method — for examining cyber defense as an element of the international security system and the interrelation between its components; and the empirical method — for analyzing practical cases of cyber operations and state practice in the field of cyber defense.

The thesis analyzes the concept of cyber defense in the international legal context and examines the sources of international law in this field, including the provisions of the UN Charter, norms of international humanitarian law, international conventions, judicial practice, and doctrinal sources.

Particular attention is paid to the analysis of the application of jus ad bellum and jus in bello norms to cyberspace and cyber operations, especially regarding the qualification of cyber operations as the use of force, armed attack, or defense in accordance with Articles 2(4) and 51 of the UN Charter. The study examines approaches to the application of international humanitarian law in cyberspace, as well as issues concerning the identification of legitimate targets and the assessment of the consequences of cyber operations. Special consideration is given to the principles of proportionality, distinction, and military necessity within cyber defense operations.

The thesis also analyzes the Tallinn Manual 2.0 and other contemporary doctrinal approaches to the international legal regulation of cyber defense. Particular attention is devoted to the practice of the Republic of Estonia, the United States of America, and the State of Israel in the field of cyber defense, including their cyber

protection models, practical experience in conducting cyber operations, and their influence on the development of international approaches in this sphere.

Furthermore, the research examines Ukraine's modern experience in the field of cyber defense under conditions of armed aggression and hybrid warfare. The necessity for further improvement of international legal mechanisms regulating cyberspace and the expediency of establishing a Special International Tribunal for the Crime of Aggression against Ukraine are substantiated, as such a tribunal may contribute to the development of international practice concerning the qualification of cyber operations.

As a result of the research, the conclusion is made regarding the necessity for further codification of international legal norms in the field of cyber defense and the development of international cooperation in the sphere of cybersecurity.

Keywords: cyber defense, cyberattack, cyber strike, cyberspace, cyber operations, cybersecurity, international law, international humanitarian law, jus ad bellum, jus in bello, UN Charter, Tallinn Manual, Geneva law, armed attack, digital space, cyber environment, international security.

Зміст

Перелік умовних скорочень

ГА ООН - Генеральна Асамблея Організації Об’єднаних Націй

КП - Кіберпростір

МГП - Міжнародне гуманітарне право

МКТЮ - Міжнародний трибунал щодо колишньої Югославії

МС ООН - Міжнародний Суд Організації Об’єднаних Націй

ООН - Організація Об’єднаних Націй

США - Сполучені Штати Америки

ВСТУП

Актуальність теми. Сучасний розвиток інформаційно-комунікаційних технологій зумовив трансформацію міжнародних відносин. Фактично, кіберпростір перетворився на окрему сферу потенційного протиборства держав. Зростання кількості кібероперацій, спрямованих як на критичну інфраструктуру держав, так і на військові та цивільні системи, актуалізує питання формування ефективних міжнародно-правових механізмів кібероборони. В умовах глобальної цифровізації кіберзагрози набувають транскордонного характеру, що ускладнює їх локалізацію та правову кваліфікацію в межах національних юрисдикцій.

Особливого значення набуває проблема співвідношення кібероборони з фундаментальними принципами міжнародного права, зокрема принципом незастосування сили та заборони погрози силою, закріпленими у Статуті ООН. Водночас відсутність універсального міжнародно-правового договору, який би комплексно регулював питання кібероборони, призводить до фрагментарності правового регулювання та різночитань у державній практиці. Це, у свою чергу, ускладнює формування єдиних стандартів поведінки держав у кіберпросторі.

Додаткову складність становить питання застосування норм міжнародного гуманітарного права (jus in bello) до кібероперацій, оскільки традиційні правові конструкції не завжди адекватно відображають специфіку цифрових атак. Виникають дискусії щодо критеріїв «збройного нападу» у кіберпросторі, меж самооборони, а також допустимості превентивних кіберзаходів.

Окремої уваги потребує практика держав у сфері кібероборони, яка демонструє різні підходи до тлумачення міжнародного права. У цьому контексті особливо актуальним є досвід України, яка в умовах збройної агресії зазнає масштабних кібероперацій, що супроводжують воєнні дії, і

змушена розвивати національну систему кібероборони з урахуванням міжнародно-правових стандартів.

Таким чином, актуальність дослідження зумовлена необхідністю комплексного аналізу міжнародно-правового регулювання кібероборони, виявлення його прогалин та визначення перспектив удосконалення правових механізмів у цій сфері.

Мета дослідження. Комплексний аналіз міжнародно-правових засад кібероборони, дослідження її місця у системі міжнародного права, а також визначення особливостей правового регулювання кібероперацій у контексті jus ad bellum та jus in bello з урахуванням сучасної практики держав і викликів для України.

Для досягнення поставленої мети визначено такі завдання:

1. дослідити поняття кібероборони та суміжних із ним понять - кіберпростору, кібервійни, кібернападу;
2. визначити місце кібероборони у системі міжнародного права;
3. розкрити систему джерел міжнародного права у сфері кібероборони;
4. встановити особливості застосування норм jus ad bellum до кібероперацій оборонного або наступального характеру;
5. здійснити аналіз регулювання кібероборони в контексті jus in bello, з’ясувати їхню застосовність;
6. проаналізувати практику окремих держав у сфері кібероборони;
7. обґрунтувати особливості кібероборони України в умовах війни;
8. сформулювати пропозиції щодо вдосконалення міжнародно-правового регулювання кібероборони.

Об’єктом дослідження. Суспільні відносини, що виникають у сфері міжнародно-правового регулювання кібероборони та використання кіберпростору державами під час забезпечення міжнародної безпеки. Йдеться про комплекс правовідносин, пов’язаних із запобіганням, здійсненням та

реагуванням на кібероперації, які можуть становити загрозу миру, безпеці або збройним конфліктам.

Предметом дослідження. Норми міжнародного права, що регулюють кібероборону, включаючи положення Статуту ООН, принципи міжнародного гуманітарного права, доктринальні підходи, а також міжнародну та національну практику держав щодо кваліфікації та реагування на кіберзагрози.

Методи дослідження. У роботі застосовано комплексний підхід, який поєднує загальнонаукові та спеціальні методи міжнародного права: діалектичний метод - для аналізу розвитку кібероборони як динамічного явища міжнародного права та виявлення суперечностей у його правовому регулюванні; історико-правовий метод - для вивчення еволюції підходів до регулювання кіберпростору та формування доктрини кібероборони; порівняльно-правовий метод - для зіставлення національних підходів різних держав до кібероборони та їх відповідності міжнародним стандартам; формально-юридичний метод - для тлумачення норм міжнародного права, що застосовуються до кібероперацій; системний метод - для дослідження кібероборони як елемента системи міжнародної безпеки та взаємозв’язку між її складовими; емпіричний метод - для аналізу практичних кейсів кібероперацій та державної практики у сфері кібероборони.

Інформаційна база дослідження включає: Статут ООН, Женевську конвенцію про захист цивільного населення під час війни (IV Конвенція), Додаткові протоколи до Женевських конвенцій та інші міжнародно-правові акти, міжнародні та національні судові рішення, документи міжнародних організацій, доктринальні джерела провідних науковців у сфері міжнародного права та кібероборони, звіти експертних груп, зокрема Талліннський посібник 2.0, а також національне законодавство та практику держав у сфері кібероборони.

Наукова новизна одержаних результатів полягає в комплексному дослідженні кібероборони як самостійного об’єкта міжнародно-правового регулювання, уточненні її місця у системі jus ad bellum та jus in bello, а також у виявленні ключових прогалин у сучасному міжнародному праві щодо регулювання кібероперацій. У роботі запропоновано узагальнення підходів держав до кваліфікації кіберзагроз і визначення критеріїв їх віднесення до «збройного нападу» у кіберпросторі.

Практичне значення одержаних результатів полягає у можливості їх використання для вдосконалення національного законодавства України у сфері кібероборони, розробки державної політики у сфері кібербезпеки, а також у науковій діяльності у сферах міжнародного права, міжнародної безпеки та кібербезпеки. Результати дослідження можуть бути використані також у діяльності державних органів, що відповідають за кіберзахист та міжнародно-правове співробітництво у цій сфері.

Апробація результатів. Апробацію результатів кваліфікаційної роботи здійснено шляхом участі у IV Всеукраїнській науково-практичній конференції «Конституція України: стан, перспективи та механізми реалізації».

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів (шести підрозділів), висновків, списку використаних джерел (144 найменування). Загальний обсяг роботи становить 106 сторінок комп’ютерного тексту.

РОЗДІЛ 1. Теоретико-правові основи кібероборони в міжнародному праві

1.1. Поняття кібероборони та її місце у системі міжнародно права

Розгляд сутності такого нового поняття, як “кібероборона”, вимагає комплексного підходу. Оскільки це питання стосується не тільки термінології, а є фундаментальною проблемою в науці та праві, в першу чергу буде доцільним розглянути суміжні поняття, застосовуючи дедуктивний метод, що полягає у “шляху від загального до конкретного”. Кібероборона за своєю природою є похідним поняттям і має спиратись на усталений в науці та практиці правовий базис, тому неможливо всебічно з’ясувати специфіку захисту в кіберпросторі, ігноруючи розкриття змісту оборони в її класичному розумінні.

В той самий час, оборона є складовою війни та водночас виступає її діалектичною протилежністю, як закономірна реакція на загрозу, тому для розуміння кібероборони та оборони необхідно з’ясувати від чого саме відбувається державний захист. При цьому, кібервійна є різновидом війни, яка змінила вимір з фізичного на цифровий або віртуальний.

І хоча з точки зору словотворення, префікс “кібер-” вказує на новий простір ведення війни та оборони, варто зауважити, що в міжнародному та національному праві, точність термінології дозволяє визначити межі відповідальності. Зокрема, нечіткість дефініювання кібероборони на національному рівні може призвести до конфлікту повноважень державних інститутів, зокрема між спеціальними службами, відповідальними за кібербезпеку та протидію тероризму, та збройними силами, відповідальними за кібероборону, та відсутності єдиної сформованої доктрини.

Власне, термін “війна”, згідно з Політичною енциклопедією, - це соціально-політичне явище, що є крайньою формою розв’язання суперечностей різного характеру, у тому числі економічних, суспільно-політичних, релігійних, національних та інших, між державами, народами

або націями засобами воєнного насильства, якими, в свою чергу, розв'язуються та досягаються цілі війни, що як під час її процесу, так і в кінцевому результаті веде до якісної зміни всіх сфер суспільного життя: соціальної, політичної, економічної, духовної, оскільки відбувається їх кардинальна перебудова. [128, с. 105-106]

Щодо концептуальних основ виникнення воєн відповідно до Політичної енциклопедії розрізняють наступні теорії, зокрема: космополітична, згідно з якою причина війна полягає в антагонізмі між національними та загальнолюдськими інтересами; біологічна, яка прямо пов'язує причини війн з біологічними умовами існування людини (концентрація населення в окремих регіонах планети); за соціально-етичною війни сприяють формуванню сили та волі як нації загалом, так і окремих осіб, яким відведена так звана «особлива історична місія»; психологічна визначає джерело війни людською психікою та схильністю людського інтелекту до агресії; географічна зводить причини до особливостей розташування країн та їхньої боротьби за території; езотерична припускає втручання вищої суті в життєві процеси на Землі з ціллю відбору людської енергії для енергетичного підживлення певних точок планети. [128, с. 105-106]

Прусський генерал Карл фон Клаузевіц у своїй книзі Vom Kriege (з німецької – "Про війну") визначив війну, як «акт примусу (сили), щоб змусити протилежну сторону виконувати нашу волю». Цю тезу частково доповнює професор Гейдельберзького університету Г. Гофмайстер, який у своїй науковій праці під назвою «Воля до війни та безпорадність політики» вказав, що війна – це є продовження політики іншими засобами. [23; 120]

Видатний італійський мислитель епохи Відродження, державний діяч та дипломат, Нікколо Макіавеллі, який прославився, зокрема такими працями як «Государ» (Державець), «Трактат про військове мистецтво» та «Роздуми наодинці». В своїх працях він називає війну ремеслом та підкреслює її

важливість як невід'ємний атрибут державотворення та захисту державного суверенітету. [104; 142]

Згадуючи досить відомий та популярний у світі трактат під назвою «Мистецтво війни», автором якого є Сунь Цзи, справедливо відзначити, що в ньому війна визначається як справа надзвичайної ваги для держави, те, що треба детально вивчати та аналізувати, досліджувати до найменших дрібниць, щоб виграти війну без бою або з найменшими втратами. Сунь Цзи підкреслював, що війна – це лише крайня міра, «останні двері» до миру. Для нього вона була в першу чергу інтелектуальною справою, адже остання є, дослівно, «Шлях-Дао обману», тобто мистецтвом брехні.

Водночас, варто зауважити, що після численного аналізу міжнародних нормативно-правових актів можна дійти висновку, що станом на сьогодні відсутнє закріплення дефініції «війна» на офіційному рівні. Натомість, міжнародним гуманітарним правом (так званим правом війни або правом збройних конфліктів), а саме – Міжнародним кримінальним трибуналом щодо колишньої Югославії, визначено поняття «міжнародного збройний конфлікт», яке де-факто є синонімом «війни», – застосування збройної сили між державами.

Оскільки війна – це конфлікт, буде цілком логічним припустити, що як і будь-який інший конфлікт, перша має підстави, які слугували її виникненню. У науці поширена теза, що конфлікт «не виникає ні з чого» та має бути причинно-наслідковий зв'язок між причинами для початку та наслідками, які виявляються у, власне, її появі.

Так, американський соціолог Льюїс Альфред Козер, відомий вивченням соціальному явищу – конфлікту, у своїй науковій роботі «Функції соціального конфлікту», дослідив феномен соціального конфлікту та дійшов висновку, що постійним джерелом конфліктів у суспільстві є безустанний дефіцит ресурсів, у тому числі нематеріальних, наприклад – влади. [89]

Враховуючи те, що підстава та мета – це хоч і дуже схожі поняття, але не однакові за змістом, вони в будь-якому разі тісно пов’язані між собою. За попередньо згаданою працею Л.Козера, мета – це елемент, що визначає прагнення до оволодіння ресурсом, в той час як підстава слугує своєрідним «спусковим механізмом», який запускає цей процес. [89]

Відтак, у міжнародному праві, зокрема гуманітарному, наразі відсутня легальна та справедлива мета війни, хоча у сучасному науковому просторі закріплена сформована Фомою Аквінським та пізніше розвинена Гуго Гроцієм теорія bellum iustum (з латинської – справедлива війна). Відповідно до її ключових положень, війна є справедливою тоді та лише тоді, коли вона відповідає декільком критеріям: jus ad bellum або справедлива причина, що передбачає самооборону, захист територіальної цілісності або протидію геноциду, при цьому агресивна війна вважається апріорі несправедливою; jus in bello або ведення війни, що полягає у дотриманні сторонами принципів ведення війни, зокрема базуючись на праві Женеви та праві Гааги; jus post bellum або завершення війни, що закладає справедливість як основу мирного договору, який остаточно усуває усі першопричини конфлікту та не запобігає приниженню переможеної сторони.

Водночас, деякі вчені та правознавці схильні вважати, що єдиною законною метою та ціллю війни є зменшення військового потенціалу супротивника, а не економічний чи політичний інтерес чи вигода. Це зокрема підкреслюється Санкт-Петербурзькою декларацією 1868 року, яка наголошує на тому, що “єдиною законною метою, досягнення якої держави повинні прагнути під час війни, є послаблення військових сил противника”. [21]

Загалом, явище «війна», як спосіб вирішення політичних суперечностей, мало місце в історії людства з найдавніших часів та до сих пір зберігають свій статус «перманентної проблеми людства». Водночас, враховуючи стрімкий розвиток людства загалом, технологій та інститутів міжнародного права, розвиваються так само і види війн. Новітніми

способами ведення війни у 21 столітті можна виокремити кібер-, інформаційні та гібридні війни.

Повертаючись до конфліктології, оскільки війна полягає у застосуванні воєнного насильства між державами, буде цілком доречно вказати, що у будь-якому конфлікті будь-якого рівня завжди є щонайменше дві конфліктуючі сторони: ініціатор конфлікту, тобто той, хто нападає або першим здійснює агресивні кроки, та «жертва конфлікту» - той, на кого спрямовані згадані дії та вимушений оборонятись. Психологію конфліктів та конфліктуючі сторони досліджував попередньо згадуваний Льюїс Альфред Козер.

Так, аналізуючи його праці, у тому числі «Функції соціального конфлікту», за Л.Козером, ініціатор – це той, хто першим заявляє про несумісність інтересів, той, хто вчиняє конфліктну дію, переводячи приховане незадоволення у відкритий простір. Хоча варто зазначити, замість використання терміну «жертва» (англ. victim), частіше вживається «респондент» (англ. respondent).

Таким чином, оборона, трактуючи це поняття через призму Закону України «Про оборону України» від 6 грудня 1991 року № 1932-XI, - це система воєнних, політичних, економічних, правових та інших заходів, які спрямовані на захист держави та її територіальної цілісності. Тобто фактично, це контр-заходи, які мають на меті відбити наступ супротивника. [132]

У 1989-1991 роках, у зв’язку з появою Інтернету, умовно розпочалось розділення світу на реальність та віртуальність, що в наступні роки призвело до об’єднання реальності та віртуальності в одну дійсність шляхом повної інтеграції останньої в життя людей. Фактично, інформаційні технології заполонили всі сфери життя - суспільне, політичне, економічне, формуючи кіберпростір, якому буде приділена окрема увага. Водночас, не буде новою фраза «все звичне – безпечне, все нове – небезпечне», яка є фундаментальним

принципом роботи людського мозку та на біологічному рівні формує собою захисний механізм. За тією самою аналогією, розвиток нового поля - КП, з його кардинально швидкою інтеграцією в процеси держави, призвів до появи нових ризиків та прогалин в її захисних механізмах. [115]

Зокрема, Міжнародний комітет Червоного Хреста визначає кібервійну як операції проти комп'ютера або цілих систем за допомогою потоків даних, коли такі операції використовуються у якості засобу та методу ведення збройного конфлікту.

Натомість, через відносну новизну цього поняття та явища як такого, а також беручи до уваги підвищений науковий інтерес до проблеми дефініювання, у деяких наукових роботах можна побачити часткове ототожнення кібервійни з інформаційною війною, або, щонайменше, пояснення їх тісного зв'язку, не диференціюючи ці явища, а, навпаки, пишучи їх через дефіс – інформаційно-технічна війна та розглядаючи кібервійну як різновид інформаційної. Так, автор статті «Кібервійна як різновид інформаційних війн. Захист кіберпростору України» пояснює виникнення інформаційної війни ескалацію інформаційних конфліктів методами пропаганди, маніпулювання та дезінформації з метою формування нових поглядів як окремих громадян, так і суспільства загалом. При цьому, кібервійна в контексті інформаційної, на думку автора, виявляється в специфічних площині та методах, які застосовуються. [114]

Загалом, цілком логічно припустити, що кібервійна - це, як і війна, суспільне явище, яке виявляється в комплексах дій різного характеру (політичного, економічного, військового), які вчиняються учасниками конфлікту та спрямовуються на зменшення військового потенціалу супротивника, але в окремій площині - кіберпросторі.

Так, продовжуючи ідею окремого простору для ведення воєнних дій, кібервійна має відбуватись в певній площині, так само, як і звичайна війна. Цією певною площиною і виступає кіберпростір.

Генеральною конференцією ЮНЕСКО на її 32 сесії 15 жовтня 2003 року в Парижі, Французька Республіка, було прийнято Рекомендацію щодо сприяння та використання багатомовності та загального доступу до кіберпростору. Згідно з якою, КП вважається віртуальним світом цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою.

Український науковець Живило Є.О. у своїй статті «Мілітаризація викликів та загроз в кіберпросторі як операційному середовищі» пояснює КП як інформаційно-операційне середовище з відповідною специфічною інфраструктурою, яке складається зокрема з усіх комунікаційний мереж, комп'ютерних систем та їхнього обміну даними на основі використання єдиної системи стандартів та протоколів, що, в свою чергу, дозволяє перетворювати вихідну інформацію в інформаційний продукт, спрямований на конкретного користувача. [124]

На думку іншого українського науковця, Д. В. Дубова, КП - це «буття, винятковість якого пов'язана з тим, що він єдиний з усіх наразі опанованих людиною просторів є екстериторіальним, адже практично позбавлений географічних обмежень, від стану якого залежить функціональність, передбачуваність та прогнозованість стабільності світової економіки, безпеки людей, всезагального зростання добробуту, суспільного розвитку.» [116]

В окремій думці щодо рішення Верховного Суду Сполучених Штатів Америки, суддею Джанетом Ріно стосовно кіберпростору було зазначено таке – це електронний світ, що являє собою не більше ніж взаємозв'язок електронних шляхів, який дозволяє користувачам маскувати свою ідентичність та беззаперечно відображає певну форму географії реального

світу, оскільки, наприклад, «шлюзи» - чати та веб-сайти існують лише у певних фіксованих «місцях» в Інтернету. Суттєвою відмінністю цифрового простору від фізичного є його гнучкість. У самому ж рішенні, згадка про КП звучала так: «в Інтернеті, міжнародній мережі взаємопов'язаних комп'ютерів, яка дозволяє мільйонам людей спілкуватися один з одним у «кіберпросторі» та отримувати доступ до величезних обсягів інформації з усього світу». [65]

Таким чином, резюмуючи різні підходи щодо визначення поняття кіберпростору, можна дійти висновку, що останній – це нефізична і тому екстериторіальна площина, окремі елементи якої «прив'язані» до певних точок та яка оперується як окремими індивідами, так і групами осіб за допомогою взаємодії комп'ютерних систем шляхом взаємного обміну даними між собою на підставі єдиних стандартів та протоколів.

При цьому, слід зазначити, що КП має безпосередній зв'язок з фізичним простором, або, фактично, залежить від другого. Це пояснюється тим, що існування кіберпростору без телекомунікаційної та енергетичної інфраструктури є неможливим. Оскільки, як було згадано, КП - це, в тому числі, мережеве обладнання, останнє працює за наявності по-перше, електроенергії, а по-друге, існуванню спільних точок обміну інформації. Таким чином, за відсутності електричної інфраструктури не існуватиме джерела живлення обладнання, яке дозволяє користувачам взаємодіяти між собою у КП.

Таку позицію підтверджує викладач Школи права Абердінського університету у Великій Британії, Ірен Коузігоу (Irène Couzigou) у своїй праці "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations", пояснюючи КП як глобальний домен в інформаційному середовищі, унікальний характер якого формується внаслідок використання електронних засобів та електромагнітного спектра для створення, обміну та використання інформації через взаємопов'язаними мережами із застосуванням інформаційно-комунікаційних технологій. При цьому, вона

наголошує на факті зберігання та циркуляції інформації, фізично розташованої у просторі, тобто, на фізичних носіях - комп'ютерах, серверах, кабелях та інших. Внаслідок чого, територіальна юрисдикція країн поширюється на КП, оскільки держави контролюють кіберінфраструктуру, якою забезпечується та обслуговується діяльність (існування) кіберпростору. [70]

У цьому зв'язку, кібероборона, розглядаючи її через призму головного поняття "оборона", – це система політичних, економічних, соціальних, військових та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення державної безпеки, територіальної цілісності та обороноздатності з метою запобіганню збройного конфлікту або мінімізацією негативного ефекту збройної агресії. [140, с. 403-404]

Варто наголосити, що обмеження кіберпростором у цьому контексті частково зменшує обсяг поняття, оскільки, як було зазначено, КП та його здатність функціонувати напряму залежить від інфраструктури, тому вплив на цю інфраструктуру як методами програмної взаємодії, так і фізичним впливом доцільно вважати заходами з кібероборони або, у деяких випадках, гібридними заходами оборони.

З такою позицією погоджується доктор технічних наук, П. М. Сніцаренко, у своїй праці він також розкриває це поняття як дії військових сил, які застосовуються в умовах відбиття збройної агресії проти держави для комплексного захисту КП (електронних інформаційних ресурсів) завдання ураження електронним інформаційним ресурсам противника, а також забезпечення безпеки критичних об'єктів інформаційної діяльності держави від ударів засобами традиційної зброї, з метою досягнення переваги, зокрема інформаційної, над противником у кіберпросторі в умовах збройного конфлікту. [136, с. 53]

На думку міжнародної групи експертів, розробників найбільш комплексної міжнародної доктрини у сфері кібероперацій - Таллінський посібник, принцип державного суверенітету поширюється на кіберпростір. Це пояснюється тим, що суверенні держави контролюють діяльність кіберінфраструктури, яка розташована на їх території. При цьому, КП умовно розділено на такі рівні, як фізичний, який складається з програмного забезпечення та допоміжної інфраструктури (сервери, комп'ютери, маршрутизатори та інші); логічний, який включає програми, дані та протоколи, які забезпечують обмін даними через фізичний рівень та соціальний - охоплює осіб та групи осіб, залучені до кібердіяльності. Варто зауважити, що міжнародною групою експертів було поставлено під сумнів дефініцію кіберпростору як "глобальної області" або "п'ятого виміру", подібному космічному або повітряному простору в розумінні "глобального спільного простору" (res communis omnium), оскільки подібні терміни ігнорують територіальні особливості кіберпростору та кібероперацій, які тим чи іншим чином впливають на принцип державного суверенітету. В якості аргументу було наведено прямий зв'язок між суб'єктом кібердіяльності, територією здійснення такої активності та його приналежності до держави. При цьому було зауважено, що жодна держава не може ані проголошувати свій суверенітет над КП, оскільки переважна частина кіберінфраструктури, яка створює цей простір, розташована на території інших суверенних держав, ані відмовлятись від нього остаточно. Було окремо наголошено, що кібердіяльність може перетинати багато кордонів або відбуватись у міжнародних водах або повітряному просторі, але виконавець завжди є фізичною або юридичною особою, яка перебуває під юрисдикцією однієї або декількох держав. [54]

Розкриваючи сутність державного суверенітету у кіберпросторі, варто згадати французького юриста Жана Бодіна (Jean Bodin), який у своїй фундаментальній праці 1576 року "Les Six Livres de la République" (з

французької - “Шість книг про державу”) в розділах VIII-X вперше створив концепцію розподілу державного суверенітету на внутрішній та зовнішній, яку в подальшому розвинув Гуго Гроцій. Так, внутрішній суверенітет полягає у верховенстві публічної влади на території держави, а зовнішній - у незалежності в зовнішніх зносинах. [71]

У Таллінському посібнику внутрішній суверенітет держави у кіберпросторі обґрунтовується здатністю держави ухвалювати будь-які заходи щодо кіберінфраструктури та кібердіяльності в межах своєї території та міжнародно-правових зобов’язань. З одного боку, державні органи виступають внутрішньоправовим регулятором та контролюючим за виконанням законодавства у сфері кібердіяльності, а з іншого - держава бере на себе зобов’язання із захисту кіберінфраструктури, розташованої на її території, та, відповідно, недоторканість та безпеку кіберсередовища від зовнішніх та внутрішніх загроз, створюючи для цього спеціальні норми права та кіберорган, а також лобіюючи ухвалення нормативно-правових рішень.

В цьому ключі, зовнішній суверенітет держави виходить із суверенної рівності держав, згідно зі статутом ООН. Таким чином, кожна держава є незалежною та вільною в ухваленні рішень та здійсненні кібердіяльності доти, доки така діяльність не суперечить міжнародним зобов’язанням та міжнародному звичаєвому праву. Такий суверенітет, у тому числі, охоплює право вибору курсу зовнішньої політики щодо діяльності у цифровому середовищі, здатністю укладати міжнародні договори, приєднуватись до міжнародно-правових режимів регулювання КП та висловлювати opinio juris щодо практики інших держав у кіберсфері. Експерти прямо наголошують, що кібероперації держави на підставі її зовнішнього суверенітету не скасовують дію обов’язкових договірних або звичаєвих норм права, і тим більше положення Статуту ООН щодо непорушності державного суверенітету. Водночас, за виняткових обставин порушення державного суверенітету шляхом здійснення кібероперацій дозволяється у разі санкціонування такої

дії Радою Безпеки ООН або в межах реалізації права на самооборону. При цьому окремо наголошено, що це правило застосовується лише у відносинах між державою, але жодним чином не поширюється на дії недержавних суб'єктів, якщо такі дії не коригуються державою або не вчиняються на її замовлення. Це пояснюється безпосередньо Статутом ООН, який накладає на держави обов'язок із непорушення державного суверенітету, і тому єдиними, хто може порушити це правило - є держави. Однак, експертами було визнано існування погляду, згідно з яким деякі недержавні суб'єкти, наприклад - терористичні угрупування, можуть порушувати державний суверенітет, однак жоден із науковців-розробників посібника не погодився з цією тезою. [54]

Одним із найбільш цитованих теоретиків кібервійни та кібероборони вважається американський вчений Мартін Лібіцкі у своїй праці 2009 року "Cyberdeterrence and Cyberwar" визначає кібероборону як критичний, але надзвичайно складний елемент безпеки держави. Зокрема, науковець ставить під сумнів доцільність такого міжнародного політичного інструмента, як "стримування", який використовувався під час Холодної війни між Сполученими Штатами Америки та Радянським Союзом за допомогою сторони запобігли виникненню ядерного конфлікту. Аргументація на користь кіберстримування як правило грунтується за логікою "кібератаки дешевші за кіберзахист", і тому Лібіцкі пропонує трансформувати систему стримування та адаптувати її до сучасних реалій, де кібератаки будуть настільки дорогими по відношенню до кібероборони, що мета та собівартість атак і буде фактором стримування. При цьому, таку позицію підтримує професор Гарвардського університету Джозеф Най. [18]

М. Лівіцкі також називає цивільну та військову кібероборону схожими, але чітко їх розрізняє. Хоча військові мережі зазвичай використовують однакове апаратне програмне забезпечення, що і цивільні, автор підкреслює наявність спільних, майже ідентичних вразливих місць. Головною метою для військових мереж, з огляду на їхні особливості у вигляді реальних ворогів,

специфічних кіберзагроз та безлічі закритих систем, - є необхідність у безперебійному постійному функціонуванні, не втрачаючи якісних показників, у тому числі, під час кібератак. Надійність (Robustness) у цьому зв’язку є головним фактором, якому необхідно приділяти багато уваги, адже вона виходить за межі інженерії мережевої безпеки та охоплює всі заходи, які дозволяють безпосередній армії, як широкій системі, працювати в критичні моменти. Окрім цього, наголошується увага на швидкості відновлення роботи. [18]

Отже, поняття кібероборони є складним та багаторівневим, і не може розглядатися ізольовано від базових категорій війни та суміжних із нею понять. Застосування дедуктивного підходу дозволило послідовно перейти від загального розуміння війни як соціально-політичного явища до визначення специфіки кібероборони як окремого напряму забезпечення державної безпеки в умовах цифровізації суспільства. Кібероборона має похідний характер та ґрунтується на класичних уявленнях про оборону держави, адаптованих до нових технологічних реалій.

Війна традиційно розглядається як форма вирішення конфліктів між державами або іншими суб’єктами шляхом застосування насильства. У науковці сформувалося декілька концептуальних підходів до пояснення причин виникнення воєн, серед яких виокремлюються космополітична, біологічна, психологічна, географічна, соціально-етична та інші теорії. Незважаючи на відмінність підходів, усі вони вказують на конфліктну природу війни та її тісний зв’язок із боротьбою за ресурси, владу, вплив або безпеку.

В міжнародному праві відсутнє універсальне нормативне визначення поняття “війна”, однак фактично його функцію виконує категорія міжнародного збройного конфлікту, яка визначається як застосування збройної сили між державами.

Аналіз праць класичних мислителів і теоретиків війни дозволив дійти висновку, що війна розглядалася не лише як військове явище, а і як політичний, соціальний та інтелектуальний процес. Карл фон Клаузевіц визначав війну як примус до виконання волі іншої сторони, а також як продовження політики іншими засобами. Нікколо Макіавеллі розглядав війну як необхідний інструмент державотворення та захисту суверенітету. Сунь Цзи наголошував на стратегічному та інтелектуальному характері війни, підкреслюючи значення аналізу, обману та мінімізації втрат.

Оборона виступає закономірною реакцією держави на зовнішню загрозу або агресію. Таким чином, оборона фактично є комплексом контрзаходів, спрямованих на відбиття агресії та забезпечення стабільності держави.

Розвиток інформаційних технологій та глобальної мережі Інтернет призвів до формування нового середовища суспільних відносин - кіберпростору. Останній поступово інтегрувався у всі сфери життєдіяльності держави та суспільства, внаслідок чого виникли нові загрози безпеці та нові форми конфліктів. Це стало передумовою появи кібервійни як нового виду війни, що реалізується у цифровому середовищі.

Кібервійна розглядається як сукупність дій політичного, військового, економічного та іншого характеру, які здійснюються в КП та спрямовані на послаблення потенціалу противника. Основною відмінністю кібервійни є використання специфічного середовища та методів впливу, які реалізуються через комп’ютерні системи, мережі та інформаційні технології. На основі аналізу наукових підходів встановлено, що КП є віртуальною, екстериторіальною площиною, яка функціонує через взаємодію інформаційно-комунікаційних систем та обмін даними між ними. Він не є повністю відокремленим від фізичного світу, оскільки його існування безпосередньо залежить від матеріальної інфраструктури - серверів, мережевого обладнання, кабельних систем та енергетичного забезпечення.

Враховуючи це, кібероборона є системою політичних, військових, економічних, соціальних та інших заходів, які здійснюються у кіберпросторі з метою забезпечення державної безпеки, територіальної цілісності та обороноздатності держави. Її сутність полягає у забезпеченні захисту держави, її інформаційної інфраструктури та суспільних процесів. Це забезпечується шляхом реалізації комплексу правових, військових, організаційних і технічних заходів.

1.2. Джерела міжнародного права у сфері кібероборони

Джерело міжнародного права - це спосіб вираження та закріплення правових норм, які спрямовані на регулювання конкретних суспільних відносин. У статті 38 Статуту Міжнародного Суду Організації Об'єднаних Націй визначений перелік джерел міжнародного права, до якого належать: загальні чи спеціальні міжнародні конвенції, що встановлюють норми, прямо визнані сторонами спору (суб'єктами міжнародного права); міжнародні звичаї, як докази загальної практики, визнаної як право; загальні принципи права, визнані світом співтовариством; міжнародні судові рішення та доктринальні праці найбільш кваліфікованих та впізнаваних юристів з різних націй.

Головна особливість та одночасно проблема кібероборони у 2026 році полягає у відсутності єдиного уніфікованого міжнародно-правового акта, який би охоплював та регулював оборону у цифровому середовищі та межі її застосування. Натомість, на сучасному етапі розвитку юридичної науки у сфері кібероборони сформувався комплексний доктринальний базис. У світлі глобальної цифровізації та переходу з паперових носіїв даних на цифрові версії, у тому числі державними органами, закріплювалась потреба у нормативно-правовому регулюванні кібероборони та кіберпростору загалом. Вагомий науковий внесок з цієї проблематики здійснила низка міжнародних інституцій та дослідників, які своїми працями заклали основу для сучасної

інтерпретації міжнародного гуманітарного права у віртуальному або цифровому середовищі.

Серед відомих дослідників цієї теми варто вказати Джозефа Найя (Joseph S. Nye Jr.), який у своїй праці “Deterrence and Dissuasion in Cyberspace” відводить міжнародному праву роль комплексного регулятора кіберконфліктів у довгостроковій перспективі, виокремлюючи чотири механізми кіберстримування: норми та табу (norms); взаємозалежність (entanglement); заперечення (denial) та покарання (punishment). [24]

Джозеф Най наголошує, що кібернорми можуть стримувати кіберагресію, через накладання репутаційних витрат виконавцю, які можуть завдати шкоди “м’якій силі” цього суб’єкта, роблячи кібератаки невигідними в розумінні співвідношення вигоди та втрати. Більше того, норми права спричиняють негативні наслідки нападнику навіть у випадку невідбиття кібератак обороною. Науковець проводить аналогію з ядерною зброєю в “конфліктах низького рівня зі слабшим актором”, вказуючи, що застосування ядерної зброї в таких випадках робить вигоду явно меншою за втрати, зокрема репутаційні. Він окремо наголошує, що у зв'язку із розвитком міжнародних норм про невикористання ядерної зброї, якими було впроваджено санкції за порушення порядку її застосування, на суб’єкта збройного конфлікту було накладено додатковий тягар відповідальності, яка полягає вже не тільки в репутаційних втратах. При цьому Джозеф Най він звертає увагу на те, що в критичних ситуаціях та у випадку появи “нових учасників” на міжнародній арені, не можна бути впевненим чи будуть враховані норми та табу як запобіжники під час прийняття тих чи інших рішень. Він також проводить іншу аналогію щодо відмови держав від використання хімічної та біологічної зброї під час збройних конфліктів, що в подальшому було трансформовано в Женевський протокол 1925 року про заборону використання хімічної та біологічної зброї. Окрім цього, у 1970-х роках було впроваджено заборони на виробництво та накопичення такої

зброї. Джозеф Най наголошує, що ці заборони, включно із санкціями за їх порушення, не завадило Радянському Союзу маніпулювати нормами правами, продовжуючи як накопичувати, так і виробляти й розробляти нову хімічну та біологічну зброю. Так само, як це не зупинило ані Саддама Хусейна, ані Башара аль-Асада від застосування хімічної зброї проти власних громадян. Таким чином, автор вказує на те, що норми права не завжди відповідають дійсності, а враховуючи складну специфіку кіберпростору та комп'ютерних програм, коли різниця між безпечною програмою та небезпечною може сягати "одного рядка коду", або ж мати подвійне призначення, створювати кібернорми про заборону створення або використання є неефективним з самого початку. Натомість, на його думку, більш плідним підходом буде створення норм, які визначають дозволену мету використання, забороняють певні типи цілей, на які можуть бути спрямовані атаки, встановити чітку межу між прийнятною поведінкою під час збройних конфліктів та такою, що порушує норми міжнародного гуманітарного права. [24, с. 60-62]

Іншим аспектом міжнародно-правового регулювання кібероборони, про який Джозеф Най згадує у своїй роботі, є необхідність створення правового підгрунтя для публічного звинувачення, або як він вказує "naming and shaming", тобто "називання та осоромлення". Інститут відповідальності у міжнародному правовому полі відіграє важливу роль, але в цифровому просторі, де особа зловмисника та його приналежність до держави або її конкретної структури замаскована протоколами захисту та залишається невідомою до представників оборони, шанс покарання, як і погрози санкціями залишаються малоймовірними та менш ефективними у порівнянні з класичними методами та засобами ведення війни. Аналогічно залишається невідомим об'єкт та час нападу, тому у такому вузькому розумінні поняття кіберстримування та кібероборони, засноване на погрозах накладення санкцій та покарання, не відіграватиме значної ролі, хоча може і має застосовуватись. Щодо "ladder of possible retaliatory responses according to

their increasing levels of belligerence", тобто шкали можливих заходів у відповідь на кіберагресію за ступенем їхньої агресивності, науковець цитує вже згаданого раніше М. Лівіцкі: дипломатичні, економічні, кібер-, застосування фізичної сили та навіть ядерної сили як останнього "якоря" (anchor) цієї шкали та фінальної відповіді. І хоча Джозеф Най вказує на труднощі, пов'язані зі стримуванням шляхом покарання, він акцентує увагу на важливості цього інституту у КП, щонайменше для руйнації міжнародної репутації та геополітичного впливу країни-агресора. [24, с. 55-56]

На доповнення до попереднього, він стверджує, що необхідність створення правової основи регуляції КП та кібероборони передбачатиме можливість здійснення колективних заходів у відповідь на розв'язування збройних конфліктів, у тому числі у кіберпросторі, що дозволить застосовувати, окрім активної кібероборони країни, яка зазнала нападу, колективні санкції, економічний бойкот та дипломатичну ізоляцію. При цьому звертає увагу на те, що за відсутності міжнародно-правових норм у цифровій сфері безпеки та оборони, подібні дії могли б трактуватись як односторонній безпідставний тиск, а за наявності - цей процес легалізується як залучення союзників до коаліції для спільної відсічі кіберагресії. [24, с. 63]

У цьому зв'язку варто зауважити, що створенню міжнародно-правових норм для регулювання нових сфер взаємодії глобальної спільноти найчастіше передує глибоке інтелектуальне дослідження наукової спільноти. У контексті кібероборони та цифрового простору, ключове місце серед доктринальних джерел у цій сфері посідає Таллінський посібник (Tallinn Manual) - результат багаторічної роботи міжнародної групи експертів під егідою Об'єднаного центру передових технологій з кіберзахисту Організації Пінічноатлантичного договору (НАТО), який став найбільш авторитетним науково-практичним коментарем щодо застосування міжнародного права до кібероперацій. [55]

Як вказано на офіційному веб-сайті Об'єднаного центру передових технологій з кіберзахисту НАТО, Таллінський посібник - це наукова робота,

яка не має юридичної сили (non-binding), написана видатними вченими та практиками з міжнародного права під керівництвом професором міжнародного права Майклом Шміттом (Michael N. Schmitt), метою якої є об'єктивне переосмислення міжнародного права, що застосовується в кіберконтексті. Посібник є політично нейтральним і не представлятиме правову позицію чи доктрину будь-якої держави чи міжнародної організації, включаючи Об’єднаного центру. [55]

Таллінський посібник версії 2.0 складається з 4 частин, розділених на розділи та секції та містить загалом 154 правила з коментарями окремих науковців міжнародної групи експертів зі спірних питань для висвітлення логіки прийняття конкретного правила та фіксації у розбіжності поглядів з того чи іншого питання.

Одним із напрямів дослідження у Таллінському посібнику 2.0 є визначення застосовності загального міжнародного права до кіберпростору та суміжних понять, які включають кібероперації та кібероборону. Окрім цього, у доктрині грунтовно пояснюється тісний зв'язок між кібероперaціями та міжнародним гуманітарним правом, яке регулює міжнародні та неміжнародні збройні конфлікти. Це свідчить про те, що під час здійснення кібероборони держави повинні дотримуватись основоположних принципів так званого права війни, у тому числі, принципу розрізнення цивільних та військових об'єктів, принципу пропорційності та принципу необхідності. У цьому розумінні, міжнародна группа експертів прямо підкреслює, що як кібератаки, так і “активна кібероборона” розглядаються як засоби ведення війни, якщо вони здійснюються в межах збройного конфлікту та мають законні цілі та мету. Неможливо не зазначити, що Таллінський посібник є першою комплексною працею, яка інтегрувала кібероборону у сферу міжнародного гуманітарного права.

Крім зазначеного, у доктрині детально проаналізовано поняття кібероперацій та їхній зв'язок із загальним міжнародним правом, у розумінні

основних принципів міжнародного права. Окрема увага приділяється у застосовності положень Статуту ООН до кібероперацій, як, наприклад, право на самооборону, незастосування сили або непорушність державного суверенітету.

Не менш важливим здобутком Таллінського посібнику 2.0 є пояснення застосовності міжнародного звичаєвого права до КП, зокрема через призму принципу належної обачності. Зміст цього принципу полягає у м'якому зобов'язанні держави не допускати використання своєї території та кіберінфраструктури для здійснення кібероперацій проти інших держав. Пояснюється спірне у міжнародній науковій спільноті питання обов'язковості цього принципу та винятки з необхідності його застосування.

Окрім згаданого, науковцями-розробниками було проаналізовано актуальність міжнародної судової практики у сфері кіберпростору, зокрема, на основі рішень Міжнародного суду ООН, а також - його Статуту.

Перша версія посібника була прийнята у 2013 році та центр уваги зосереджувався на міжнародно-правовому розгляді кібероперацій під час збройних конфліктів та праві держави на самооборону в цифровому вимірі. Друга та актуальна у 2026 році версія, опублікована у 2017 році, грунтується на надбаннях першої, проте розширює кібероперації в мирний час, тобто такі, які відбуваються не під час збройних конфліктів або не відповідають критеріям війни. У 2021 році Міжнародна група експертів розпочала підготовку третьої версії, яка включатиме перегляд існуючих розділів та дослідження нових тем, що мають значення для держав, при цьому залучаючи до розробки додатково міжнародні форуми як на регіональних рівнях, так і на міжнародному - ООН, а також академічні дослідження та багатосторонні ініціативи за участю урядів, промисловості та громадянського суспільства. [55]

Аналізуючи джерела міжнародного права у сфері кібероборони, доречно зазначити, що Таллінський посібник 2.0, який є найбільш авторитетною доктриною та, відповідно, одним з джерел міжнародного права зі згаданого напряму, він аргументовано в різних частинах та розділах відсилає до інших джерел міжнародного права.

Продовжуючи аналіз джерел міжнародного права у сфері кібероборони, у цьому контексті логічною згадкою є дослідження значення міжнародного звичаю та його ролі у регулюванні КП. Оскільки за відсутності спеціальних конвенцій частіше за все міжнародно-правовий звичай виступає гнучким регулятором міжнародних відносин. У випадку кібероборони та кіберпростору загалом, серед звичаїв центральне місце посідає принцип due diligence (належна обачність).

Цей принцип, який фактично відтворює стандарт очікуваної поведінки держав, є широко використовуваним у різних сферах міжнародних відносин та міжнародного права, відповідно до якого держави повинні здійснювати належну обачність, забезпечуючи при цьому невикористання або протидію використанню своєї території та об’єктами, над якими здійснюється державний суверенітет, для заподіяння шкоди іншим державам. У контексті кіберсфери належна обачність полягає у недопущенні державою використання своєї території або кіберінфраструктури для здійснення кібероперацій, які спрямовані проти інших держав. [54]

Лектор Школи права при Ессекському університеті у Великій Британії, Антоніо Коко (Antonio Coco) у своїй статті “‘Cyber Due Diligence’: A Patchwork of Protective Obligations in International Law” розглядає належну обачність як перспективний механізм забезпечення миру та безпеки у цифровому просторі, оскільки вимагає від держав докладати максимальних зусиль для запобігання, припинення та усунення потенційної загрози, спричиненої внаслідок кібероперацій, які корегувалися або здійснювалися з території відповідної держави, незважаючи при цьому на джерело

походження операцій такого роду. Зокрема, автором в якості прикладу наводиться пандемія COVID-19, під час якої країни-учасниці Європейського Союзу “закликали” кожну країну дотримуватись зазначеного принципу та вживати відповідні заходи проти суб’єктів, які провадять діяльність у цифровому просторі, що містить негативний ефект, у відповідності до міжнародного права. Водночас, Антоніо Коко акцентує увагу щодо спірності питання стосовно обов’язковості держави вжити запобіжні або контрзаходи, оскільки, як він посилається на доповідь 2015 року Групи урядових експертів ООН з питань сприяння відповідальній поведінці держав у кіберпросторі в контексті міжнародної безпеки, ухваленій консенсусом ГА ООН, “держави не повинні свідомо дозволяти використовувати свою територію для міжнародно-протиправних діянь із застосуванням інформаційно-комунікаційних технологій”, де відповідне положення прямо сформульовано як добровільна та необов’язкова норма. В оригінальному фрагменті тексту доповіді це підтверджується безпосередньо англійським дієсловом “should”, тобто у значенні “мають” або “слідувало б”, що вказує на наполегливу рекомендацію, але ж ніяк не зобов’язання. На думку автора, надмірна зосередженість наукової спільноті на терміні належна обачність та його застосовності до КП призвело до підходу за принципом “‘all-or-nothing”: або досягнуто консенсусу щодо кіберпросторової належної обачності, або існує юридична прогалина, яка призводить до відсутності юридичних зобов’язань та передбачає добровільну основу такої діяльності.

Попередньо згадувана викладач Школи права Абердінського університету у Великій Британії, Ірен Коузігоу у своїй праці зазначає рішення Міжнародного суду ООН у справі протоки Корфу, The Corfu Channel Case (United Kingdom v. Albania) 1949, згідно з яким кожна держава зобов’язана “не допускати свідомо використання своєї території для дій, що суперечать правам інших держав”, підкреслюючи позитивне зобов’язання держав запобігати використанню своєї території або будь-якої іншої зони, на яку

поширюється виключна територіальна юрисдикція цієї держави, для здійснення діяльності, яка завдає або має на меті завдати шкоду суб'єктам або об'єктам, які перебувають під територіальним суверенітетом іншої держави. Ірен Коузігоу щодо КП наводить у приклад окрему думку судді МС ООН у справі 2003 року Islamic Republic of Iran v. United States of America, зокрема вказуючи, що обов'язок запобігати шкідливій транскордонній діяльності, яка здійснюється з території держави або підконтрольної їй території, застосовується у тому числі до кіберпростору, шляхом встановлення, наприклад, місцезнаходження комп'ютера, з якого здійснюється шкідливий кібератак. Автором також було звернуто увагу на іншу справу Міжнародного суду ООН - Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), в якій судом було визнано обов'язок Нікарагуа запобігати використанню своєї території як транзитного маршруту для незаконного постачання зброї повстанцям у Сальвадорі. Отже, Ірен Коузігоу, проводячи аналогію, зауважила, що обов'язок запобігати негативному впливу у КП поширюється у тому числі у випадках, коли така діяльність може транзитуватись територією іншої країни. [70]

Повертаючись до справи щодо протоку Корфу та розглядаючи її через призму позиції міжнародної групи експертів, яка займалась розробкою Таллінського посібника 2.0, варто зазначити, що експерти хоча і визнали позицію щодо обов'язковості запобіганню шкідливої діяльності, але жоден з членів експертної групи такий підхід не розділив. Основна аргументація полягала так само, як і було зазначено попередньо, у трактуванні слів "should" та "must", оскільки перше значить "повинні", а друге - "зобов'язані". У цьому зв'язку на державу не покладається прямий обов'язок запобігати, натомість запобігання "твердо рекомендується". При цьому, експерти зауважили, що принцип належної обачності тривалий час відображений у міжнародній судовій практиці та "виходить" із принципу державного суверенітету і тому є загальним принципом, але обов'язковим у

кіберконтексті. Додатком обґрунтуванням у цьому випадку слугувала теза, що “нові технології підпадають під дію вже існуючого міжнародного права за відсутності прямої вказівки щодо їх виключення або винятковості”. [54]

У контексті кібероборони, які є різновидом кібероперацій, міжнародна група експертів наголосила на застосовності цього принципу як у випадку коли такі операції провадяться державними інституціями, так і недержавними суб’єктами. Якщо у першому випадку головна аргументація ґрунтувалась на тому, що держава здійснює контроль над всією кіберінфраструктурою, яка розміщена в межах її території, а також перебуває під її виключним контролем (дипломатичні представництва, морські та повітряні судна), і тому несе тягар відповідальності за незавдання шкоди іншим країнам. Хоча у цьому зв’язку, Таллінським посібником виокремлено виняткові випадки, як, наприклад, ведення кібердіяльності, яка не є забороненою, як наприклад шпигунство. Окрім цього, міжнародна група експертів наголосила на тому, що міжнародне право порушують держави, а не фізичні особи чи приватні суб’єкти і тому, на їхню думку, виключно кібероперації, здійснювані державами або приписувані державам, порушують принцип недоторканності суверенітету. Водночас, з іншого боку, експерти погодились, що у деяких випадках принцип належної обачності у світлі останніх світових тенденцій є застосовним до кібероперацій, здійснюваних недержавними суб’єктами, які, як вже зазначалось, хоча і не порушують міжнародного права, тим не менш, завдають шкоди іншим державам. В якості прикладу було наведено незаборонені кібероперації, які здійснюються недержавними суб’єктами, але, якби вони б здійснювались державами, то вважались би забороненими. Водночас, точний поріг збитків, з досягненням якого застосовується принцип належної обачності вважається невизначеним у міжнародному праві і обмежується змістом “серйозні негативні наслідки”. [54]

Таким чином, принцип належної обачності демонструє м’який обов’язок держав запобігати використанню їхньої кіберінфраструктури для

здійснення шкідливим кібероперацій. Цей принцип переважно спрямований на забезпечення належної поведінки держав у мирний час, в той час як міжнародне гуманітарне право, або право війни, визначає межі дозволеної діяльності під час збройних конфліктів. У цьому контексті, важливо дослідити застосовність міжнародного гуманітарного права до кіберпростору, як джерела міжнародного права у сфері кібероборони.

За Таллінським посібником, кібероперації, попри свою відносну новизну, здійснювані під час міжнародного або неміжнародного збройного конфлікту, підпадають під сферу дії міжнародного гуманітарного права, хоча в ключових міжнародно-правових актах останнього відсутні спеціальні норми, які регулювали б такі операції. Водночас, це питання залишається предметом дискусій, оскільки ключовим, як і у випадку застосовності принципу належної обачності, є невизначеність меж, з досягненням яких вимагається втручання. Міжнародна група експертів наводить два приклади із історії, де у 2007 році Естонія зазнала проти себе тривалих кібероперацій, але право збройних конфліктів було незастосовним через недостатність у ситуації “рівня збройного конфлікту”, а також збройні конфлікти між Грузією та російською федерацією у 2008 році та Україною і російською федерацією, коли норми міжнародного гуманітарного права були застосовані. За логікою експертів, в останніх двох прикладах застосовність права збройних конфліктів мала місце через складний характер бойових дій, які включали в себе фізичну конфронтацію, а не лише цифрову, зокрема стверджується, що для застосування міжнародного гуманітарного права необхідно також існування зв’язку між відповідною кібердіяльністю та конфліктом. [54]

Слід вказати, що проблема застосування права збройних конфліктів до кібероперацій також зумовлена надмірною складністю із встановлення суб’єкта, який здійснює кібердіяльність, його місцезнаходження, зв’язку із державою, а також передбачити можливий об’єкт нападу.

Загалом, у посібнику підлягає розгляду лише кібератаки у значенні “кібероперації”, хоча і вказується, що зміст поняття не обмежується лише ними, тому важливим доповненням буде акцент на так званій “активній кібероборонi”, яку у цьому зв’язку слід розуміти як контр-кібератака здійснена в межах оборони.

Аналогічно до попереднього, міжнародна група експертів стверджує, що застосування права збройних конфліктів у сфері кібероперацій в контексті неміжнародних збройних конфліктів є суперечливим та неоднозначним, що пояснює тим, що держава зберігає певні права та обов’язки у сфері, наприклад, правоохоронної діяльності, і тому вірогідніше буде застосовуватись внутрішнє право та міжнародне право, регулююче права людини, а не право збройних конфліктів. [54]

Тим не менш, доречно буде згадати застереження Мартенса, яке знайшло своє відображення в Женевських конвенціях, та суть якого звучить наступним чином: “оскільки технології людства постійно розвиваються і тому неможливо створити абсолютний та вичерпний перелік заборонених засобів ведення війни, міжнародна спільнота під час збройних конфліктів, обираючи засоби ведення війни, має виходити із принципів міжнародного права, а також принципів гуманності та людяності”.

Виходячи із базиса, який заклав Мартенс у своєму застереженні, можна дійти висновку, що хоча МГП не містить норм, які прямо регулюють кібероперації, заснований ним підхід, який був офіційно закріплений у праві збройних конфліктів, створює правове підґрунтя для регуляції кібероперацій. При цьому, у міжнародному гуманітарному праві чітко визначено поняття цивільної та військової інфраструктури, із прямою забороною атак на першу і тому здійснення кібероперацій, у тому числі кібероборони, проти цивільних об’єктів є неприпустимим, що вкотре підтверджує те, що міжнародне гуманітарне право слід вважати джерелом у сфері кібероборони.

Розглядаючи кібероборону, як різновид оборони, не можна не вказати Статут ООН, який закріплює фундаментальні принципу у сфері миру та світової безпеки. Професор права Колумбійської школи права Метью Ваксман (Matthew C. Waxman) в одній із своїх праць - “Cyber Attacks as "Force" under UN Charter Article 2(4)”, дослідив якою мірою Статут ООН регулює кібератаки та, пов’язані з ними наступальну та оборонну діяльність у КП. Зокрема, він акцентував увагу на адаптивності статті 2(4) Статуту до кібератак, оскільки вона містить пряму заборону погрозу силою або її застосування. На його думку, саме ця стаття є відправною точкою, яка відображає фундаментальні принципи, на яких ґрунтується більшість міжнародно-правових норм у сфері міжнародної безпеки. У праці він також виокремив допустимість застосування сили у відповідь в контексті 51 статті Статуту, яка надає право на самооборону, до змісту поняття якої належить і кібероборона. [13]

Доктор Амр Еззат Махмуд Елхав (Dr. Amr Ezzat Mahmoud Elhaw) зазначив, що у випадку, коли кібератаки, які відповідають юридичному визначенню “збройного нападу”, можуть слугувати підставою для реалізації права на самооборону, у тому числі у цифровому просторі. Водночас, він звертає увагу, що кібероборона буде в межах правового поля статті 51 Статуту лише у відповідь на застосування сили на збройних напад держави, а не недержавного суб’єкту, за винятком, коли недержавні дії можуть бути атрибутовані державі-покровительці або держави-замовниці цих операцій. [86]

У Таллінському посібнику додатково до попереднього зазначається обов’язкова наявність транскордонного характеру кібератак задля можливості легального застосування кібероборони. [54]

Резюмуючи наведене вище, кібероборона існує в межах правового поля права на самооборону, гарантованого статтею 51 Статуту ООН, що в свою

чергу підтверджує факт того, що Статут ООН є джерелом міжнародного права у сфері кібероборони.

Резюмуючи вищевикладене, міжнародно-правове регулювання кібероборони перебуває на стадії активного формування. Наразі відсутній єдиний універсальний міжнародно-правовий акт, який би комплексно визначав межі, механізми та порядок здійснення оборонної діяльності у КП. Незважаючи на це, сформувався значний доктринальний та нормативний базис, який дозволяє застосовувати чинні міжнародно-правові норми до кіберпростору та кібероперацій.

Джерелами міжнародного права відповідно до статті 38 Статуту Міжнародного Суду ООН є міжнародні конвенції, міжнародні звичаї, загальні принципи права, а також судова практика та доктрина найбільш авторитетних фахівців у галузі права. За відсутності спеціалізованої конвенції, ці джерела формують основу сучасного правового регулювання кібероборони.

Значний внесок у формування сучасного розуміння кібероборони здійснили міжнародні дослідники та експерти. Зокрема, Джозеф Най розглядає міжнародне право як один із ключових механізмів довгострокового стримування кіберконфліктів. Існуючі міжнародні норми можуть стримувати кіберагресію шляхом створення репутаційних, політичних та економічних втрат для держави-агресора. Однак їхня ефективність у сфері кіберпростору знижується через особливості цифрового середовища, насамперед анонімність суб’єктів кібердіяльності та подвійне призначення багатьох цифрових технологій.

Особливе місце серед джерел міжнародного права у сфері кібероборони займає наукова доктрина - Таллінський посібник 2.0. Хоча він не має юридично обов’язкової сили, він є комплексним науково-практичним коментарем, який систематизує підходи до застосування міжнародного права у КП. Таллінський посібник містить значну кількість правил та коментарів,

які охоплюють: питання державного суверенітету, права на самооборону, незастосування сили, міжнародного гуманітарного права та відповідальності держав у кіберпросторі.

Таллінська дирекція визнає повну застосовність загального міжнародного права до кібероперацій та кібероборони. У межах цієї концепції кібероперації, які здійснюються під час міжнародних або неміжнародних збройних конфліктів, підпадають під сферу дії міжнародного гуманітарного права. При цьому держави зобов'язані дотримуватись основоположних принципів права збройних конфліктів, зокрема принципу розрізнення цивільних і військових об'єктів, принципу пропорційності та принципу військової необхідності.

Міжнародне звичаєве право застосовується до сфери кібероборони. Ключове значення у цьому контексті має принцип due diligence. Його зміст полягає у необхідності недопущення використання території або кіберінфраструктури держави для здійснення шкідливих кібероперацій проти інших держав.

Разом із тим, питання юридичної обов'язковості принципу належної обачності у КП залишається дискусійним. Частина науковців та міжнародних експертів вважає його загальним принципом міжнародного права, який поширюється і на цифрове середовище. Інші - що відповідні міжнародні документи містять переважно рекомендаційні формулювання та не створюють прямого юридичного обов'язку для держав. Попри це, міжнародна судова практика, зокрема справа про протоку Корфу, підтверджує існування обов'язку держав не допускати використання своєї території для діяльності, що завдає шкоди іншим державам. У контексті кіберпростору цей підхід трансформується в обов'язок держави вживати заходів для запобігання використанню її кіберінфраструктури для здійснення шкідливих кібератак.

Міжнародне гуманітарне право є одним із ключових джерел міжнародного права у сфері кібероборони. Незважаючи на відсутність спеціальних норм, присвячених кібероперaціям, положення Женевських конвенцій та основні принципи права збройних конфліктів поширюються і на цифровий простір. Особливе значення у цьому контексті має застереження Мартенса, відповідно до якого навіть за відсутності прямого нормативного регулювання сторони конфлікту зобов'язані керуватися принципами гуманності та загальними принципами міжнародного права. Це створює правове підґрунтя для поширення міжнародного гуманітарного права на кібероперації та кібероборону.

Право збройних конфліктів забороняє здійснення кібератак проти цивільної інфраструктури та цивільних об'єктів. Відповідно, кібероборона повинна здійснюватися виключно з дотриманням принципів гуманності, пропорційності та розрізнення військових і цивільних цілей.

Дослідження положень Статуту ООН дозволило дійти висновку, що цей міжнародний акт також є фундаментальним джерелом права у сфері кібероборони. Стаття 2(4) Статуту закріплює заборону погрози силою або її застосування, а стаття 51 гарантує державам право на самооборону у випадку збройного нападу. У сучасних умовах це право поширюється і на КП. Водночас встановлено, що застосування права на самооборону у відповідь на кібератаку можливе лише за умови, якщо така атака досягає рівня збройного нападу та має транскордонний характер.

Таким чином, міжнародно-правове регулювання кібероборони формується на основі комплексного поєднання міжнародних договорів, міжнародних звичаїв, загальних принципів права, судової практики та доктринальних джерел. Незважаючи на відсутність єдиного спеціалізованого міжнародного договору у сфері кібероборони, сучасне міжнародне право містить нормативний та доктринальний базис для регулювання кіберпростору.

РОЗДІЛ 2. Міжнародно-правове регулювання кібероборони

2.1. Кібероборона у системі jus ad bellum

Jus ad bellum, дослівно з латинської - “право на війну”, один із базових інститутів міжнародного публічного права, який включає в себе міжнародно-правові норми та принципи, які визначають правомірність та підстави застосування збройної сили державою.

У своїй фундаментальній праці “War, Aggression and Self-Defence”, Йорам Дінштейн (Yoram Dinstein) зазначив, що jus ad bellum визначає умови, за яких держава може законно вдатися до застосування збройної сили. При цьому він акцентує увагу на тому, що у світлі розвитку міжнародного права та внаслідок глобального переосмислення світового порядку після завершення Другої світової війни у 1945 році, дефініція цього принципу відійшла від загальної концепції “права на війну” до моделі категоричного обмеження застосування збройної сили та деталізації виняткових ситуацій такого використання. [94]

У Статуті ООН статтею 2 (4) чітко визначено, що “усі Члени утримуються в своїх міжнародних відносинах від погрози силою або її застосування проти територіальної цілісності, або політичної незалежності будь-якої держави, або будь-яким іншим чином, несумісним із Цілями Об’єднаних Націй”. [11]

На доповнення щодо застосування сили, Міжнародний суд ООН підкреслив, що заборона застосування сили та, відповідно, право на самооборону застосовується до “будь-якої сили, незважаючи на зброю, яка застосовується”. Таким чином, Суд прямо підкреслив, що вид зброї в цьому зв’язку не має значення, оскільки важливим є факт її неправомірного застосування і тоді доречно резюмувати, що застосування сили, наприклад - шкідливого програмного забезпечення, у цифровому просторі підпадає під дію Статуту ООН. [54]

Доповнюючи позицію Міжнародного Суду ООН, доречно виокремити офіційну позицію Уряду Нідерландів, яка полягає в можливості застосування у відповідь на кіберагресію зброю як кібернетичного характеру, так і кінетичного. [17]

Міністерство збройних сил Французької Республіки у 2019 році оприлюднило офіційну позицію, згідно з якою МГП слід вважати застосовним до кібероперацій під час збройних конфліктів. Зокрема, Францією було наголошено на необхідності дотримання принципів розрізнення, пропорційності та гуманності у кібепросторі. [38]

При цьому, міжнародні експерти, які здійснювали розробку Таллінського посібнику 2.0, в процесі дискусій щодо використання поняття "збройного конфлікту" з акцентом на терміни "збройний" та, відповідно, "зброя", дійшли висновку, що ключовим фактором є не зброя як така, а позиція щодо наслідків. Якщо наслідки, які спричинила та чи інша кібероперація, є аналогічними тим, що могли виникнути від застосування класичної, у військовому розумінні, зброї, тоді кібероперація за відсутності фізичної зброї трактувалась би як збройний напад. Водночас, було визнано існування окремої позиції щодо відсутності кваліфікації дій як збройного нападу за умови відсутності кіберзброї. Навпаки, ототожнення збройного нападу із застосуванням сили штучно звужує зміст другого поняття, оскільки, як вже було пояснено, наявність кінетичної зброї не є вимогою. [54]

Водночас, не кожне застосування сили досягає рівня збройного нападу. МС ООН підкреслив, що масштаб та наслідки спричинені застосуванням сили не завжди перевищують поріг, який необхідний для кваліфікації операції як збройного нападу. Лише у випадку досягнення або перевищення певного рівня шкодою, заподіяною застосуванням сили, державі надається право відповідати силою у порядку самооборони. Формулювання "масштабу та наслідків" залишається невизначеним у міжнародному праві та трактується у міжнародних судових справах індивідуально до кожної ситуації. Суд хоча і

зазначив, що «розрізняти найтяжчі форми застосування сили, які кваліфікуються як збройний напад, та інші, менш тяжкі форми, які залишаються застосуванням сили», але критерії визначення цих форм надані не були. [54]

Розглядаючи це питання, міжнародні експерти вдаються до аналогій, за якими, наприклад, кіберрозвідка або кіберкрадіжка хоча і є кібероперaціями, які спричинятимуть негативні наслідки, але в міру незначної шкоди не підлягатимуть кваліфікації як збройний напад. В той час, як кібероперація, яка спричиняє загибель людини або завдає серйозні тілесні ушкодження, знищує майно - відповідатиме критеріям масштабності та серйозності наслідків. [54]

На доповнення до цього доречно зазначити результати другої сесії Відкритої робочої групи ООН (Open-Ended Working Group) у лютому 2020 року, а також роботи двох Груп урядових експертів ООН (Group of Governmental Experts) з питань розвитку у сфері інформації та телекомунікацій у контексті міжнародної безпеки у 2013 та 2015 роках, під час яких було підтверджено застосовність міжнародного права, включаючи Статут ООН у сфері цифрового середовища. [30]

У ході конференцій було розглянуто численні підходи держав щодо включення кібератак до змісту збройного нападу, зокрема базуючись на правових позиціях Сполученого Королівства Великої Британії та Північної Ірландії, Французької Республіки, Естонської Республіки та Королівства Нідерланди, оскільки саме ці держави мали найбільш змістовні та конкретизовані підходи до кваліфікації кібератак як збройних нападів. Оскільки кожна із зазначених держав підтвердила факт того, що кібератака може досягати рівня збройного нападу, необхідною умовою є співмірність її наслідків із наслідками атак кінетичного характеру. Позиція Великої Британії полягає у тому, що кібератака спрямована проти критичної інфраструктури, зокрема ядерних об’єктів країни, диспетчерської вежі управління повітряних

рухом, медичні служби - такі операції будуть прирівнені до збройного нападу через потенційність загрози людським життям. Французька сторона визначила як збройний напад кібератаки, які здатні завдати значних людських втрат або істотну фізичну чи економічну шкоду або навіть катастрофу. Естонія вважає, що кібероперація проти цифрової інфраструктури, критично необхідної для функціонування суспільства, підпадає під визначення збройного нападу. Правова позиція Нідерландів вказує, що для кваліфікації кібератаки як збройного нападу необхідно оцінити масштаб та наслідки конкретного інциденту, а також підтвердити транскордонний характер такої атаки. [17]

Так само, як і позиція Нідерландів, так і Таллінської дирекції базується на необхідності акцентувати увагу на транскордонності збройного нападу, як обов'язковому елементі. Цей критерій завжди виконується під час здійсненні як державою, так і недержавними суб'єктами від імені та на замовлення держави, операцій у цифровому середовищі проти іншої держави. Проблемним є питання транзитності операцій, у випадку, коли недержавні суб'єкти здійснюють кібероперації на території однієї держави, але діють від імені іншої, оскільки транскордонність характеру зберігається, але у цьому аспекті вона набуває додатково транзитного значення і тому у правовому полі залишається повноцінно невизначеним та дискусійним. [54]

Крім того, у випадку застосування сили, держава, яка зазнала нападу, у відповідь може застосовувати "контрзаходи". Такі дії визначаються, як ті, що "за інших обставин суперечили б міжнародним зобов'язанням із незастосування сили, але вони набувають правомірного характеру у випадку застосування проти держави-агресора, яка першою вчинила міжнародно-протиправне діяння за умови, що такі контрзаходи мають на меті припинення збройної агресії держави-агресора або забезпечення відшкодування." Варто зауважити, що контрзаходи слід відрізняти від реторсії, оскільки остання полягає у вчиненні правомірних недружніх дій, наприклад у розірванні

дипломатичних або консульських зносин, закритті закордонних дипломатичних установ або висланні дипломатів з країни акредитації. Доречно наголосити, що контрзаходи є мірою дозволеної поведінки, як миттєва реакція не протиправне діяння у міжнародному просторі, і тому вони можуть бути застосовані лише під час вчинення міжнародно-правового діяння, а не після його закінчення як покарання або помста. Контрзаходи, які включають активну кібероборону, мають бути пропорційними завданній шкоді, а не перевищувати її, тобто відповідати принципу пропорційності. До того ж, необхідно розмежовувати поняття колективної самооборони та контрзаходів, оскільки останні можуть застосовуватись виключно державою, яка зазнала збройної агресії. [14]

За Статутом ООН, правомірне застосування сили у відповідь допускається виключно у двох випадках - реалізації права держави на самооборону та у випадку санкціонування відповідних дій Радою Безпеки ООН. При цьому в даному випадку, самооборона може бути як колективною, так й індівідуальною, але при здійсненні цього права держава або держави мають невідкладно повідомити Раду Безпеки ООН для здійснення останньою заходів із підтримки міжнародного миру та безпеки. [11]

Невід’ємне право на колективну чи індивідуальну самооборону закріплено у статті 51 Статуту ООН, яка відображає міжнародно-звичаєве право з цього питання, та передбачає правомірність її застосування виключно у разі збройного нападу до того, як Рада Безпеки ООН не здійснить необхідних заходів із підтримки міжнародного миру та безпеки. [11]

При цьому, право держави на застосування сили в порядку самооборони поширюється не тільки на кінетичні збройні напади, але й на ті, що здійснюються у кіберпросторі. Міжнародна група експертів одностайно дійшла висновку щодо можливості кваліфікації кібероперацій як “збройний напад” за умови комплексності, у розумінні “complex” як “складність” або “багаторівневість”, через призму положень Статуту ООН. У якості

додаткового аргументу щодо цієї позиції, експерти навели у приклад вже згадану позицію Міжнародного суду ООН щодо ядерної зброї, у консультативному висновку якої спосіб здійснення нападу не має значення, натомість, до уваги береться здатність заподіяти надмірної шкоди. Конкретизуючи це питання, було проведено аналогію щодо застосування ядерної, хімічної або біологічної зброї, яка моментально "активує" право на самооборону, оскільки наслідком такої атаки однозначно є серйозні страждання або смерть, і тому аналогія має застосовуватись до кібероперацій, які за своєю метою можуть спричинити або спричинять страждання або смерть людей. [54]

Окрім цього, міжнародним правом, зокрема, Статутом ООН, не передбачена вимога щодо застосування оборонної сили того самого характеру, що і атакуючої. Таким чином, здійснення кібероборонних операцій у відповідь на кібернетичний збройний напад буде еквівалентним та правомірним так само, як і застосування фізичної (кінетичної) сили у відповідь на кібератаку, яка за своїми якісними та кількісними характеристиками відповідає рівню збройного нападу. [11]

За таких обставин виникає проблема щодо застосовності права на самооборону у відповідь на серію кібероперацій за умови, що кожна окремо не досягає рівня загрози з яких вона кваліфікується як збройний напад, але всі вони в сумі - досягають цієї межі. Тобто, чи буде сукупність кібероперацій вважатися збройним нападом, чи кожна дія буде розглядатись окремо. В таком випадку, логічно припустити, що якщо буде доведено факт їхнього взаємозв'язку, який має включати в себе: один і той самий суб'єкт виконував операцію (або замовник); одна й та сама ціль та мета; досягнення в сукупності необхідного рівня масштабу. Виконавцем кібероперацій в цьому зв'язку може виступати як держава, так і недержавний суб'єкт, який представляє державу або дії від її імені чи в її інтересах. Під ціллю слід розуміти в глобальному контексті - інша держава або альянс, а метою -

зменшення військового потенціалу супротивника, політична, економічна, соціальна дестабілізація тощо.

Іншим правомірним випадком здійснення кібероперацій з метою оборони, як вже зазначалось раніше, є санкціонування Радою Безпеки ООН заходів із підтримки миру та безпеки. Статутом ООН уповноважено Раду Безпеки визначати існування загрози або факту порушення миру та надавати рекомендації щодо заходів на його відновлення. [11]

Рада Безпеки має повноваження визнати кібероперації як загрозу миру чи актом агресії in abstracto так само, як це було зроблено щодо поширення зброї масового знищення або міжнародний тероризм. Після ухвалення рішення щодо відповідного визнання, Радою Безпеки розглядається питання щодо вибору та застосування незбройних заходів для виконання рішення про відновлення світової безпеки та миру, таких як економічні або логістичні (поштові, морські, повітряні, радіокомунікаційні та інші) обмеження або розрив дипломатичних відносин. [54]

Саме в цьому контексті може бути застосовано часткове або повне припинення шляхів сполучення у КП. Як було визначено раніше, державний суверенітет поширюється на кіберпростір, оскільки держава здійснює контроль та нагляд над кіберінфраструктурою і в цьому зв’язку створення “цифрової блокади” може розглядатися своєрідною кібероборoною. Оскільки за умови підвищення недоступності власного КП для держави, яка зазнала відповідних санкцій від Ради Безпеки, та створення додаткових “ліній” захисту від несанкціонованого втручання може виступати своєрідною “превентивною кібероборoною”.

В даному випадку, оскільки згідно із Статутом ООН, усі держави-члени Організації Об’єднаних Націй зобов’язані безумовно виконувати рішення Ради Безпеки, закриття доступу до власного кіберпростору шляхом припинення сполучень, у цьому розумінні - взаємообміну даними через

спільні мережі, та провадження “цифрової блокади” доцільно вважати колективною кібероборoною або, щонайменше, різновидом пасивної кібероборони.

Окрім цього, грунтуючись на статті 42 Статуту ООН, у разі недостатності заходів із незбройного врегулювання конфлікту, Радою Безпеки ООН може бути санкціоновано застосування сили, що, як вже було досліджено, включатиме в себе і кібероперації. Таллінська група міжнародних експертів з цього питання навела у приклад ситуацію, за якою одна держава розробляє потенціал ядерної зброї та послідовно ігнорує як вимоги Ради Безпеки припинити таку діяльність, так й економічні санкції. У такому разі уповноваження Радою Безпеки держав на провадження кібероперацій проти цієї держави з метою нейтралізації потенційної загрози із розвитку програми озброєнь не буде вважатися атакою, а навпаки - заходами активної кібероборони. [11; 54]

На підтвердження цієї позиції, Рада Безпеки в своїх Резолюціях може вживати формулювання “усіх необхідних заходів” або його аналогії, що передбачає майже повну необмеженість вибору щодо заходів, окрім конвенційної зброї як хімічна, біологічна або ядерна, для припинення факту загрози світового порядку. Тому кібероперації, в межах правил міжнародного гуманітарного права, підпадають під цю категорію та є законним засобом негайного оборонного реагування. [90]

Водночас, Статутом ООН передбачено можливість звернення Ради Безпеки ООН до міжнародних організацій та регіональних угод для здійснення примусових заходів із припинення акту агресії під контролем Ради. Водночас, статтею 52 Статуту визначено право регіональних угод або організацій на вдавання до заходів із підтримки світового миру та безпеки без прямого дозволу Ради Безпеки. [11]

І хоча у Статуті відсутнє визначення терміну “регіональний”, в межах кваліфікації “регіональної організації” це не має значення, оскільки Рада Безпеки здатна уповноважити будь-яку державу-учасницю та будь-яке об’єднання держав, звертаючись до них напряму, а не до організації, яку представляють ці держави.

Будь-яке застосування сили державою, у тому числі в рамках реалізації права на самооборону, повинно відповідати принципам необхідності та пропорційності, які становлять частину міжнародного звичаєвого права та були визнані Нюрнберзьким процесом.

Принцип необхідності у jus ad bellum передбачає застосування сили на тому рівні, який є об’єктивно необхідним для відбиття майбутнього або припинення вже існуючого збройного нападу. Зокрема, цим принципом встановлено, що застосування збройної сили має бути винятковим, останнім заходом впливу, коли всі інші заходи ненасильницького характеру, зокрема - дипломатичні та економічні, є або недієвими (неефективними), або недостатніми для врегулювання збройного конфлікту. В контексті кібероборони ключовим фактором оцінки необхідності є наявність або навпаки відсутність альтернативних варіантів поведінки для стримування країни-агресора. У цьому зв’язку можна виокремити засоби пасивної кібероборони, які включають в себе стійкість та автоматизованість програмного забезпечення, яке без втручання ззовні, здатне повністю нейтралізувати загрози несанкціонованого втручання у мережеве обладнання. За цією аналогією, якщо активні операції з кібероборони не включають застосування сили та є достатніми для стримування або відбиття збройного нападу, то використання інших заходів із активної кібероборони, які вже можуть завдати непомірної шкоди, суперечитиме критерію крайньої необхідності. [54]

Водночас, якщо операції з кібероборони не можуть обґрунтовано вважатися достатніми для припинення збройного нападу та запобіганням

подальшим атакам як кібернетичного, так і фізичного характеру, правом на самооборону допускається вжиття заходів, які перетинатимуть дозволений поріг застосування сили для повної або часткової нейтралізації джерела небезпеки. В цьому контексті необхідно розуміти зміст джерела небезпеки, тому доречно буде навести приклад умовного збройного конфлікту між державою А та державою Б. Якщо держава А розпочала кібератаки проти держави Б, цілями яких стали веб-сторінки державних органів влади, нейтралізація яких призведе до паралізації електронної взаємодії між державними органами на невизначений строк напередодні проведення надзвичайно важливого вседержавного референдуму, і в держави Б система пасивного кіберзахисту не є достатньою для відбиття атак. То в цьому контексті, операції з кібероборони, спрямовані на тимчасову нейтралізацію джерела загрози - розвідувальному управлінню з кібердіяльності або департаменту кібердіяльності міністерства оборони держави А, буде вважатись необхідним та не порушуватиме цієї умови.

Аналогічна ситуація була приведена у приклад Таллінською дирекцією - групою міжнародних експертів. Оцінювати необхідності з позиції держави, яка зазнала проти себе застосування сили, необхідно виходячи з конкретних обставин конфлікту. Наприклад, якщо держава А здійснючи кібернетичні атаки на кіберінфраструктуру держави Б, зазнала силових кібероперацій з метою самооборони держави Б у відповідь, такі атаки будуть вважатися правомірними та необхідними навіть за умови, якщо держава А ухвалила рішення про припинення кібератак проти Б, а держава Б не знала про це на момент здійснення кібероборони. [54]

Не менш важливий принцип - пропорційності, який після встановлення факту необхідності застосування сили, визначає її допустимий обсяг. Мета цього принципу - це обмеження масштабу, тривалості та інтенсивності оборонних дій, у тому числі в цифровому середовищі, а також встановлення меж, перетин яких призведе до порушення правомірності такого

застосування. Фактично, принцип пропорційності вказує на потребу визначення необхідних для нейтралізації загрози, яка слугувала підставою для реалізації права на самооборону, якісних та кількісних характеристик тієї чи іншої кіберооборонної операції перед її безпосереднім здійсненням. При цьому прямої вимоги щодо відповідності обсягу застосованої сили до сили, використаної під час збройного нападу, не передбачено, оскільки ефективність захисту та обсяги необхідні для його досягнення залежать від конкретного контексту. За певних умов та обставин для успішного відбиття або припинення нападу використовуваний обсяг сили може бути великим, тоді як в діаметрально протилежних - навпаки, меншим. [80]

Принципи пропорційності та необхідності пов’язані між собою, оскільки справедливість підстав для здійснення наступального або оборонного кіберзаходу встановлює наявність справедливої причини, зокрема чи здійснюється така операція у відповідь небезпідставно, тобто за умови, наприклад зовнішньої агресії або реальній загрозі критично важливій інфраструктурі. Водночас, Томас Хурка (Thomas Hurka) зазначає, що “справедливі підстави не відіграють роль у встановленні справедливої причини” і тому сам факт називання таких підстав справедливими є недоречним. Навпаки, він вважає, що у цьому зв’язку відбувається маніпуляція поняттям, оскільки називаючи причину справедливою, при оцінці пропорційності, акцентується увага не лише на позитивному результаті та благах, які плануються досягти шляхом наступальних або оборонних кібероперацій, а навпаки - узаконюючи їх справедливістю підстави навіть при порушенні цього принципу. [62]

На думку Сеани Валентайн Шифрін (Seana Valentine Shiffrin) є неправильним одностороннього застосування принципу пропорційності в контексті релевантності критеріїв під час оцінки пропорційності. Вона окремо зазначає, що оцінка пропорційності у випадку завдання шкоди має мати таку саму релевантність, як і у випадку отримання вигоди. Наводячи у

приклад необхідність співмірного врахування економічних витрат та економічних переваг при оцінюванні пропорційності. Водночас, С.В. Шифрін вказує на те, що шкода повинна бути більшим важелем впливу у розрахунках пропорційності. Вона виходить із позиції, що керуючись науковою літературою щодо метафізики шкоди, усунення шкоди є морально важливішим, ніж завдання еквівалентної вигоди. [32]

Однак факт того, що як завданна шкода, так і набута вигода внаслідок наступальних або оборонних кібернетичних операцій, хоча і безпосередньо не пов’язані із “справедливою підставою” (just cause), вони повинні враховуватись при оцінці пропорційності. Крістофер Джей Еберлі (Christopher J. Eberle) зазначає, що блага та негативні наслідки мають значення для оцінки пропорційності, але не залежать виключно від справедливої підстави. Розрахунок вигоди від кібероперації є необхідним щонайменше для визначення доцільності такої операції через призму потенціалу та розміру нанесеної шкоди як державі-цілі, так і власній державі як під час здійснення операції, так і в коротко- та довгостроковій перспективі після її завершення. У цьому зв’язку він проводить аналогію за умови неміжнародного збройного конфлікту, в якому у війні уряду та збройних сил проти повстанської армії, яка здійснює атаки на прикордонні території держави, здійснення операції проти повстанців може бути надзвичайно витратною, але в свою чергу це призведе до суттєвих економічних переваг в довгостроковій перспективі у зв’язку із припиненням збройного конфлікту та стимулюванням економічного розвитку. Так само, здійснення державою операції з активної кібероборони у відповідь на численні кібератаки недержавного суб’єкта іншої країни, ця кібероборонна операція позбавить можливості здійснювати майбутні кібератаки та завдасть економічної шкоди державі, яка не забезпечила припинення кібератак згідно з принципом належної обачності. При цьому, у довгостроковій перспективі ця кібероборонна операція сприятиме економічній вигоді шляхом підвищення

рівня довіри та покращення умов міжнародної торгівлі. І тому економічні вигоди повинні визнаватися релевантними у більш широкому сенсі, оскільки вона рідко мають виключно економічний характер і впливають на добробут суспільства загалом, а тому повинні враховуватись при визначенні пропорційності. [67]

Водночас, принцип пропорційності під час здійснення кіберзаходів може порушувати межі допустимого втручання та співвідношення між потенційною військовою перевагою та можливими гуманітарними наслідками, які регулюються jus in bello. Це пояснюється тим, що у випадку як наступальних кібероперацій, так і оборонних, існує проблема із встановлення потенційної шкоди фізичним особам. Якщо під час операції з активної кібероборони, яка спрямовується виключно на відстеження мережі правоохоронної служби держави-агресора з метою її зламу та отримання доступу до інформації для вдосконалення власних систем захисту та розвитку кіберможливостей, то навіть враховуючи ризики витоку персональних даних цивільних осіб, принцип пропорційності буде дотримано без порушення міжнародного гуманітарного права. [61]

У своїх дослідженнях принципу пропорційності, зокрема у сфері кібероборони, Джефф МакМахан (Jeff McMahan) та Роберт МакКім (Robert McKim) зазначили, що допустимість врахування певної вигоди від кібероперації може залежати від характеру використовуваних засобів, тобто за умови існування альтернатив для досягнення цілі кібероборони, то варто застосовувати ту, що завдає найменшої шкоди. За аналогією, у випадку необхідності нейтралізувати військове командування, яке розташовано у місті та представляє собою мобільний штаб, використання кінетичної сили для фізичної нейтралізації цілі у випадку, коли можна здійснити операцію у цифровому просторі та паралізувати зв’язок із військовим угрупуванням, яке діє відповідно до наказів центру, - буде недоречним та таким, що ймовірніше порушить принцип пропорційності, особливо за умови цивільних втрат.

Таким чином, якщо заходи з кібероборони не завдають значної шкоди, усі позитивні наслідки мають бути включеними до оцінки пропорційності.

У цьому контексті шкода, якщо вона заподіяна цивільному населенню, автоматично сама по собі виступає вагомим контраргументом щодо допустимості та доцільності такої операції. Безумовно, що навіть за наявності надзвичайно великих побічних вигод, як наприклад зростання економічного розвитку в регіоні, вони не будуть рівними завданій шкоді особливо за умови загибелі цивільного населення. Проте, у випадку коли єдина шкода, яку зазнало цивільне населення внаслідок кібероперації є часткове або повне порушення роботи Інтернету - доцільність кіберзаходу через призму принципу пропорційності простежується. [63; 64]

Проте з іншого боку, існує проблема, яка полягає в тому, що суб'єкти здійснення операцій з кібероборони та кібернаступу під час оцінки пропорційності повинні враховувати лише заплановані наслідки у розумінні завданої шкоди та отриманої від цього вигоди, тоді як побічні, незаплановані переваги значення не мають. Таким чином, у разі здійснення кібернетичної операції з метою протидії кіберагресії прораховуються та враховуються в оцінці пропорційності лише ті наслідки та шкода, які безпосередньо пов'язані з метою провадженої операції. У цьому зв'язку ймовірна шкода залишається як поза межами регулювання, так і поза увагою під час оцінювання за принципом пропорційності. Натомість, у моральній та політичній філософії, зокрема у межах дотрини подвійного ефекту (the Doctrine of Double Effect), ті наслідки, що хоча і не були включені до складу мети, але мали б, оскільки були передбачуваними - визнаються актуальними. При цьому формулювання мети кібероперації з навмисного завдання шкоди може оцінюватись як більш негативне, якщо це розглядати з принципів моральності, але такий підхід ґрунтується суто на припущеннях о неправомірності мотивах виконавця або замовника кібероперації та не має міжнародно-правового підґрунтя. [61]

Водночас, аналізуючи принцип пропорційності у сфері кібероборони, виникає проблема щодо його застосування в окремих випадках. Наприклад, як було вказано раніше щодо визначення сукупності кібератак як повноцінного збройного нападу, аналогічна проблема наявна й у питанні кібероборони. Якщо серія кібератак, кожна з яких за рівнем наслідків не відповідає порогу збройного нападу, то за сукупністю цих операцій це може вважатися збройним нападом, якщо вони пов'язані спільним суб'єктом та метою і в сумі досягають необхідного масштабу та рівня збройного нападу. В такому випадку виникає проблема щодо трактування сукупності кібероборонних операцій проти держави-агресора, якщо в сумі вони значно перевищують рівень завданої шкоди, як порушення принципу пропорційності. Проводячи паралель, варто навести у приклад дві різних ситуації.

У першому держава А здійснила кібератаку проти держави Б, яка входить до альянсу держав. За статутом цього альянсу, напад на одного з учасників є підставою для здійснення контрзаходів, користуючись правом на колективну самооборону. У цьому зв'язку, усі держави-члени альянсу здійснили кібероборонні операції, кожна з яких окремо за рівнем шкоди є меншою або відповідною тій, що була завдана державі Б.

У другому сценарії одна держава здійснює серію кібератак на столицю другої держави, нейтралізуючи зв'язок на невизначений термін часу. У відповідь, у рамках децентралізованої організації кібероборони, різні військові угрупування збройних сил держави, яка зазнала нападу, здійснюють серію кібероборонних операцій проти держави-нападниці. Кожна з кібероборонних операцій відповідає завданій шкоді за рівнем або є нижчою.

В обох випадках за сукупністю кібероперацій з оборони рівень завданої шкоди очевидно був більший та, відповідно, порушував принцип пропорційності. Це пояснюється тим, що як альянс, так і децентралізовані військові угрупування у складі збройних сил, діяли з однаковою метою, від

одного й того самого суб’єкта (представляючи інтереси альянсу та держави відповідно).

Отже, jus ad bellum у сучасному міжнародному праві трансформувалося із концепції “права на війну” у систему жорстких обмежень щодо застосування сили.

Застосування сили визнається правомірним лише у виняткових випадках, прямо передбачених Статутом ООН. Кібероперації, наслідки яких є співмірними із наслідками кінетичних атак, можуть кваліфікуватися як застосування сили або як збройний напад, що активує право держави на індивідуальну чи колективну самооборону.

Підходи держав та міжнародних експертів свідчать про поступове формування звичаєвої міжнародно-правової практики щодо застосовності Статуту ООН до кіберпростору. Зокрема, правові позиції Франції, Нідерландів, Великої Британії та Естонії підтверджують можливість кваліфікації кібератак як збройних нападів за умови співмірності їхніх наслідків із кінетичними атаками. Аналогічного підходу дотримується й Талліннський посібник 2.0, який акцентує увагу не на технічному характері зброї, а на ефекті та наслідках її застосування.

Важливими у сфері кібероборони є принципи необхідності та пропорційності, які визначають допустимі межі оборонного реагування. Принцип необхідності вимагає, щоб застосування сили мало місце за відсутності ефективних ненасильницьких альтернатив. Принцип пропорційності обмежує масштаб, інтенсивність і тривалість кібероборонних операцій обсягом, необхідним для нейтралізації загрози.

Міжнародне право не встановлює вимоги щодо ідентичного характеру засобів оборони, а тому відповідь на кібератаку може здійснюватися як кібернетичними, так і кінетичними засобами за умови дотримання критеріїв необхідності та пропорційності.

Jus ad bellum поступово адаптується до цифрової реальності. Відсутність уніфікованих критеріїв кваліфікації кібератак, визначення порогу збройного нападу та оцінки пропорційності кібероборони свідчить про те, що сфера міжнародного права продовжує перебувати на етапі активного формування та розвитку.

2.2. Кібероборона у системі jus in bello

У попередньому розділі цієї роботи було проаналізовано питання кваліфікації кібернетичних атак як збройного напад у розумінні Статуту ООН, правових позицій держав та Міжнародного суду ООН з урахуванням наукових напрацювань, включаючи найбільш авторитетну доктрину з порушеного питання - Таллінського посібнику. Оскільки кібератаки можуть досягати рівня збройного нападу, за умови їхньої відповідності масштабам та наслідкам кінетичним застосуванням сили.

Світове визнання можливості існування збройного нападу у КП, можливості застосування державами права на колективну або індивідуальну самооборону, а також здатності санкціонування Радою Безпеки ООН рішень про здійснення заходів із підтримки світового миру та безпеки у відповідь на кіберагресію створює підстави для визначення права, що має застосовуватись. Оскільки було з’ясовано, що збройний напад є юридичним фактом, який свідчить про виникнення міжнародного збройного конфлікту, відтак відповідні правовідносини підпадають під сферу правового регулювання міжнародного гуманітарного права.

Міжнародне гуманітарне право є галузю міжнародного публічного права, яке встановлює правила ведення збройних конфліктів з метою мінімізації насильства під час війни шляхом правового регулювання відносин між державами щодо захисту жертв війни, включаючи цивільне населення та військовополонених, обмеження засобів та методів ведення війни. [7]

Таким чином, МГП не втрачає здатності правового регулювання та обмеження під час збройних конфліктів, якщо площина, в якій відбуваються воєнні дії знаходиться у віртуальному, тобто цифровому середовищі. До того ж, вже згадуване у цій роботі застереження Мартенса, яке закріплене в джерелах міжнародного гуманітарного права, а саме в Додаткових протоколах I та II до Женевських конвенцій, вказує обов'язок з дотримання державами-сторонами збройного конфлікту гуманного та людяного підходу до вибору методів та засобів ведення війни навіть у випадку, коли такі засобу або методи не є забороненими. [105; 106]

Включення застереження Мартенса до Женевських та Гаазьких конвенцій в першу чергу розширило сферу застосування гуманітарного права в еволюційному розумінні, оскільки передбачило можливість обмежувати правом Женеви та правом Гааги не лише ті засоби та методи ведення війни, що існували на час його імплементації до відповідних конвенцій, а в тому числі ті, що мали б з'явитись в майбутньому в процесі технологічного розвитку та потенційної практичної зміни в підходах до ведення збройних конфліктів. Гаазьким міжнародним судом також було визнано позитивний вплив функціонування декларації Мартенса, підкресливши його ефективність в контексті адаптивності до світових тенденцій в контексті розвитку військових технологій. При цьому, статтями 35-36 Додаткового протоколу I до Женевських конвенцій прямо вказується на відсутність у сторін конфлікту абсолютного права на вибір засобів та методів ведення війни, натомість наголошується обов'язок утримання від використання тих засобів, які здатні спричинити надмірні ушкодження або страждання, а також визначати правомірність нових засобів ведення війни, виходячи як з положень права збройних конфліктів, так і з інших міжнародно-правових актів.[4]

Сполученими Штатами Америки та іншими країнами була підтримана позиція, що право збройних конфліктів є застосовним до кіберпростору. Кібероперація розглядатиметься як збройний напад в залежності від її

наслідків, а не від використаних засобів її вчинення, оскільки вона має призвести до знищення майна або заподіянні значної шкоди людям. Окремо підкреслюючи на складності запобіганню не стільки операціям, які підпадають під закони міжнародного гуманітарного права, скільки кібератакам суб'єктів, які не досягають рівня збройного нападу. [24]

Зокрема, реалізація кіберзасобами права держави на самооборону не перебуває поза межами jus in bello, оскільки навіть у випадку правомірної самооборони держава зобов'язана утримуватись від попадань і тим більше руйнувань цивільної інфраструктури, особливо тієї що вважається критичною, тим самим забезпечуючи розмежування військових та цивільних цілей, а також враховувати потенційні гуманітарні наслідки до проведення кібероперацій.

Особливе значення у формуванні застосовності міжнародного гуманітарного права до кібероборони відіграє Таллінський посібник, в якому пояснено логіку та принципи застосування окремих положень міжнародного гуманітарного права до збройних конфліктів у КП. Зокрема розкривається сутність базових принципів таких як розрізнення цивільних та військових об'єктів, принцип пропорційності та військової необхідності, а також обов'язок вживати запобіжних засобів під час проведення операцій у КП. Якщо принципи пропорційності та військової необхідності були проаналізовані в межах цього дослідження, додатковий аналіз яких у контексті міжнародного гуманітарного права буде проведено за необхідності додаткової конкретизації, то принцип розрізнення є надзвичайно важливим для розуміння застосування права збройних конфліктів у кіберпросторі і тому його буде розглянуто окремо.

Принцип розрізнення, закріплений статті 48 Додаткового прокотолу I до Женевських конвенцій, полягає у розрізненні, тобто не ототожнюванні, цивільного населення та комбатантів, а також цивільних та військових об'єктів та відповідно спрямовуванні атак виключно проти воєнних об'єктів.

У відповідності до положень Додаткового протоколу І та Женевської конвенції ІІІ, цивільне населення не може бути об’єктом нападу і складається із цивільних осіб, а цивільними особами прийнято вважати будь-яких осіб, які не є:

1. представниками особового військового складу збройних сил сторони збройного конфлікту, включно із ополченням, добровольчими загонами та організованими руху опору, які належать до однієї зі сторін конфлікту та за умови, що вони: мають постійний розпізнавальний знак, який видно на відстані, відкрито носять зброю, здійснюють свої операції відповідно до законів та звичаїв війни під командуванням законної особи, яка відповідає за їхні дії;

2. жителями неокупованих територій, які під час наближення ворога озброюються і не формуючись в організовані збройні сили відкрито носять зброю та дотримуються правил та звичаїв війни. [105]

Заборона здійснення нападів, які включають в себе як оборонні так і наступальні кібероперації, історично походить із згадуваної в першому розділі цієї роботи Санкт-Петербурзької декларації 1868 року, яка передбачала, що “єдиною законною метою держави під час збройного конфлікту є зменшення військового потенціалу супротивника”. Це положення було інкорпороване в перший Додатковий протокол до Женевських конвенцій та підлягає обов’язковому застосуванню як під час міжнародних збройних конфліктів, так і неміжнародних. [21; 54]

Аналогічно до цивільного населення, відповідно до положень права Женеви, цивільним об’єктом є будь-який об’єкт, який не є військовим, тобто який через свій характер, призначення, розташування та/або використання не вносить ефективний вклад у воєнні дії, і тому вони не мають бути об’єктом нападу навіть у випадку, коли у однієї із сторін конфлікту наявні сумніви щодо їх можливого застосування не у цивільних цілях. [105]

Доктор Ахмед Аубаіс Аль-Фатлаві (Ahmed Aubais Al-Fatlawi) у своїй праці писав, що у міжнародному гуманітарному праві “цивільні об’єкти уособлюють недоторканність людського життя”, оскільки ними є всі об’єкти, що не належать до військових цілей, визначення яких насамперед стосується об’єктів матеріального світу і це, в свою чергу, викликає питання у контексті кібероперацій як оборонного, так і наступального характеру. Зокрема чи вважатимуться елементи інформаційних систем законними цілями і якщо так, то які саме: фізична кіберінфраструктура (сервери, вежі зв’язку та інші) чи цифрові дані, які в ній містяться. Міжнародний комітет Червоного Хреста у 1987 році охарактеризував “об’єкти” як “видимі та матеріальні”, таким чином вказуючи, що атаки на цифрові дані не вважатимуться об’єктом нападу взагалі. Водночас, на думку автора праці такий підхід є недоречним з двох позицій, по-перше, аналізуючи правові підходи інших науковців та країн, дані можуть мати критичне значення для цивільного населення і в такому разі вони мають захищатись правом Женеви як цивільні об’єкти через свою гуманітарну цінність, а по-друге, у випадку кібернетичної атаки на дані, внаслідок якої порушується функціонування фізичного цивільного об’єкту. То в даному випадку цифрові дані мають виступати в ролі цивільного об’єкту, оскільки вони, разом із матеріальним об’єктом, створюють взаємозалежну єдину систему. [5]

У Таллінському посібнику також наголошується, що цифрові дані слід розглядати як “об’єкт”, оскільки за невключення цього поняття до змісту цивільних об’єктів, існуватиме загроза здійснення проти них кібероперацій, що може залишити критично важливі цивільні масиви інформації, до яких належать відомості щодо соціального забезпечення, податкові чи банківські записи, без належного захисту в межах права збройних конфліктів. Водночас, кіберінфраструктура, до якої належать зокрема комп’ютерні мережі та інші матеріальні елементи, в залежності від цілей застосування та її характеру теж може бути цивільним об’єктом. [54]

Кубо Мачак (Kubo Mačák), який у своїй праці виступає в ролі критика Таллінського посібника, при цьому також висловив протилежну Міжнародному комітету Червоного Хреста позицію, а саме “для цілей визначення операцій цифрові дані як такі повинні розглядатися як об’єкт”. На його думку, якщо дані не вважатимуться об’єктом, то видалення великих обсягів цивільної інформації, яка становить як індивідуальний для кожної цивільної особи, так і глобальний, суспільний інтерес виходитиме за межі сфери дії права збройних конфліктів і буде суперечити принципу захисту цивільного населення від негативних наслідків воєнних дій. Проводячи аналогією із атакою на поштове відділення, яке використовувалось як місце опорний пункт дислокації військового угрупування, внаслідок якого було знищено листи, які там зберігалися, такий напад відповідав принципу пропорційності та нормам права збройних конфліктів. В такому випадку, чому напад в кіберпросторовому еквіваленті не є застосовним до фізичного. Беззаперечно, чинна архітектура міжнародного гуманітарного права є застарілою для сучасних реалій, тим не менш, вона не повинна відхілятись від очікувань держав. Знищення даних кібероперацією будь-якого характеру, чи то оборонного, чи то наступального, не має залишатись поза межами правового регулювання. [47]

Сполученими Штатами Америки просувається позиція щодо застосовності міжнародних законів збройних конфліктів, якими забороняються як наступальні, так і оборонні атаки на цивільне населення, до кіберпростору. При цьому, представниками США було запропоновано заборонити націлювання на цивільні об’єкти не тільки під час збройних конфліктів, а ще й у мирний час, зокрема наголошуючи на необхідності держави не здійснювати і не підтримувати діяльність, яка навмисно завдає шкоди критичній інфраструктурі або іншим чином перешкоджає її функціонуванню або використанню для надання послуг населенню. Тобто

уникати застосуванню кіберзасобів проти цивільних об’єктів в будь-який час - мирний та військовий. [24]

Колишній начальник відділу міжнародного права Офісу Генерального судді-адвоката збройних сил США, Ерік Талбот Дженсен (Eric Talbot Jensen) також визначає об’єктами правового регулювання міжнародним гуманітарним правом цифрові дані, а саме - електронні військові комунікації, наприклад, щодо наказу про початок здійснення атаки або розвідувальні звіти. Через військову мету цих даних, за своєю природою вони виступають законною цілею для кібероборонної або кібернаступальної операції, оскільки успішне перехоплення таких повідомлень або нейтралізація каналу зв’язку слугуватиме перевагою під час збройного конфлікту. [15]

Загалом, правознавець Марко Сассолі (Marco Sassoli) наголошує на необхідності зміни підходу до класифікації кібероперацій у межах міжнародного гуманітарного права з урахуванням їх специфіки та особливого характеру. Зокрема, він пояснює це тим, що взята за правило необхідність завдання матеріальної шкоди створює перешкоди для класифікації кібероборонних або кібернаступальних операцій, оскільки ключова проблема полягає в тому, що вони не завдають матеріальної шкоди, як наприклад - видалення даних, в класичному розумінні. Під час його розгляду “підходу наслідків” (effects approach), операція може і має вважатися шкідливою або руйнівною з огляду на її результати. І в такому випадку, це може як захистити інформацію, що використовується виключно в цивільних цілях, та, в свою чергу, легалізувати операції з, наприклад, ліквідації інформації, яка використовується у воєнних цілях. Таким чином, навіть якщо операція в КП не призводитиме до кінетичного знищення або пошкодження, то віртуальне знищення кібероб’єкта матиме стратегічне значення та буде вважатись таким, що визнається військовою ціллю. [5]

Доречно окремо розглянути застосовність права Женеви до кібероперацій як оборонного так і наступального характеру, спрямованих на

критичну цивільну інфраструктуру. За положеннями Додаткового протоколу І, критичною цивільною інфраструктурою є така, що внаслідок руйнування, знищення або виведення з ладу призведе до наслідків катастрофічного характеру. Міжнародне гуманітарне право до таких об’єктів відносить зокрема “запаси продуктів харчування, сільськогосподарські райони, що виробляють продовольство, посіви, худобу, споруди для забезпечення питною водою й запаси останньої, а також іригаційні споруди спеціально з метою не допустити використання їх цивільним населенням або супротивною стороною як засобу підтримання існування, незалежно від мотивів”. [105]

У розрізі кіберплощини, ця норма набуває нового значення, оскільки атака може здійснюватись без фізичного втручання, спричиняючи при цьому серйозні гуманітарні наслідки. До таких можна віднести, наприклад, електронну документацію медичних установ або централізованих систем водопостачання, здійснення кібероперацій проти яких призведе до завдання шкоди на системи, які забезпечують базові життєві функції населення. Тобто, якщо кібероперацією, якою було заблоковано доступ до електроенергії, води або теплопостачання, особливо в зимовий період року, може вважатися щонайменше протиправним у розумінні міжнародного гуманітарного права. Щонайбільше, за умови достатньої кваліфікації та доказової бази, такий напад може бути кваліфікованим Міжнародним кримінальним судом актом геноциду. Натомість, блокування, наприклад, доступу до інформаційних ресурсів не досягає достатнього рівня суспільної небезпеки і тому не підпадатимуть під регулювання міжнародного права. [130]

За правом Женеви, одним із критеріїв визначення військових об’єктів є їх розташування. Хоча зазначене поняття застосовується географічної місцевості та реального, фізичного існування об’єкту в просторі, тому умовна IP-адреса не є розташуванням, хоча вона має прямий зв’язок із кіберінфраструктурою, яка може становити військовий об’єкт. Позиція підкріплюється тим, що ознаку “військовий” робить не фактичне

використання, а ефективність внеску у здійснення воєнних дій завдяки цьому розташуванню. Наприклад, кібероперація проти програмного забезпечення системи водосховища може призвести до значного витоку води на територію місцезнаходження водосховища, на якій зокрема базується численне військове угрупування противника. Така операція матиме за мету позбавлення подальшої можливості використання ворогом цієї території у військових цілях і тому відповідна територія є військовим об’єктом за критерієм розташування, оскільки за своїм основним функціональним призначенням вона не несе характеру військового об’єкта, але в даному конкретному випадку - набуває такого значення. [54]

Позиція міжнародної групи експертів, на думку автора цієї роботи, є дещо спірною, оскільки, як було вказано, IP-адреса не є розташуванням, але водночас, вона пов’язана із кіберінфраструктурою та може бути “закріплена” за військовим об’єктом. Наприклад, закріплена за міністерством оборони IP-адреса очевидно відрізняється від IP-адреси веб-сайту міністерства освіти. У цьому зв’язку, отримання інформації щодо IP-адреси останнього та скерування подальших кібероперацій проти нього очевидно буде нападом на цивільний об’єкт, який за принципом розташування де-факто та де-юре визнається незаконною ціллю для кібератак.

Продовжуючи дослідження критеріїв військових об’єктів, міжнародна група приділила увагу їх можливого використання у військових цілях та застосовності цього критерія до кіберінфраструктури та простору. Яскравим прикладом у цьому розумінні є комп’ютерна мережа, яка зазвичай є цивільним об’єктом, але у разі її використання у військових цілях - передбачається втрата цього статусу і набуття нового - або “військовий об’єкт” або, скоріш за все, “об’єкт подвійного призначення”. Останнє є більш справедливим, оскільки використання комп’ютерної мережі ймовірно продовжуватиметься у тому числі й у цивільних цілях. Водночас, застосовність цього критерію вимагає окремої уважності та обережності,

оскільки за наведеної ситуації, не вся мережа стане військовою ціллю, якщо, наприклад, виключно один маршрутизатор у її складі матиме подібний статус. [54]

Професор Майкл Шмітт у своїй праці підкреслював особливо велике значення “подвійного призначення” об’єктів. Такі об’єкти використовуються як в цивільних цілях, так і у військових. Правом Женеви визначено, що як тільки цивільний об’єкт почав використовуватись у військових цілях, він автоматично набуває відповідного статусу та узаконює можливість здійснювати проти нього атаки. На його думку, головною проблемою в контексті кіберпростору є те, що велика частина кіберінфраструктури де-факто з моменту введення в експлуатацію має подвійне призначення, а тенденції щодо зміни підходу у майбутньому часі відсутні. Зокрема, він наводить у приклад те, що військові операції частково здійснюються кабелями та іншими засобами зв’язку, належність яких до змісту поняття кіберінфраструктури було доведено в попередніх розділах цього наукового дослідження, та які одночасно використовуються для цивільного трафіку. Електронна техніка (комп’ютери, GPS-навігатори тощо), яка використовується військовими для здійснення операцій також використовується у цивільних цілях. Окрему згадку він приділяє підприємствам, які виробляють відповідну продукцію як для цивільних, так і для військових цілей, теж набувають статусу військових об’єктів. [84]

На доповнення цього списку варто зауважити соціальні мережі, якими протягом російсько-українського збройного конфлікту поширювалась інформація, що становить військовий інтерес, та якими щодня з побутових, політичних, фінансових, наукових та інших питань користуються мільйони користувачів по всьому світу, навіть під час збройного конфлікту.

Розширюючи приклад М. Шмітта щодо підприємств, доречно вказати аналогічний підхід міжнародної групи експертів Таллінського посібника 2.0. Так, завод із виробництва комплексних рішень, які включають комп’ютерне

обладнання разом із програмним забезпеченням до нього, та на умовах контракту із збройними силами сторони конфлікту здійснює регулярні поставки такої продукції, є військовим об’єктом за критерієм використання навіть за умови здійснення таких поставок приватним компаніям, сферою діяльності яких є суто цивільна. Більш складним є випадок, коли завод виробляє продукцію, яка не є військовою, але використовується у таких цілях, підкреслюючи складність визначення без даних щодо масштабу обсягів виробництва та значимості такої продукції у військовому контексті. Натомість, експерти погодились, що цивільні об’єкти, які стали військовими через відповідне застосування, після припинення факту існування такої підстави, автоматично повертають собі цивільний статус. Однак у випадку тимчасового припинення військового використування цього об’єкта із повторним поверненням до такого - зазначений об’єкт залишиться із статусом “законної військової цілі”. [54]

Колишній начальник відділу міжнародного права Офісу Генерального судді-адвоката збройних сил США, Ерік Талбот Дженсен (Eric Talbot Jensen) визначає об’єктами подвійного призначення комерційних постачальників - цивільні компанії, які здійснюють поставку апаратного та програмного забезпечення уряду країни, яка є стороною збройного конфлікту. Оскільки, якщо такі компанії надають відповідні комплексні рішення з кібербезпеки як для юридичних та приватних осіб, які діють виключно у цивільній сфері, так і державним органам. Більше того, такі компанії не обов’язково мають бути повноцінними підприємствами, які виробляють нову продукцію, навпаки, автор стверджує на можливості визнання консалтингових IT-компаній законними цілями за умови, що вони здійснюють технічну підтримку для підтримання захищеності цивільних клієнтів та державних органів в умовах збройного конфлікту одночасно, якщо така підтримка стороні збройного конфлікту надає перевагу у веденні війни. При цьому, Ерік Талбот Дженсен вказує на змішаний характер цивільних та військових об’єктів в умовах

взаємопов’язаного кіберсередовища, внаслідок чого кібернападу можуть зазнати оточуючі цивільні об’єкти, хоча це і буде вважатись порушення правил та звичаїв війни. В цьому контексті він має на увазі те, що частина компанії або її послуг, що забезпечує державні потреби у веденні війни, зокрема у кібероборoні можуть бути законними цілями, тоді як невоєнні частини компанії та її послуг - є захищеними з точки зору права, але у дійсності можуть зазнати наслідків від безпосереднього нападу на першу категорію. [15]

В цьому випадку має застосовуватись принцип пропорційності та вимога вживати запобіжних заходів під час здійснення кібератаки або активної кібероборони. Очікується, що стороною, що ініціює кібероперацію, враховується будь-яка потенційна шкода захищеним цивільним особам (населенню) та об’єктам. Кібероперації створюють унікальні виклики в цьому контексті, оскільки КП хоча і окреслений відносними межами кіберінфраструктури, але у випадку, наприклад, передачі військових даних чітко визначити частину мережі, якою вони проходитимуть, може бути неможливим. За таких обставин, статус військового об’єкта набуває або уся мережа, або найбільш очікувані та прораховані її елементи, які будуть використані для створення каналу зв’язку. Прямою аналогією є мережа автомобільних доріг, яка перебуває в користуванні як військовими, так і цивільними транспортними засобами. За таких умов, навіть маючи доступ до супутникових даних, сторона конфлікту не може бути абсолютно впевненою щодо маршруту пересування військових сил і тому саме та частина дороги, яка є найбільш вірогідною для перевезення військових об’єктів аналогічно набуватиме відповідного статусу. Враховуючи це, підстави для диференціації підходу відсутні. [54]

Застосування принципу пропорційності має ґрунтуватись на оцінці потенційних наслідків кібероборонних та кібернаступальних операцій не лише з технічної точки зору, а й базуватись на їх впливі на цивільне

населення, інфраструктуру, гуманітарну ситуацію в регіоні та на контекст, в якому вони здійснюються. Наприклад, повне або часткове зупинення роботи телекомунікаційної мережі, яка належить до кіберінфраструктури та є об'єктом подвійного призначення, оскільки забезпечує одночасно мобільний зв'язок як між цивільним населенням, так і між командуванням в збройних силах, може завдати загрозу для цивільних через неможливість викликати швидку медичну допомогу або інші оперативно-рятувальні служби. Комплексний аналіз та планування кібероперацій, включаючи можливі ризики та наслідки, дозволяє провести межу між правомірними та неправомірними діями в контексті міжнародного гуманітарного права. [130]

Резюмуючи вищевикладене, міжнародне гуманітарне право зберігає свою регулятивну функцію незалежно від площини здійснення воєнних дій.

Положення статей 35–36 Додаткового протоколу I до Женевських конвенцій підтверджують, що сторони конфлікту не мають необмеженого права на вибір засобів і методів ведення війни. Закріплена у Додаткових протоколах до Женевських конвенцій Декларація Мартенса підтверджує це та одночасно забезпечує адаптивність права збройних конфліктів до новітніх технологій.

Реалізація права держави на самооборону у кіберпросторі не звільняє її від обов'язку дотримуватись норм jus in bello. Навіть під час оборонних операцій держави зобов'язані забезпечувати розмежування між цивільними та військовими цілями, уникати ураження цивільної інфраструктури та враховувати потенційні гуманітарні наслідки їх проведення.

Особлива увага науковцями приділена визначенню статусу цифрових даних та елементів кіберінфраструктури. Було встановлено існування двох основних підходів.

Перший, підтриманий Міжнародним комітетом Червоного Хреста, виходить із того, що поняття "об'єкт" стосується лише матеріальних та

видимих речей, а тому цифрові дані не можуть вважатися об’єктом нападу. Другий підхід, підтриманий низкою науковців та міжнародною групою експертів Таллінського посібника, виходить із необхідності визнання цифрових даних об’єктом правового захисту. Аргументується це тим, що невизнання даних цивільними об’єктами залишатиме без належного правового захисту критично важливу цивільну інформацію.

Щодо критичної цивільної інфраструктури встановлено, що кібероперації проти систем енергозабезпечення, водопостачання, медичних інформаційних систем або інших об’єктів, які забезпечують базові життєві потреби населення, можуть спричинити катастрофічні гуманітарні наслідки. І тому розглядатимуться як порушення міжнародного гуманітарного права.

При цьому, значна частина сучасної кіберінфраструктури одночасно використовується як у цивільних, так і у військових цілях. Це стосується комп’ютерних мереж, телекомунікаційних систем, програмного забезпечення, соціальних мереж, кабелів зв’язку, а також підприємств та ІТ-компаній, які надають послуги як цивільним користувачам, так і державним органам або збройним силам. У випадку використання таких об’єктів для підтримки воєнних дій вони можуть набувати статусу військової цілі. Однак це не скасовує обов’язку дотримуватись принципів пропорційності та вживати запобіжних заходів для мінімізації шкоди цивільному населенню.

Таким чином, МГП є застосовним до кібероборони та кібероперацій у цілому. Основні принципи права збройних конфліктів залишаються чинними і в умовах цифрового середовища. Разом із тим, специфіка КП, нематеріальний характер цифрових даних, поширеність об’єктів подвійного призначення та складність прогнозування наслідків кібератак свідчать про необхідність подальшого розвитку міжнародно-правових підходів до регулювання кіберконфліктів.

РОЗДІЛ 3. Практика та перспективи розвитку кібероборони

3.1. Практика окремих держав у сфері кібероборони

Сьогодні економіка та національна безпека Сполучених Штатів Америки напряму залежить від інформаційних технологій та кіберінфраструктури. Новітні технології забезпечують безперервне функціонування критичної інфраструктури країни у переважній більшості секторів держави, як то енергетичний, транспортний, фінансовий, військовий, промисловий та інші. У цьому зв'язку США регулярно зіткається з численними кібератаками з різних напрямів і тому запроваджують механізми ефективного захисту критичної інфраструктури, інформаційних мереж та систем, а також заходи із контролю якості використовуваного ІТ-обладнання. Однією із ключових складових стратегії національної безпеки країни у сфері КП є міжнародна співпраця у сфері обміну інформації та модернізації існуючих систем кіберзахисту, а також створення правового режиму регулювання кібероперацій. [36]

Протягом двох останніх десятиліть, США розробили стратегії та доктрини у сфері кіберпростору, а також створили окремі спеціалізовані підрозділи як у складі збройних сил, так і у складі спеціальних служб. Одним із таких прикладів є створення Кіберкомандування та Сил кібермісій (Cyber Mission Force). При цьому, формуванню таких структур передував ґрунтовний науково-правовий підхід до визначення загального, але чітко сформованого та одностайного, бачення впливу КП на збройні конфлікти. Таке комплексне дослідження віднайшло своє відображення в оборонних кіберстратегіях, які ухвалялись у 2011, 2015 та 2018 роках з подальшим оновленням та удосконаленням, послідовність та безперервність формування яких демонструє регулярний перегляд вже сформованих поглядів на відповідність вимогам та тенденціям розвитку рівня технологій для максимізації конкретики у сфері оборони кіберпростору та змістовному осмисленню уявлень про військові кібероперації. [85]

Доречно зазначити, що періоди ухвалення кожної з стратегій з оборони у КПпередували рокам видання Таллінського посібнику (2013, 2017 та розробка нової версії з 2021 року). За такою аналогією, можна виокремити не тільки комплексний підхід США до правового визначення КП та операцій у ньому, але також світового наукового товариства.

Повертаючись до практичного впливу кіберстратегій у сфері оборони США, вони дозволили досягти згоди між бюрократичними групами у довгостроковій перспективі, розмежовуючи сфери відповідальності та впливу. Було визначено які оборонні інституції провадять свою діяльність у відповідь на нові загрози у КП, та якими мають бути відповіді на них. І хоча першими документами, ухваленими у 2011 та 2015 роках, було змінено риторику Міністерства оборони США щодо Інтернету та кіберпростору в цілому з оптимістичної, “про демократичні цінності” на песимістичну - “занепокоєння щодо загроз у кіберсередовищі”, позиція щодо протидії кібератакам, базовим уявленням про ескалацію збройних конфліктів в умовах кіберзагроз, а також необхідності стримування залишались однаковими. Президентом США, Дональдом Трампом, було поставлено під сумнів доцільність продовжувати підхід свого попередника, Барака Обами, за каденції якого було ухвалено дві кіберстратегії, і тому нова редакція 2018 року зазнала суттєвих змін про доречність кіберескалації внаслідок кіберагресії на більш деталізовану унормованість та ефективність кіберстримування. [85]

Кіберкомандування США або USCYBERCOM, створене за ініціативи Міністерства оборони, посідає важливе місце у сфері захисту й оборони національних інтересів держави у КП та володіє широким спектром повноважень з кібероборонних та кібернаступальних операцій. USCYBERCOM це об’єднане бойове командування, яке у співпраці із іншими командуваннями різних видів збройних сил США, забезпечують функціонування стратегічних та оперативних штабів, які здійснюють

планування та контроль за виконанням кібероперацій в цифровому середовищі. [95]

Кіберкомандування США також є відповідальним за захист мереж Міністерства оборони, оборону держави загалом та уповноважене на проведення кібероперацій на підтримку інших підрозділів збройних сил. Однією з операцій активної оборони в кіберпросторі була Stuxnet, спільна кібероперація Ізраїля та Америки. За допомогою шкідливого програмного забезпечення, США, заклавши у основу цієї операції цифрове середовище як місце ведення бойових дій, спричинили фізичного пошкодження центрифуг для збагачення урану в Ісламській Республіці Іран. Проведення цієї операції, як і факт її успіху та реальних кінетичних наслідків, трансформував класичне уявлення про територію держави та кордони, додавши у зміст цього визначення КП. [93]

Продовжуючи розвиток кібероборони та розробку нових кібертехнологій, з метою об’єднання розрізнених зусиль, за ініціативи USCYBERCOM було створено Об’єднану архітектуру ведення кібервійни (Joint Cyber Warfighting Architecture), основним завданням якої є визначення сумісності операційної інфраструктури, яка є сукупністю технологічних, системних, процесних та кадрових ресурсів, які забезпечують безперебійну роботу, з кіберінструментами, а також з засобами командування та управління, необхідними для здійснення моніторингу та керування операціями. Одним із результатів роботи згаданої Об’єднаної архітектури стало Постійне середовище кіберпідготовки (Persistent Cyber Training Environment), під час створення якого було визначено ціллю підтримка навчання, оцінювання та здійснення кібероперацій. Фактично, такий центр є кіберпросторовим полігоном для підвищення кваліфікації кадрових ресурсів, оскільки був створений за моделлю Національного тренувального центру армії США. Навчальний процес забезпечується системою емуляції за допомогою віртуальних засобів у поєднанні з фізичним обладнанням та

дозволяє невеликим групам учнів-операторів кіберпросторових операцій готуватись до їхнього майбутнього практичного застосування. При цьому важливо зазначити, що ідея створення такого центру полягала не лише в необхідності масштабування якісного спеціалізованого навчання представникам кіберсил США. За допомогою симуляцій кібероперацій, як в оборонному, так і в наступальному контексті, в рамках навчання збирається значний обсяг статистичної інформації без фактичної необхідності завдання реальної шкоди. Відповідна інформація аналізується як в цілях модернізації власних систем з кібероборони та захисту, так і з метою прорахунку та інтегрування більш оптимальних способів здійснення операцій, а також для створення правової бази, ґрунтуючись на потенційних наслідках імплементації таких операцій в реальне життя як США, так й іншими країнами під час збройних конфліктів. [95]

Розглядаючи іноземний практичний досвід у сфері кібероборони, не можна пропустити Державу Ізраїль, оскільки кіберпротистояння між Ізраїлем та Іраном є одним із найбільш відомих прикладів кібервійни, а враховуючи загострення політичної ситуації між країнами навесні 2026 року та, відповідно, збільшенням інтенсивності бойових дій, аналіз моделі кібероборони Ізраїлю є важливим для наукового-дослідницького контексту. Значимим моментом у кібервійні між державами стала американсько-ізраїльська кібероперація 2010 року Stuxnet проти ядерного центру у Натанзі. Відтоді країнами в двосторонньому порядку було посилено активність у цифровому просторі, обмінюючись регулярними кібератаками як на військову, так і цивільну та критичну інфраструктуру. Сутність системи кібероборони Ізраїлю розкривається, зокрема в межах дослідження ірансько-ізраїльського конфлікту у тому числі у цифровому середовищі. Ця кібервійна є не лише регіональним збройним конфліктом міжнародного характеру, але показовим прикладом взаємодії інформаційних технологій із військовою необхідністю і тому відтворює значимість кіберможливостей держави для її

національної безпеки та оборони, наголошуючи на необхідності створення ефективних систем оперування КП та кіберінфраструктурою.[39]

Держава Ізраїль вважається однією з найбільш високорозвинених кібердержав у світі, оскільки створив унікальні з технологічної точки зору підходи до оборони та розвідки у цифровому середовищі, які реалізуються, зокрема висококваліфікованими та впізнаваними у світі підрозділами, наприклад, підрозділ 8200. Кіберможливості Ізраїлю дозволяють завдавати ударів по іранській інфраструктурі непомітно та розглядаються як безпосередньо державою, так і міжнародною спільнотою заходами із активної оборони та превентивного стримування. [39]

Система ізраїльських органів, які спеціалізуються на кібероборони, є складною та багаторівневою, оскільки розділена на цивільні, військові та розвідувальні структури, які співпрацюють та пов’язані між собою.

Ізраїльський національний кібердиректорат був утворений внаслідок злиття Національного управління з кібербезпеки та Ізраїльського національного кібербюро, обидва цих органи були створені паралельно. Завданням Національного управління з кібербезпеки було здійснення захисту цивільного КП, але без надання правоохоронних функцій. Ізраїльське національне кібербюро аналогічно забезпечувало захисту кіберпростору країни, а також розробку національної стратегії кібербезпеки, розвитку технологій та координації дій між державним і приватним секторами. У цьому зв’язку, внаслідок їх об’єднання, Кібердиректорат резолюцією Уряду Ізраїлю отримав усі відповідні функції та став відповідальним за всі аспекти цивільного кіберзахисту - від формування политики та розвитку кіберможливостей до оперативної кібероборони. Другим органом цивільного кіберзахисту є комп’ютерна група реагування на надзвичайні ситуації. Це ключовий елемент довгострокової стратегії захисту цивільного кіберсектору, оскільки, з одного боку, вона здійснює обробку інформації про кіберінциденти та доступна для цивільних користувачів, а з іншого,

уповноважена на обробку чутливої інформації та секретними структурами. [40]

Підрозділ Генерального штабу Сил оборони Ізраїлю “C4I та кібероборона” відповідальний за мережеву безпеку, її оборону та обслуговування в межах Сил оборони Ізраїлю. Він відіграє центральну роль у кібербезпеці країни, оскільки для завдань та цілей Сил оборони здійснює підготовку спеціалістів із інформаційних та комунікаційних технологій, розробку програмного забезпечення, проєктування архітектури інформаційно-комунікаційних систем, а також розробку криптографічно захищених систем обміну даними.

Військова розвідка Ізраїлю Aman є незалежною службою, яка не входить до складу збройних сил та підпорядковується безпосередньо Прем’єр-міністру. Підрозділ 8200, який є прямим аналогом Агентству національної безпеки США або Урядового центру зв’язку Великої Британії, в Aman відповідальний за перехоплення, збір та аналіз інформації, а також за дешифрувальні операції. Військова розвідка здійснює кібернаступальні інформації та операції з експлуатації комп’ютерних мереж, в той час, як C4I та кібероборона - за операції у сфері кібероборони. [40; 41]

До кібероперацій, розроблених та проведених відповідним підрозділом, офіційно визнаних Силами оборони Ізраїлю, окрім «Stuxnet», належать «Flame» та «Duqu», хоча деякі джерела приписують участь підрозділу 8200 також до інших. [41]

Кібероперація “Stuxnet” отримала відповідну назву від назви комп’ютерного хробака (worm), тобто шкідливого програмного забезпечення, яка має своєю ціллю системи програмно-апаратний комплекс для моніторингу промислових процесів, збору інформації з датчиків у реальному часі та дистанційного керування обладнанням (SCADA). Хоча процес створення програмного забезпечення залишається офіційно не розкритим,

беззаперечно за потребувало значних фінансових, кадрових та часових ресурсів. [44]

Stuxnet, написаний на декількох мовах програмування, за обсягами був більшим за його аналогів, при цьому його окремі компоненти були зашифрованими. [74]

Його дія була спрямована на зараження комп'ютерів, які працювали на операційній системі Microsoft Windows, використовуючи одразу чотири вразливості "нульового дня": автоматичне виконання через підключені USB-носії, підключення через спільні принтери, а також дві інші вразливості із ескалацією привілеїв (запуск програмного забезпечення навіть на комп'ютерах із заблокованим доступом). Для завантаження свого rootkit-компонента, Stuxnet використовував попередньо викрадені справжні сертифікати драйверів RealTek і JMicron, завдяки яким хробак отримував можливість шукати шкідливе програмне забезпечення Siemens Simatic WinCC/Step-7, яке використовувалось для управління обладнанням. Після зараження файлами отримувався доступ до програмованих логічних контролерів, якими регулюється робота промислових пристроїв, дозволяючи віддалено оперувати ними. [75; 76]

Окрім цього, Stuxnet міг взаємодіяти з іншим зараженим системним обладнанням та серверами, розташованими в Данії та Малайзії, для оперативного оновлення та своєчасної передачі даних. [44]

Основною ціллю, як було вказано, був іранський ядерний об'єкт - центр збагачення урану в Натанзі. Ціллю у вужчому розумінні були центрифуги з обробки урану у кількості 164 одиниць, і той факт, що хробак був запрограмований на атаку групи пристроїв по 164 об'єкти навряд чи був випадковим збігом. [25]

Важливо зазначити, що така кібероборонна операція, хоча і мала ціллю ядерний об'єкт, але програмне забезпечення та спосіб нейтралізації загрози,

була здійснена без загрози для цивільного населення Ірану, тобто, у рамках принципів військової необхідності та пропорційності, у межах вимог міжнародного гуманітарного права. [33]

Серед інших відомих кібероперацій, офіційно визнаних Силами оборони Ізраїлю, є ті, які хоча були пов’язані із шпигунством у кіберпросторі, але здійснювались з цілями оборони або наступу як у кібер, так і у реальному середовищах, та які здійснювались за допомогою складного багатофункціонального модульного шкідливого програмного забезпечення Flame. Розробником цього програмного забезпечення також вважається підрозділ 8200 у співпраці з зовнішніми підрядниками, зокрема, через схожість із Stuxnet модулю-плагіну, та існує припущення про можливість застосування Flame для цілей операції Stuxnet. [82]

Сфера дії “Flame” була спрямована на персональні комп’ютери під управлінням Microsoft Windows, поєднуючи численні методи самопоширення та атак, а також спеціальні способи введення в дію коду. Програмне забезпечення здійснює збір інформації, зокрема шляхом реєстрації натискань клавіш, збереження знімків екрану, активації мікрофонів та вебкамер у разі їх наявності на пристрої, а також на аналізі носіїв інформації, підключених до інфікованого пристрою, але не обмежуючись ними. Додатковою особливістю Flame була здатність вмикати Bluetooth-модуль та зберігати інформацію про сусідні пристрої для поширення шкідливого програмного забезпечення на пов’язані пристрої. Подібно до Stuxnet, код програми та її суміжні файли був стиснений та зашифрований щонайменше п’ятьма різними методами та мав не менш п’яти різних форматів вкладень. Розвідувальні кібердії забезпечувались спроможність програмного забезпечення структурувати зібрану інформацію в базах даних з подальшою їх передачею на віддалені сервери військово-розвідувального командування, використовуючи мережеве з’єднання. [88]

Якщо Stuxnet здійснював фізичне або віртуальне руйнування цілі кібероперації, Flame - кіберрозвідку, то Duqu 1.0 та 2.0 за своєю цифровою природою були шпигунськими програмами для підготовки кібероперації, зокрема проти Ірану та Угорщини. [82]

Варто зауважити, що усі згадані попередньо шкідливі програмні забезпечення, включаючи Duqu обох версій, фактично належать до однієї “цифрової сім’ї” через їхню надзвичайну схожість одна на одну у контекстах архітектури проєктування, внутрішньої структури та механізмів роботи. Водночас, у зв’язку із відмінними цілями застосування, існували й очевидні відмінності. Як було визначено, Stuxnet створювався з метою завдання шкоди у фізичному та цифровому просторі цілі військової кібероперації через кіберінфраструктуру, натомість, Duqu був спрямований не на знищення, а на викрадення інформації, що становить розвідувальний інтерес. [88]

Загалом, практичний досвід Ізраїлю у сфері кібероборони різносторонній та охоплює розробку та практичне застосування широкого спектру засобів у КП. Зокрема, у лютому 2018 році, у рамках кібероборонних заходів, підрозділов 8200 було виявлено та попереджено терористичний напад Ісламської держави Іраку й Леванту (ІДІЛ) на цивільний авіалайнер з рейсом із Австралії до Об’єднаних Арабських Еміратів через вчасне цифрове перехоплення та передання австралійській стороні інформації. Зазначеному підрозділу приписується допомога у запобіганні іншим складним операціям, зокрема іранських атак проти державних та приватних організацій в Ізраїлі, Туреччині, Катарі, Об’єднаних Арабських Еміратах, Саудівській Аравії та Лівані. [82]

Естонія є одним із найбільш помітних прикладів розвитку національної системи кібероборони. Окрім цього, саме Естонська Республіка є своєрідним центром розвитку міжнародного підходу до розуміння КП та регулювання кібероперацій, завдяки розташованому в її столиці, Талліні, Об'єднаного центру передових технологій з кіберзахисту НАТО.

Історичною передумовою для трансформації системи кібероборони країни слугували події квітня та травня 2007 року під час яких естонські об’єкти зазнали місштабних атак російського походження. Термін “російського походження” вжитий навмисно, оскільки фактично більшість кібератак були здійснені з території росії, IP-адреси вказували на щонайменше 177 держав, в деяких з них було встановлено ланцюжковий зв’язок із російськими урядовими установами, насамперед - з головним розвідувальним управлінням. Офіційною причиною таких атак було визначено політичне рішення Естонської сторони перенести радянський військовий меморіал з центру столиці до її околиці, хоча існують підстави вважати, що вони були спровоковані імперіалістичною зовнішньою політикою російської федерації та кремлівської влади безпосередньо. Оскільки після здобуття незалежності Естонська Республіка активно інвестувала власні бюджетні кошти та залучала зовнішні інвестиції у розвиток кіберпросторових технологій та суміжної інфраструктури, у 2007 році держава значною мірою покладалась на інформаційні сервіси у переважній більшості сфер життя - від банкінгу до транспорту, наслідки кібератак на урядову та комерційну кіберінфраструктуру Естонії, зокрема інформаційно-комунікаційні системи Президента, Прем’єр-міністра, Парламенту, міністерств, політичних партій, банків та інтернет-провайдерів, виявились руйнівними. Відомо, що застосовувались кібератаки типу відмови в обслуговуванні (DoS), розподілені (відбуваються з різних IP-адрес) атаки типу відмови в обслуговуванні (DDoS), дефейсменту (defacement) - отримання несанкціонованого доступу та заміна оригінального наповнення веб-сайту іншим (провокаційним), а також ті, що спрямовувались на знищення цифрових даних. Через це було паралізовано діяльність органів державної влади, у тому числі у сфері здійснення соціальних виплат та збору податків. [9; 14; 66]

Такий інцидент став передумовою для повного переосмислення як підходу держави до регулювання та вдосконалення моделі кібероборони, так і міжнародного бачення проблеми правового регулювання кібероперацій та КП. У цьому зв'язку, розвинута модель кібероборонної діяльності Естонії включає не тільки протоколи реагування на кібератаки та їх загрози, а також координацію між внутрішніми відомствами держави та міжнародними партнерами, судово-правові інструменти для підтримки безпеки державної кіберінфраструктури. Варто наголосити, що розвиток та становлення сучасної моделі кіберзахисту країни здійснювався у співпраці з європейськими та трансатлантичними міжнародними організаціями та за їх рекомендацій, що передбачило багатогранність підходу до кібероборонних заходів, зокрема з урахуванням права Європейського Союзу, загальних положень міжнародного права та права збройних конфліктів. Це призвело до інтеграції у національну правову та оборонну системи стандартизованих комплексів безпекових заходів, що в сумі із науковими надбаннями республіки створило унікальну естонську модель кібероборони. Модель якої базується на принципі взаємозв'язку ланок законодавчого, організаційного, оперативно-тактичного та міжнародного управління. [27]

Законодавчі ініціативи та існуюча нормативно-правова база Естонської Республіки передбачає визначення відповідальності за кібератаки, протоколи безпеки та оборони в цифровому середовищі. Естонія посилила свою роль у міжнародному співробітництві щодо забезпечення інформаційної безпеки шляхом просвітницької діяльності, навчань, наукових досліджень та розвитку технологій. Вона також є прикладом того, як державний і приватний сектори повинні взаємодіяти для забезпечення безпеки всіх зацікавлених сторін. [56]

Національний план розвитку оборони на 2017–2026 роки є третім десятирічним стратегічним планом Естонії та містить сім основних цілей: забезпечення безперервності функціонування держави та суспільства, міжнародну безпеку, стратегічні комунікації, внутрішню безпеку, підтримку

цивільного сектору та військову оборону. Лише частина цього документа є публічно доступною. [26]

Естонська оборонна модель у сфері кіберпростору ґрунтується на розподілі меж впливу та відповідальності між цивільним та військовим секторами, що дозволяє ефективно застосовувати як військові, так і цивільно-правові інструменти з протидії кібернападів для захисту державної кіберінфраструктури та цифрового середовища. В рамках цієї концепції створені інформаційно-аналітичні системи для попередження кіберінцидентам, а також механізми сповіщення та координації між державними органами та приватним сектором. За відповідних обставин, створюються умови для зменшення часу реагування на кіберзагрози та відновлення після завданої шкоди.

Інституційна архітектура кібероборони Естонії складається із Міністерства оборони та Національного агенства кібербезпеки (Kaitseväe Kaitseliit). Міністерство оборони є відповідальним за національну оборону у тому числі у кібернетичному вимірі. У лютому 2014 року було створено Департамент кіберполітики та інформаційно-комунікаційних технологій, який спеціалізується на питаннях кіберполітики та підпорядковується Державного секретаря Міністерства оборони. Заснований у серпні 2018 року Департамент Кіберкомандування Сил оборони Естонії є головним органом у сфері захисту КП в межах Міністерства оборони. Окрім цього, Департамент відповідальний за надання інформаційно-комунікаційних послуг, стратегічних комунікацій. Захист інформаційно-комунікаційних систем, планування та організація операцій в інформаційному та кіберпросторах належить до сфери відповідальності Центру інформаційних та кібероперацій. [26]

Забезпечення національної оборони в цифровому середовищі підтримується унікальною в межах світової практики структурою, Спеціалізований добровільний підрозділ Естонської ліги оборони

(Küberkaitseliit). Зазначена добровольча організація, яка налічує більше 15 тисяч учасників, складається із спеціалістів з питань кібербезпеки та оборони як державного сектору, так і приватного. Відповідним національним законом його було інтегровано до системи національної оборони із визначенням його структури, управління, членства та функціонування. У цьому зв'язку в рамках естонської моделі діє принцип швидкої координації між цивільними та військовими кіберструктурами для термінової адаптації до загроз проти національної недоторканності та безпеки КП. [26]

Узагальнюючи практичний досвід Сполучених Штатів Америки, Держави Ізраїль та Естонської Республіки у сфері кібероборони, можна дійти висновку, що сучасний КПстав одним із ключових елементів забезпечення національної безпеки, оборони та безперервного функціонування держави.

Залежність критичної інфраструктури від інформаційних технологій зумовила необхідність формування комплексних систем кіберзахисту, які поєднують правові, організаційні, технічні та військові механізми реагування на кіберзагрози. Кібероборона більше не розглядається виключно як допоміжний елемент інформаційної безпеки, а є самостійним напрямом оборонної політики та міжнародного безпекового співробітництва.

Практика США свідчить про системний підхід до формування кібероборони як окремого компоненту національної оборони держави. Протягом останніх десятиліть у США було створено нормативну, стратегічну та інституційну основу функціонування кіберпростору в умовах сучасних загроз. Ухвалення оборонних кіберстратегій у 2011, 2015 та 2018 роках відобразило поступову трансформацію поглядів держави на природу кіберзагроз та способи реагування на них.

Створення Кіберкомандування США (USCYBERCOM) та Сил кібермісій стало наслідком комплексного науково-правового підходу до розуміння ролі КП у збройних конфліктах. USCYBERCOM отримало широкі

повноваження щодо захисту мереж Міністерства оборони США, планування та проведення кібероперацій, а також координації діяльності з іншими видами збройних сил.

Американська модель кібероборони демонструє поєднання оборонних та наступальних кіберможливостей, що дозволяє державі використовувати цифрове середовище як повноцінний театр військових дій.

Практичний досвід Ізраїлю у сфері кібероборони демонструє високий рівень інтеграції військових, розвідувальних та цивільних кіберструктур. Ізраїль сформував багаторівневу систему кіберзахисту, в межах якої функціонують спеціалізовані органи цивільного та військового призначення.

Ключову роль у військовій сфері відіграють підрозділ «C4I та кібероборона» та підрозділ 8200 у складі військової розвідки Aman. Їх діяльність охоплює кібероборону, кіберрозвідку, дешифрувальні операції, перехоплення інформації та проведення кібернаступальних дій.

Кібероперації “Stuxnet”, “Flame” та “Duqu” стали прикладами складних багаторівневих кіберінструментів. Stuxnet був спрямований на фізичне пошкодження промислової інфраструктури через ураження програм управління обладнанням. Flame використовувався переважно для кіберрозвідки та збору інформації. Duqu був орієнтований на підготовку майбутніх кібероперацій шляхом викрадення даних розвідувального значення.

Ізраїльська модель підтверджує, що ефективна система кібероборони потребує тісної взаємодії між сектором безпеки, розвідкою, науково-технологічними структурами та цивільними органами. А практичний досвід демонструє ефективність кіберрозвідки та кібероборони у запобіганні загрозам національній безпеці.

Естонська модель кібероборони сформувалася під безпосереднім впливом кібератак 2007 року, які продемонстрували критичну залежність

сучасної держави від цифрової інфраструктури. Масштабні атаки на органи державної влади, банківський сектор, інформаційні системи та інтернет-провайдерів фактично паралізували функціонування окремих сфер державного управління та стали поштовхом до комплексного переосмислення підходів до кібербезпеки.

Естонія створила модель координації між цивільним та військовим секторами. Вона охоплює Міністерство оборони, Департамент кіберполітики та інформаційно-комунікаційних технологій, Кіберкомандування Сил оборони та Центр інформаційних і кібероперацій.

Особливістю її моделі є існування добровольчого підрозділу Küberkaitseliit, який інтегрований до системи національної оборони та забезпечує швидку координацію між державними та приватними спеціалістами у сфері кібербезпеки.

Отже, досвід США, Ізраїлю та Естонії свідчить про те, що КП остаточно закріпився як повноцінний вимір сучасних конфліктів, а кібероперації стали важливим інструментом забезпечення національної безпеки, стримування загроз та реалізації оборонної політики держав.

3.2. Кібероборона України в умовах війни. Проблеми регулювання

Російська агресія проти України розпочалася у 2014 році з окупації Криму та ескалації збройного конфлікту на сході України. Генеральна Асамблея ООН ухвалила резолюцію A/RES/68/262 “Territorial Integrity of Ukraine”, якою підтвердила суверенітет і територіальну цілісність України та не визнала незаконну анексію Криму російською федерацією. [77]

24 лютого 2022 року НАТО офіційно засудило повномасштабне вторгнення Російської Федерації в Україну, назвавши його “невиправданим і неспровокованим нападом”. [53]

У заяві глав держав і урядів НАТО від 25 лютого 2022 року дії Росії були визначені як “повномасштабне вторгнення в Україну”. [73]

Генеральна Асамблея ООН під час Надзвичайної спеціальної сесії у 2022 році ухвалила резолюцію щодо агресії проти України (“Aggression against Ukraine”), засудивши застосування Росією сили проти суверенної держави. [2]

Повномасштабне вторгнення росії в Україну у 2022 році продемонструвало еволюцію сучасної війни, у якій кіберпростір та інформаційне протиборство відіграють ключову роль поряд із традиційними кінетичними бойовими діями. Історичний аналіз засвідчує траєкторію ескалації кіберпротистояння між росією та Україною, що створило підґрунтя для складних кібероперацій, зафіксованих у 2022 році. Технічні оцінки міжнародних експертів підкреслюють високий рівень шкідливого програмного забезпечення, яке застосовувалося для шпигунства, дестабілізації та маніпулювання інформацією. Важливою особливістю конфлікту стала демократизація кібервоєнних дій, коли поряд із державними ініціативами значну роль почали відігравати громадські рухи та хактивістські групи, що вели боротьбу за інформаційні наративи та здійснювали контрнаступальні дії. Глобальні наслідки кібернетичного виміру російсько-українського збройного конфлікту є масштабними та свідчать про необхідність формування міжнародних кібернорм, механізмів колективного захисту, а також переосмислення ролі недержавних суб’єктів у геополітичних протистояннях.

Перший факт вдалої атаки на об’єкти енергетики зареєстровано 23 грудня 2015 року в Україні, яку пов’язують із проросійськими суб’єктами. Про це заявила прес-служба Міністерства енергетики та вугільної промисловості України. Атака була здійснена на три енергопостачальні організації: “Прикарпаттяобленерго”, “Київобленерго” та “Чернівціобленерго”. Зазначена атака мала кібернетичний та комплексний характер і складалась із: попереднього зараження мереж за допомогою підроблених листів електронної пошти з використанням методів соціальної

інженерії; отримання несанкціонованого доступу до управління автоматизованих систем диспетчерського управління підстанціями; виведення з ладу елементів кіберінфраструктури (джерела безперебійного живлення, модеми); знищення інформації на серверах та робочих станціях; кібератака на телефонні номери кол-центрів, з метою перевантаження ліній і, відповідно, відмови в обслуговуванні знеструмлених абонентів. [113]

Окрім атак на енергосистему, критична інфраструктура України, зокрема залізнична система, робота аеропортів та урядові вебсайти, у період з 2015 по 2017 рік зазнала численних кібератак. Ці атаки, які часто пов'язували з російськими державними угрупованнями, були спрямовані на порушення функціонування сервісів, створення хаосу та підрив довіри до українських інституцій. [8; 60]

Російська сторона здійснювала розвідку та попереднє розміщення кіберзасобів у певних українських енергетичних і комунікаційних мережах щонайменше з березня 2021 року. Проте під час самого вторгнення, а також упродовж кількох тижнів, що йому передували, росія переважно застосовувала модифіковані форми атак, які вже використовувалися проти Грузії у 2008 році та України у 2014 році. Зокрема, російські спеціальні служби здійснювали дефейсинг вебсайтів та DDoS-атаки проти сайтів українських міністерств і підприємств приватного сектору. Було також виявлено кілька випадків активації шкідливого програмного забезпечення, здатного знищувати дані на жорстких дисках комп'ютерів. Це програмне забезпечення, відоме під назвою "WhisperGate", поширилося на окремі урядові мережі України та фінансові установи, а також зачепило Латвію й Литву, однак не спричинило значних масштабних порушень. Водночас не виключено, що масштабніші атаки були попереджені завдяки своєчасному виявленню та усуненню загроз, пов'язаних із програмами-вайперами, українським урядом і західними компаніями у сфері кібербезпеки. [79]

Безпосередньо після початку вторгнення дефейсинг вебсайтів та атаки типу DoS швидко переросли у масштабне онлайн-протистояння в інформаційному просторі за участю росіян та українців. Це мало ознаки кібер вандалізму, а також поширення фейкових новин і пропаганди в межах інформаційної боротьби за суспільну підтримку та громадську думку. Попри це, не спостерігалося значних спроб Росії вивести з ладу критичну національну інфраструктуру України, хоча напередодні вторгнення американські посадовці попереджали, що деструктивні кібердії під час конфлікту можуть бути “іншими за масштабом, характером і рівнем складності порівняно з інцидентами мирного часу”. [92]

Однак у процесі розвитку війни поступово проявлялися й інші кібернетичні аспекти конфлікту. З’ясувалося, що 24 лютого, менш ніж за годину до вторгнення в Україну, росія здійснила атаку на європейську мережу компанії Viasat — супутникової системи, що належить американській компанії. Атака призвела до порушення інтернет-зв’язку для кількох тисяч користувачів Viasat в Україні, спричинивши перебої у комунікаціях державних установ і компаній. [69]

Операція включала злам, здійснений ГРУ - російським військовим розвідувальним агентством, унаслідок якого були виведені з ладу наземні модеми системи одночасно з DDoS-атакою на саму мережу. Імовірно, основними цілями атаки були український уряд, Збройні сили України та поліція, які значною мірою покладалися на зв’язок, забезпечуваний Viasat. Очевидно, що цілі та час проведення атаки були настільки важливими для російської сторони, що вона була готова ризикувати можливим поширенням наслідків за межі України. Імовірно, російське військове та політичне командування переслідувало й інші кібернетичні цілі, оскільки значна частина операцій проти українських мереж була спрямована на збір персональних даних громадян України. Серед іншого це могло бути

пов’язано зі спробами ідентифікувати осіб, які з найбільшою ймовірністю могли б співпрацювати з окупаційними силами або чинити їм опір. [111]

У ході розвитку збройного конфлікту росія посилила кібероперації проти критичної національної інфраструктури України. Зокрема, йшлося про проникнення в одну з найбільших енергетичних систем України у лютому 2022 року з метою здійснення деструктивного впливу 8 квітня за допомогою тих самих методів, які росія використовувала під час атак на Україну у 2015 та 2016 роках. Українські спеціалісти з кібербезпеки нейтралізували цю загрозу. Українська сторона повідомила, що шкідливе програмне забезпечення під назвою “Industroyer2” проникло до системи управління електромережею та у разі успішної реалізації атаки могло б залишити без електропостачання близько двох мільйонів людей. [111]

Наприкінці квітня компанія Microsoft повідомила, що відстежила понад 237 російських кібероперацій проти України з часу, що передував вторгненню. Частина з них виявилася успішною: було зафіксовано “майже 40 окремих деструктивних атак, які призвели до незворотного знищення файлів у сотнях систем десятків українських організацій”. Водночас значну кількість атак вдалося відбити. Загалом, за оцінкою Microsoft, Україна не зазнала того масштабного загальнонаціонального паралічу систем, якого очікували багато експертів. [72]

У червні 2022 року високопосадовці європейських кіберструктур дійшли висновку, що росія виявилася неготовою до ведення скоординованої кібернетичної та кінетичної війни. На їхню думку, російська кібердіяльність проти України була масштабною, проте погано спланованою й організованою, що свідчило про менший рівень кіберспроможностей росії, ніж вважалося раніше. [68]

Аналогічної позиції дотримувався Джеремі Флемінг, керівник британської служби GCHQ, який зазначив, що вплив російських кібероперацій виявився “меншим, ніж очікували ми — і вони самі”. [10]

Попри це, звіти Microsoft у поєднанні з дослідженнями інших компаній, таких як Cisco, Google та ESET, а також дані українських органів влади, свідчать про наявність масштабного та динамічного кібернетичного виміру російсько-українського збройного конфлікту. Ймовірно, що, розраховуючи на швидку та успішну військово-наступальну кампанію проти України, російська сторона спочатку вважала достатніми кібероперації, подібні до тих, які застосовувалися у 2008 та 2014 роках. У сценарії “короткої війни” росія, ймовірно, прагнула зберегти українську критичну інфраструктуру у працездатному стані для подальшого використання після захоплення Києва та встановлення контролю над Україною. Це також може пояснювати концентрацію зусиль на зборі персональних даних українських громадян шляхом шпигунства.

Однак, після провалу наступу на Київ і переходу росії до ведення локалізованої війни на підтримку сепаратистського режиму у східному регіоні Донбасу, її кібертактика повернулася до підходів, які застосовувалися проти України з 2014 року: атак на критичну національну інфраструктуру з метою послаблення спроможності держави забезпечувати оборону своєї території. Проте цього разу масштаб та інтенсивність російських кібероперацій значно перевищували все, що раніше застосовувалося проти України. Один із американських посадовців у сфері кібербезпеки охарактеризував це як “масштабний” кібернаступ, спрямований на досягнення стратегічного ефекту. [34]

Однією з ключових причин провалу російської федерації стало посилення української кібербезпеки завдяки допомозі розвідувальних, кібербезпекових та інших державних структур Сполучених Штатів Америки і Великої Британії. У роки, що передували вторгненню, США суттєво

інвестували у розвиток спроможностей та стійкості української системи кібербезпеки. Зокрема, Міністерство енергетики США співпрацювало з Україною у сфері посилення кіберзахисту енергетичного сектору, а Міністерство фінансів США — у напрямі підвищення кіберстійкості фінансових послуг.

Починаючи з 2020 року, Сполучені Штати Америки розміщували технічних експертів у структурах українського уряду з метою посилення спроможностей України щодо реагування на кіберінциденти та відновлення після них. Крім того, США постачали програмне й апаратне забезпечення для підвищення рівня захищеності та стійкості об’єктів критичної інфраструктури. Також із грудня 2021 року Кіберкомандування США направило фахівців, які «проводили оборонні кібероперації спільно з персоналом Кіберкомандування України, здійснюючи пошук активності противника та виявлення вразливостей». Паралельно Сполучені Штати надавали дистанційну розвідувальну, аналітичну та консультативну підтримку з-за меж України. Аналогічну допомогу здійснювали британські служби GCHQ та National Cyber Security Centre.

Після початку війни Федеральне бюро розслідувань США (FBI) та Агентство з кібербезпеки й безпеки інфраструктури США (CISA) надали Україні додаткову розвідувальну інформацію, слідчу підтримку та технічні рекомендації. Водночас United States Agency for International Development сприяло розгортанню додаткових американських технічних експертів і забезпечило передачу понад 6750 засобів екстреного зв’язку, зокрема супутникових телефонів та терміналів передачі даних, для постачальників життєво важливих послуг, державних службовців і операторів критичної інфраструктури в ключових секторах, таких як енергетика та телекомунікації. [29]

У 2021 році Microsoft надала фінансову та технічну допомогу на суму 239 мільйонів доларів США. У квітні 2022 року компанія повідомила, що її

команди з кібербезпеки тісно співпрацюють з українськими урядовцями для виявлення та усунення загроз українським мережам, одночасно інформуючи уряд США та надаючи посадовцям НАТО й Європейського Союзу докази поширення російської кібердіяльності за межі України. [72]

Водночас значного навантаження зазнавали й російські мережі, які піддавалися постійним кібератакам з боку численних добровольчих груп та окремих осіб, що діяли переважно з власної ініціативи. До таких груп належали “Network Battalion 65”, “Elves” (об’єднання понад 4000 добровольців із 13 країн Центральної та Східної Європи), “Cyber Partisans” (антиурядова група з Білорусі), а також хакерське організація Anonymous, якп на початку вторгнення оголосила “війну” росії. Діяльність цих груп не координувалася безпосередньо українською владою, однак отримувала її схвалення. Вони стали відомими під назвою “IT Army of Ukraine” переважно тому, що потенційні цілі для атак публікувалися в урядовому Telegram-каналі з аналогічною назвою.

Діяльність таких кібердобровольців включала масштабне викрадення та оприлюднення електронних листів, паролів, документів, фінансової інформації та інших даних російських організацій. У березні 2022 року, за даними литовської компанії цифрової безпеки Surfshark, обсяг оприлюднених у мережі облікових даних, пов’язаних із росією, перевищив половину світового показника та був у п’ять разів більшим, ніж два місяці до цього. [83]

Сполучені Штати Америки та Велика Британія проводили ефективні розвідувальні операції проти росії як до початку війни, так і під час неї, про що свідчить значний обсяг розвідувальної інформації, оприлюдненої ними публічно. Відомо, що вони тісно співпрацювали з українською владою у сфері захисту та безпеки українських мереж. Водночас невідомо, чи включала ця співпраця проведення наступальних кібероперацій, або ж США та Велика Британія здійснювали власні операції паралельно з українськими.

Росія неодноразово стверджувала, що США брали участь у таких діях, посилаючись, зокрема, на інтерв'ю телеканалу Sky News у червні 2022 року з генералом Paul Nakasone, командувачем US Cyber Command. У ньому він заявив: "ми провели серію операцій у всьому спектрі - наступальних, оборонних та інформаційних операцій», додавши, що ці дії були законними та здійснювалися за погодженням із відповідними цивільними органами влади". [91]

Проте кібероперації також використовуються для маніпулювання даними та інформацією або навіть для їх навмисного впровадження з метою впливу на мислення, поведінку людей, введення їх в оману чи прихованого примусу. Такі дії можуть мати широкий спектр як військових, так і невійськових наслідків у мирний час і під час війни та можуть здійснюватися як військовими структурами, так і цивільними суб'єктами. Сполучені Штати та Велика Британія переважно використовували саме такі операції у боротьбі проти терористичної організації Islamic State, і саме вони, ймовірно, є найбільш поширеним видом наступальних кібероперацій у сучасних конфліктах, зокрема й у російсько-українському збройному конфлікті. [16]

Вторгнення 2022 року супроводжувалося застосуванням складного шкідливого програмного забезпечення, спрямованого на конкретні елементи української інфраструктури. Однією з помітних родин шкідливого програмного забезпечення була "X", що мала багатофункціональні можливості — від шпигунства до безпосередньої дестабілізації. Аналіз цього програмного забезпечення виявив його потенційне походження, а схожість програмного коду вказувала на зв'язок із раніше відомими кіберінструментами, афілійованими з Росією [79]

Попри це, оборонні спроможності України, посилені міжнародною співпрацею та допомогою міжнародних партнерів, продемонстрували ефективність колективної кібероборони. Упродовж років, що передували вторгненню 2022 року, Україна активно зміцнювала власну систему

кібернетичної оборони, усвідомлюючи неминучі загрози з боку свого російської федерації. Значну роль у захисті від російських кібернаступів, а й у проведенні контратак відігравав так званий український кіберальянс, створений українськими активістськими групами хакерів. Їх діяльність охоплювала викриття російських кампаній дезінформації та оприлюднення розвідувальних даних про російських оперативників.

Усвідомлюючи масштаб кіберзагроз, з якими зіткнулася Україна, низка західних держав, зокрема Сполучені Штати Америки та країни-члени Європейського Союзу, надали українським посадовцям підготовку у сфері кібербезпеки. Метою цього навчання було посилення спроможності України ефективно виявляти, пом’якшувати та нейтралізувати кіберзагрози.

У такий спосіб Україна впровадила інтегрований підхід до кібероборони, об’єднавши цивільних експертів, хактивістські групи та військовий персонал. Ця стратегія співпраці забезпечила створення комплексного механізму захисту шляхом консолідації ресурсів, експертних знань і розвідувальної інформації для протидії складним кіберзагрозам. [16]

Окрім державних кібероперацій, цифровий простір став ареною активного розвитку громадянського спротиву. Соціальні мережі перетворилися на поле боротьби за інформаційні наративи. Поки росія намагалася контролювати інформаційний простір за допомогою кампаній дезінформації, українські громадяни та глобальна інтернет-спільнота протидіяли цим наративам, часто використовуючи цифрові інструменти для перевірки інформації в режимі реального часу. [50]

У міру розгортання війни виникли численні платформи та ініціативи, створені звичайними громадянами для перевірки та спростування неправдивої інформації. Ці зусилля часто ґрунтувалися на методологіях розвідки з відкритих джерел (OSINT), у межах яких публічно доступні дані, такі як супутникові знімки, дописи в соціальних мережах і методи геолокації,

використовувалися для підтвердження або спростування певних тверджень.[31; 50]

Кібернетичний вимір російсько-українського збройного конфлікту 2022 року став першим прикладом воєнного кіберконфлікту між двома державами, чиї кіберможливості виявилися загалом співставними. Українська система кібербезпеки, яка й без того була достатньо потужною, отримала додаткове посилення завдяки підтримці урядів-партнерів та приватних компаній, тоді як ефективність російських кібероперацій виявилася нижчою, ніж очікувалося.[16]

Операція Служби безпеки України “Павутина”, реалізована у 2025 році проти стратегічної авіації російської федерації, стала однією з найбільш резонансних та концептуально нових форм застосування сили у сучасному збройному конфлікті. Її особливість полягає не лише у значному військовому ефекті, що полягав у виведенні з ладу елементів російської стратегічної авіації, але й у характері самої операції, яка поєднала ознаки кінетичної та кібернетичної атаки. У цьому контексті “Павутина” становить особливий інтерес для міжнародно-правового аналізу кібероборони, оскільки демонструє поступове стирання меж між кінетичними та кібернетичними формами ведення війни.

За відкритими даними, зокрема за електронним виданням Business Insider, операція полягала у прихованому переміщенні FPV-дронів на територію російської федерації, їх маскуванні у мобільних контейнерних конструкціях та подальшому одночасному ударі по кількох стратегічних аеродромах, де базувалися літаки Ту-95, Ту-22М3, А-50 та інші носії крилатих ракет, що систематично використовувалися для обстрілів української території. Особливу увагу привертає використання елементів автономної навігації, відкритого програмного забезпечення, систем дистанційного управління та алгоритмів автоматизованого наведення у

випадку втрати зв’язку з оператором. Це дозволяє стверджувати, що операція не була виключно традиційною диверсійною акцією, а базувалася на комплексному поєднанні фізичного та цифрового компонентів.

У міжнародно-правовому вимірі ключовим питанням є визначення того, чи може операція “Павутина” вважатися формою “активної оборони” (active defense). Концепція активної оборони у сучасній безпековій доктрині передбачає застосування проактивних або навіть наступальних заходів із метою недопущення, послаблення або припинення ворожого нападу. На відміну від суто пасивної оборони, що обмежується реагуванням після фактичного завдання шкоди, активна оборона допускає нейтралізацію джерела загрози до моменту реалізації чергового акту агресії. У випадку “Павутини” об’єктами ураження стали саме ті військові платформи, які систематично використовувалися російською федерацією для ракетних атак по цивільній інфраструктурі України. Відтак операція мала не лише наступальний, але й превентивно-оборонний характер, оскільки була спрямована на зниження спроможності держави-агресора здійснювати подальші удари. [54]

Положення статті 51 Статуту ООН закріплюють невід’ємне право держави на індивідуальну та колективну самооборону у випадку збройного нападу. У сучасній доктрині міжнародного права дедалі частіше визнається, що самооборона може включати не лише безпосереднє відбиття атаки, але й дії, спрямовані на припинення безперервної загрози. Російські стратегічні бомбардувальники, які використовувалися для регулярних масованих ударів по українських містах, становили постійний інструмент такого нападу. За цих умов їх ураження може розглядатися як реалізація права на самооборону, навіть попри те, що операція здійснювалася поза безпосередньою лінією фронту та на території держави-агресора. Саме це наближає “Павутину” до концепції active defense у сучасному безпековому розумінні. [11]

Додатковим аргументом на користь кваліфікації операції як активної оборони є її функціональний зв’язок із захистом цивільного населення. Відомо, що літаки Ту-95 та Ту-22М3 регулярно використовувалися для запуску ракет Х-101, Х-555 та інших засобів ураження по українській енергетичній та цивільній інфраструктурі. Знищення або пошкодження таких платформ мало безпосередній вплив на здатність росії продовжувати кампанію терору проти цивільного населення України. Таким чином, операція мала оборонну мету навіть попри свій виражений наступальний спосіб реалізації.

Разом із цим постає питання про те, чи слід вважати операцію “Павутина” суто кінетичною операцією, чи все ж гібридною операцією із кібернетичними елементами. Формально безпосереднє ураження літаків здійснювалося фізичними засобами - FPV-дронами з вибуховими зарядами. З цієї точки зору наслідки операції були класично кінетичними. Проте сучасне міжнародне право дедалі більше враховує не лише результат застосування сили, але й технологічний механізм її реалізації. У випадку “Павутини” вирішальне значення мали цифрові системи управління, автономна навігація, захищені комунікаційні канали, програмне забезпечення для координації рою дронів та елементи штучного інтелекту. Без цих компонентів реалізація операції у настільки складному географічному та оперативному масштабі була б практично неможливою. [22]

Особливого значення набуває використання автономних алгоритмів наведення у разі втрати сигналу управління. Відповідно до оприлюднених даних, окремі безпілотники могли продовжувати виконання завдання після втрати зв’язку з оператором, використовуючи попередньо запрограмовані маршрути та алгоритми розпізнавання цілей. Це свідчить про наявність елементів цифрової автономності, що зближує операцію з сучасними формами cyber-enabled operations - тобто операціями, у яких кібернетичні технології забезпечують або суттєво посилюють кінетичний ефект. У

міжнародній практиці такі дії дедалі частіше розглядаються як складова ширшого кібернетичного середовища ведення війни.

Водночас важливо розмежовувати власне кібероперацію та операцію із використанням цифрових технологій. У вузькому значенні кібероперацією традиційно вважається діяльність, спрямована безпосередньо проти інформаційних систем, мереж, серверів або цифрової інфраструктури противника. “Павутина” не містила публічно підтверджених ознак проникнення у російські інформаційні системи чи руйнування цифрової інфраструктури шляхом програмного впливу. Основний ефект був досягнутий фізичним знищенням літаків. Саме тому кваліфікувати її як “чисту” кібероперацію було б юридично неточно. Проте її можна вважати гібридною операцією, у якій кібернетичні засоби стали невід’ємною частиною кінетичного ураження. [54; 55]

У сучасній доктрині міжнародної безпеки дедалі частіше використовується поняття hybrid warfare, що охоплює інтеграцію традиційних військових засобів, інформаційних операцій, кіберінструментів, автономних систем та асиметричних методів впливу. “Павутина” фактично демонструє нову стадію еволюції такого підходу. Операція поєднала агентурну підготовку, приховану логістику, цифрові системи координації, автономні технології, елементи штучного інтелекту та високоточне кінетичне ураження. Саме комплексність цих компонентів дозволяє говорити про гібридний характер операції, а не про її виключно кінетичну природу.

Крім того, операція має важливе значення для розвитку міжнародно-правового розуміння кібероборони. Традиційно кібероборона асоціювалася із захистом інформаційних систем від несанкціонованого доступу, атак на мережі або шкідливого програмного забезпечення. Проте сучасні конфлікти демонструють, що кібероборона поступово виходить за межі суто цифрового простору та охоплює комплекс заходів із нейтралізації технологічної

спроможності противника. У цьому сенсі “Павутина” може розглядатися як приклад розширеного розуміння кібероборони, де цифрові системи стають інструментом досягнення оборонного ефекту у фізичному просторі.

Таким чином, операція СБУ “Павутина” не може бути однозначно класифікована ані як виключно традиційна військова атака, ані як класична кібероперація у вузькому значенні цього терміна. Її правова та технологічна специфіка полягає саме у поєднанні кінетичних і цифрових елементів, що дозволяє характеризувати її як гібридну операцію в межах сучасної концепції кібероборони. Водночас її спрямованість на нейтралізацію засобів здійснення постійних атак проти України дає підстави розглядати її як форму активної оборони, сумісної з правом держави на самооборону відповідно до статті 51 Статуту ООН. Операція також демонструє трансформацію сучасної війни, у якій цифрові технології дедалі більше інтегруються у фізичне застосування сили, формуючи нову архітектуру міжнародної безпеки та нові виклики для міжнародного права. [11; 54]

В межах розгляду проблеми правового розгляду кібероборони в рамках міжнародного права через призму російсько-українського збройного конфлікту, в першу чергу важливо зазначити відсутність офіційного правового визначення простору, оборони та інших складових збройних конфліктів, відображеного в міжнародних правових актах. В цьому зв’язку, перспективним рішенням з цього напряму є створення Спеціального трибуналу за злочин агресії проти України, покликаного виконати функцію міжнародного кримінального трибуналу над російською федерацією.

Ефективність спеціального трибуналу розкривається в комплексному підході до вироблення та кодифікації міжнародних правових підходів щодо кібероборони та кіберпростору із врахуванням авторитетних наукових доктрин, зокрема Таллінського посібника 2.0. Досвід попередніх міжнародних кримінальних трибуналів - Нюрнберзького, Югославського та

Руандського - підтверджує важливість міжнародних судових інституцій для цілей міжнародного права не тільки у контексті застосування чинних положень міжнародного права, але й у створенні судових прецедентів, які формують нові норми з подальшою їхньою інтеграцією до загальноприйнятих стандартів систем jus in bello та jus ad bellum. [122; 125]

В умовах російської збройної агресії саме спеціальний міжнародний трибунал здатний виробити узгоджені між собою дефініції кібервійни, кібероборони, кібернападу та правового статусу КП та операцій в ньому таким чином, щоб вони не суперечили вже існуючим правовим нормам із суміжних понять. За аналогією, МКТЮ внаслідок своєї процесуальної значимості створив дефініції міжнародного та неміжнародного збройного конфлікту, які були стали повноцінним доповненням міжнародного гуманітарного права. [122]

Одним із найбільш значимих потенційних внесків Спеціального трибуналу за злочин агресії проти України може стати закріплення правового статусу кібероборони через призму статті 51 Статуту ООН, яка гарантує невід'ємне право держави на індивідуальну та колективну самооборону у разі збройного нападу. Досвід Естонії у 2007 році не був визнаний збройним нападом, але від того часу практика держав та доктринальні підходи змінили вектор руху у бік визнання наступальних кібероперацій, еквівалентних за наслідками збройному нападу кінетичного характеру, як "збройного нападу" у розумінні jus ad bellum. Таллінський посібник 2.0, послідовні позиції Сполучених Штатів Америки, Французької Республіки, Великої Британії, Естонської Республіки та інших держав прямо віддзеркалюють консенсус щодо застосовності положень Статуту ООН до КП. У цьому ключі, новий трибунал, оперуючи фактичними обставинами збройної агресії проти України, зафіксованих міжнародними та українськими національними групами під час розслідувань, матиме реальну можливість вперше окреслити

межі правомірної самооборони кібернетичними засобами та методами у відповідь на кібернапад. [11; 17; 54]

Одночасно із цим, Спеціальним трибуналом в межах його повноважень може бути здійснено визначення правового статусу КП та його застосовності в міжнародному гуманітарному праві. І хоча право збройних конфліктів є нейтральним та універсальним у застосуванні до засобів і методів ведення війни згідно з Декларацією Мартенса, відсутність офіційно визначених у правовому полі вказаних понять та підтверджень щодо їх застосовності до правил та звичаїв ведення війни, призводить до різностороннього трактування та уникнення відповідальності, як у випадку з кібератаками проти цивільної інфраструктури Естонії у 2007 році. Закріплення трибуналом застосовності принципів міжнародного гуманітарного права до кіберпростору передбачатиме можливість уніфікації стандартів оцінки нападів у цифровому середовищі. [24; 105; 106]

Аналогія з прецедентами Міжнародних кримінальних трибуналів щодо Руанди та колишньої Югославії зможе концептуалізувати ключові дефініції кібервійни, -оборони та -нападу. Наприклад, у МКТЮ, починаючи з рішення у справі проти Tadić, було уніфіковано рамки кваліфікації конфліктів у практиці держав та міжнародних органів. Подібно, Нюрнберзьким процесом було розкрито матеріальний зміст злочинів проти миру й людяності, які дедалі були закладені в основу універсальних конвенцій та Статуту Міжнародного кримінального суду. Таким чином, у цифровому вимірі, Спеціальний трибунал зможе надати критерії для практичного визначення кібернападу для відповідності порогу застосовності jus ad bellum та jus in bello. [42; 125]

Додатково Спеціальним трибуналом щодо злочину агресії проти України може бути проведено межі категорій операцій, тобто: кібердії, які становлять “напади” (атаки) у розумінні Додаткового протоколу І до Женевських конвенцій, а які - ні. Зрештою, головною метою Спеціального

трибуналу за злочин агресії проти України стане офіційне закріплення в міжнародному праві поняття “кібервійни” та суміжних із них, а також притягнення до відповідальності російську федерацію за збройну агресію, а “кремлівський режим” за злочини геноциду. Як в свій час Міжнародний кримінальний трибунал щодо колишньої Югославії одночасно унормував поняття міжнародних та неміжнародних конфліктів та притягнув до відповідальності винних у скоєні воєнних злочинів осіб з вищого політичного складу. [42]

Узагальнюючи кібернетичний вимір російсько-українського збройного протистояння, слід констатувати, що збройна агресія російської федерації проти України стала одним із найбільш показових прикладів трансформації сучасних воєнних конфліктів.

Починаючи з 2014 року, росія системно використовувала кібероперації як елемент гібридної агресії, поєднуючи їх із військовими, інформаційними та політичними інструментами впливу. Повномасштабне вторгнення 2022 року підтвердило тенденцію до інтеграції кібероперацій у загальну військову стратегію держави-агресора. Російська федерація активно використовувала DDoS-атаки, дефейсинг вебресурсів, шкідливе програмне забезпечення типу “wiper”, а також операції зі збору персональних даних українських громадян.

Попри значну кількість яких, Україні вдається уникнути загальнонаціонального колапсу критичної інфраструктури. Однією з причин цього - модернізація української системи кібербезпеки у співпраці зі Сполученими Штатами Америки, Великою Британією та іншими міжнародними партнерами. Допомога партнерів включає технічну підтримку, розгортання спеціалістів з кібербезпеки, постачання обладнання, проведення спільних оборонних кібероперацій та постійний обмін розвідувальною інформацією.

Україна змогла сформувати комплексний підхід до кібероборони, який об’єднав державні органи, міжнародних партнерів, приватний сектор і громадянське суспільство. Наприклад, формування так званої “IT Army of Ukraine” стало прикладом нової моделі цифрового громадянського спротиву, яка поєднала ініціативи держави та добровольчих груп.

Кібернетичний компонент війни також продемонстрував поступове стирання меж між кібероперaціями та традиційними військовими діями. Прикладом цього є операція Служби безпеки України “Павутина”, яка поєднала фізичне ураження стратегічної авіації російської федерації з використанням цифрових технологій, автономної навігації, програмного забезпечення та елементів штучного інтелекту.

Досвід російсько-українського збройного конфлікту також виявив суттєві прогалини міжнародного права у сфері регулювання кіберпростору та кібероборони. Відсутність офіційно закріплених міжнародно-правових дефініцій кібернападу, кібервійни, кібероборони та правового статусу КП ускладнює застосування норм jus ad bellum та jus in bello до сучасних цифрових конфліктів.

У цьому контексті особливого значення набуває перспектива створення Спеціального трибуналу за злочин агресії проти України. Такий трибунал потенційно здатний не лише забезпечити притягнення російської федерації до відповідальності за агресію, але й сформувати нові міжнародно-правові підходи до кваліфікації кібероперацій, визначення меж самооборони у КП та застосування МГП до цифрового середовища.

Досвід Нюрнберзького трибуналу, МКТЮ та Трибуналу щодо Руанди свідчить про здатність міжнародних судових інституцій формувати нові правові стандарти та уніфікувати підходи до кваліфікації сучасних форм конфліктів. У випадку російсько-українського збройного конфлікту це може стосуватися визначення критеріїв кібернападу, меж правомірної

кібероборони, статусу КП як сфери застосування міжнародного гуманітарного права, а також розмежування між кібероперaціями та іншими формами гібридного впливу.

Таким чином, російська збройна агресія стала ключовим етапом у розвитку сучасного розуміння кібероборони та міжнародно-правового регулювання КП. Вона продемонструвала, що кібероперації є невід'ємним елементом сучасної війни, здатним впливати на функціонування критичної інфраструктури, інформаційний простір, державне управління та військові процеси. Одночасно російська збройна агресія проти України підтвердила необхідність вироблення уніфікованих міжнародних норм, які б регламентували застосування сили у КП, визначали межі відповідальності держав та недержавних суб'єктів, а також забезпечували ефективний механізм міжнародно-правового реагування на кіберзагрози у майбутніх конфліктах.

Висновки

Актуальність дослідження кібероборони у міжнародному праві зумовлена стрімким розвитком інформаційних технологій та трансформацією кіберпростору на окрему сферу міжнародного протиборства. Сучасні кібероперації дедалі частіше використовуються державами як інструмент політичного, військового та стратегічного впливу, що створює нові виклики для міжнародної безпеки та чинної системи міжнародного права. В умовах зростання кількості кібератак на критичну інфраструктуру, державні інформаційні системи та оборонний сектор особливої ваги набуває питання формування ефективних міжнародно-правових механізмів кібероборони та вироблення єдиних підходів до правової кваліфікації кібероперацій.

У ході дослідження було досягнуто поставленої мети та виконано визначені завдання: досліджено поняття кібероборони та її місце у системі міжнародного права, проаналізовано джерела міжнародно-правового регулювання у цій сфері, встановлено особливості застосування норм jus ad bellum та jus in bello до кібероперацій, а також здійснено аналіз практики окремих держав і сучасного досвіду України у сфері кібероборони.

В межах кваліфікаційної роботи було досліджено поняття кібероборони та суміжних із ним. Отже, було встановлено, що кібероборона на сучасному етапі розвитку міжнародного права є складним і багатовимірним явищем. Відсутність уніфікованого договірного визначення зумовлює різні доктринальні підходи до тлумачення терміну та його змістового обсягу. У роботі обґрунтовано, що кібероборона повинна розглядатися як сукупність правових, організаційних і технічних заходів держави, спрямованих на запобігання, виявлення та припинення кібероперацій, які можуть становити загрозу суверенітету, територіальній цілісності або міжнародній безпеці.

Також було проаналізовано джерела міжнародного права у сфері кібероборони. Відповідно до статті 38 Статуту МС ООН, джерелами міжнародного права є міжнародні конвенції, міжнародні звичаї, загальні

принципи права, а також судова практика та доктрина найбільш авторитетних фахівців у галузі права.

Аналіз положень Статуту ООН дозволив дійти висновку, що він є фундаментальним джерелом права у сфері кібероборони. Стаття 2(4) Статуту закріплює заборону погрози силою або її застосування, а стаття 51 гарантує державам право на самооборону у випадку збройного нападу. У сучасних умовах це право поширюється і на КП.

МГП, незважаючи на відсутність спеціальних норм, присвячених кібероперaціям, є джерелом у сфері кібероборони. Положення Женевських конвенцій та основні принципи права збройних конфліктів поширюються і на цифровий простір. Особливе значення у цьому контексті має застереження Мартенса, відповідно до якого навіть за відсутності прямого нормативного регулювання сторони конфлікту зобов'язані керуватися принципами гуманності та загальними принципами міжнародного права.

Міжнародні звичаї також застосовуються до сфери кібероборони, зокрема принцип due diligence. Його зміст полягає у необхідності недопущення використання території або кіберінфраструктури держави для здійснення шкідливих кібероперацій проти інших держав.

Особливе місце серед джерел міжнародного права у сфері кібероборони займає наукова доктрина - Таллінський посібник 2.0. Хоча він не має юридично обов'язкової сили, він є комплексним науково-практичним коментарем, який систематизує підходи до застосування міжнародного права у КП.

В межах аналізу jus ad bellum було встановлено, що кібероперації за певних умов можуть бути кваліфіковані як застосування сили або збройний напад у розумінні статті 2(4) Статуту ООН. Зокрема, було визначено, що в межах статті 51 Статуту ООН кібероборонні операції відповідають праву держави на самооборону. Водночас відсутність універсальних критеріїв такої

кваліфікації створює значну правову невизначеність. У роботі підкреслено, що ключовими критеріями оцінки мають виступати масштаб, наслідки та рівень шкоди, завданої кібероперацією, зокрема її вплив на критичну інфраструктуру та функціонування держави.

Правові позиції Франції, Нідерландів, Великої Британії та Естонії підтверджують можливість кваліфікації кібератак як збройних нападів за умови співмірності їхніх наслідків із кінетичними атаками. Аналогічного підходу дотримується й Талліннський посібник 2.0, який акцентує увагу не на технічному характері зброї, а на ефекті та наслідках її застосування.

Обов'язковими у сфері кібероборони є принципи необхідності та пропорційності, які визначають допустимі межі оборонного реагування. Принцип необхідності вимагає, щоб застосування сили мало місце за відсутності ефективних ненасильницьких альтернатив. Принцип пропорційності обмежує масштаб, інтенсивність і тривалість кібероборонних операцій обсягом, необхідним для нейтралізації загрози.

У контексті jus in bello доведено, що норми міжнародного гуманітарного права можуть застосовуватися до кібероперацій за умови їхнього зв'язку зі збройним конфліктом. Водночас існуючі положення МГП не завжди повною мірою враховують специфіку КП, зокрема питання атрибуції, визначення об'єктів атаки та оцінки шкоди. Це зумовлює необхідність подальшого розвитку як договірних, так і доктринальних підходів до регулювання кібероперацій у збройних конфліктах.

Щодо цифрових даних як об'єкту у сфері дії МГП закріпилось два протилежних підходи. Перший - це позиція Міжнародного комітету Червоного Хреста, полягає в незастосовності міжнародного гуманітарного права до цифрових даних через їхню нематеріальну та невидиму природу. Другий, підтриманий як деякими урядами держав, так і науковою спільнотою, зокрема Таллінською дирекцією, наголошує на застосовності

положень МГП до цифрових даних через їхню значимість для військових та цивільних цілей.

Щодо критичної інфраструктури було досліджено, що кібероперації проти систем енергозабезпечення, водопостачання, медичних інформаційних систем або інших об'єктів, які забезпечують базові життєві потреби населення, можуть спричинити катастрофічні гуманітарні наслідки, розглядатимуться як порушення МГП.

Подвійність використання сучасної кіберінфраструктури пояснюється частим застосуванням комп'ютерних мереж, телекомунікаційних систем, програмного забезпечення, соціальних мереж, кабелів зв'язку тощо як цивільним населенням, так і державними органами або збройними силами. У випадку використання таких об'єктів для підтримки воєнних дій вони можуть набувати статусу військової цілі.

Аналіз практики окремих держав, зокрема Естонії, Сполучених Штатів Америки та Ізраїлю, дозволив виявити різні моделі організації кібероборони. Практика США свідчить про системний підхід до формування кібероборони як окремого компоненту національної оборони держави. Протягом останніх десятиліть державними органами було створено нормативну, стратегічну та інституційну основу функціонування кіберпростору в умовах сучасних загроз. Ухвалення оборонних кіберстратегій у 2011, 2015 та 2018 роках відобразило поступову трансформацію поглядів держави на природу кіберзагроз та способи реагування на них. Створення Кіберкомандування США (USCYBERCOM) та Сил кібермісій стало наслідком комплексного науково-правового підходу до розуміння ролі КП у збройних конфліктах. USCYBERCOM отримало широкі повноваження щодо захисту мереж Міністерства оборони США, планування та проведення кібероперацій, а також координації діяльності з іншими видами збройних сил.

Ізраїль, у свою чергу, характеризується інтеграцією кібероборони в загальну систему національної безпеки з високим рівнем оперативної ефективності. Його кібероперації “Stuxnet” (спільна із США), “Flame” та “Duqu” стали прикладами складних багаторівневих кіберінструментів. Stuxnet був спрямований на фізичне пошкодження промислової інфраструктури через ураження програм управління обладнанням. Flame використовувався переважно для кіберрозвідки та збору інформації. Duqu був орієнтований на підготовку майбутніх кібероперацій шляхом викрадення даних розвідувального значення.

Естонія демонструє високий рівень інституціоналізації кіберзахисту та активну участь у формуванні міжнародних доктринальних підходів. Естонська модель кібероборони сформувалася під безпосереднім впливом кібератак 2007 року, які продемонстрували критичну залежність сучасної держави від цифрової інфраструктури. Масштабні атаки на органи державної влади, банківський сектор, інформаційні системи та інтернет-провайдерів фактично паралізували функціонування окремих сфер державного управління та стали поштовхом до комплексного переосмислення підходів до кібербезпеки. Особливістю її моделі є існування добровольчого підрозділу Küberkaitseliit, який інтегрований до системи національної оборони та забезпечує швидку координацію між державними та приватними спеціалістами у сфері кібербезпеки.

Проаналізований у межах кваліфікаційної роботи досвід України у сфері кібероборони в умовах збройної агресії, дозволив встановити її системний характер та тісний зв’язок із загальною оборонною стратегією держави. Виявлено, що КП є альтернативною площиною гібридного протистояння. Таке підкреслюється в операції СБУ “Павутина”, де кібероперації супроводжують традиційні воєнні дії, що підсилює актуальність застосування як норм jus ad bellum, так і jus in bello.

Було розглянуто доцільність подальшого розвитку міжнародно-правових механізмів притягнення до відповідальності за агресивні дії у КП. У цьому контексті перспективним напрямом визначено створення спеціального міжнародного трибуналу щодо злочину агресії проти України, який міг би забезпечити належну правову кваліфікацію, у тому числі кібероперацій як елементів агресії. Такий підхід має історичні паралелі з діяльністю Нюрнберзького трибуналу, Трибуналів щодо колишньої Югославії та Руанди, які відіграли ключову роль у розвитку міжнародного кримінального та гуманітарного права.

Загалом, проведене дослідження дозволяє зробити висновок, що міжнародне право перебуває на етапі активного формування підходів до регулювання кібероборони. Водночас існуюча нормативна база є недостатньою та потребує подальшого розвитку як на глобальному, так і на регіональному рівнях. Перспективи вдосконалення пов’язані з поступовою кодифікацією правил поведінки держав у кіберпросторі, розширенням договірної бази та зміцненням міжнародного співробітництва у сфері кібербезпеки.

Список використаних джерел

1. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks / Yin C., Zhu Y., Fei J., He X. // IEEE Access. 2017. Vol. 5. P. 21954–21961.
2. Aggression against Ukraine : resolution / adopted by the General Assembly // United Nations General Assembly (11th emergency special session : 2022).
3. An Enhancing Framework for Botnet Detection Using Generative Adversarial Networks / Yin C., Zhu Y., Liu S., Fei J., Zhang H. // 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD). 2018. P. 228–234.
4. Application of International Humanitarian Law in Changing Dimensions of Armed Conflict vis-à-vis Cyber Warfare / Ashutosh Pandey // Unity Journal. 2025. Vol. 6, № 1. P. 284–296. DOI: 10.3126/unityj.v6i1.75698.
5. Are Cyber Powers Challenging International Humanitarian Law, or Is Cyberspace Still a Legal Blind Spot? / Dr. Ahmed Aubais Al-Fatlawi // Arab Journal of Legal and Political Sciences. 2025. Vol. 2, № 2. DOI: 10.64184/ajlps.V2.I2.Y2025.
6. Armed Attack in Cyberspace: Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands' Right of Self-Defence / F.M.E. Oorsprong, P.A.L. Ducheine, B.M.J. Pijpers // Amsterdam Law School Legal Studies Research Paper. 2021. № 2021-29. 31 p. DOI: 10.2139/ssrn.3934417.
7. Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts : ICRC Expert Meeting, 21–22 January 2020, Geneva // International Committee of the Red Cross. Geneva, 2021. 40 p.
8. BlackEnergy Malware Used in Ukraine Power Grid Attacks / Eduard Kovacs. 2016. URL: https://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks/ (дата звернення: 15.05.2026).
9. Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia / Dita Aulia Salma, Fahlesa Munabari // Jurnal Diplomasi dan Keamanan. 2024. DOI: 10.36080/djk.2412.
10. By Invitation: The Head of GCHQ Says Vladimir Putin Is Losing the Information War in Ukraine / Jeremy Fleming // The Economist. 2022.
11. Charter of the United Nations : міжнародний документ від 26 червня 1945 р. // United Nations Treaty Series. Vol. 1. P. 16.

12. Chinese Approach to International Law with Regard to Cyberspace Governance and Cyber Operation: From the Perspective of the Five Principles of Peaceful Co-existence / Lixin Zhu, Wei Chen // Chinese Journal of International Law. DOI: 10.1163/22115897_02001_010.
13. Cyber Attacks as “Force” Under UN Charter Article 2(4) / Matthew C. Waxman // Yale Journal of International Law. 2011. Vol. 36.
14. Cyber Operations and the Jus Ad Bellum Revisited / Michael N. Schmitt // Villanova Law Review. 2011. Vol. 56.
15. Cyber Warfare and Precautions Against the Effects of Attacks / Eric Talbot Jensen // Texas International Law Journal. 2013. Vol. 48.
16. Cyber Warfare as Part of Information Warfare of Russia Against Ukraine Since the Beginning of the 2022 Russian Invasion / Kateryna Fedotenko // Věda a perspektivy. 2023. № 8(27). DOI: 10.52058/2695-1592-2023-8(27)-351-357.
17. Cyber-attacks and the Right of Self-Defense: A Case Study of the Netherlands / Ferry Oorsprong, Paul Ducheine, Peter Pijpers // Journal of Cyber Policy. 2023. DOI: 10.1080/25741292.2023.2179955.
18. Cyberdeterrence and Cyberwar / Martin C. Libicki. Santa Monica : RAND Corporation, 2009. 238 p.
19. Cybersecurity and Cyber Defence: National Level Strategic Approach / Darko Galinec, Darko Možnik, Boris Guberina // Automatika. 2017. Vol. 58, № 3. DOI: 10.1080/00051144.2017.1407022.
20. Cybersecurity Military Entities of the United States of America / Monika Pajurek // Przegląd Strategiczny.
21. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, 29 November / 11 December 1868.
22. Defence Ukraine – Operation Spiderweb: Ukraine's $7bn Strike, електронне видання. URL: https://www.defenceukraine.com/en/insights/operation-spiderweb-ukraine-drone-attack-analysis/ (дата звернення 15.05.2026)
23. De la guerra / Karl Von Clausewitz. Barcelona : Ediciones Obelisco, 2015.
24. Deterrence and Dissuasion in Cyberspace / Joseph S. Nye Jr. // International Security. 2017. Vol. 41, № 3. DOI: 10.1162/ISEC_a_00266.

25. “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” / D. Albright, P. Brannan, C. Walrond. — Washington, D.C. : Institute for Science and International Security, 2010.
26. Estonia’s National Cybersecurity and Cyberdefense Posture Policy and Organizations / Kevin Kohler. Zürich : ETH Zurich, 2020. DOI: 10.3929/ethz-b-000438276.
27. “Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security”, Christian Czosseck, Rain Ottis, Anna-Maria Talihärm, International Journal of Cyber Warfare and Terrorism, vol. 1, no. 1, 2011, pp. 24–34, DOI: https://doi.org/10.4018/ijcwt.2011010103
28. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/ (дата звернення 15.05.2026)
29. Fact Sheet on U.S. Security Assistance for Ukraine / U.S. Department of Defense. 10 May 2022. URL: U.S. https://www.defense.gov/News/Releases/Release/Article/3027295/fact-sheet-on-us-security-assistance-for-ukraine/ (дата звернення: 15.05.2026).
30. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note by the Secretary-General. — New York : United Nations, 2015. — 17 p. — (UN Doc. A/70/174)
31. Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia’s War Against Ukraine / D. Svyrydenko, W. Możgin // Future Human Image. 2022. Vol. 17. P. 39–46.
32. “Harm and Its Moral Significance.” / S. V. Shiffrin // Legal Theory. — 2012. — Vol. 18, No. 3. — P. 357–398. — DOI: 10.1017/S1352325212000080.
33. Hotspot Analysis: Stuxnet / Marie Baezner, Patrice Robin // Center for Security Studies ETH Zürich.
34. How Russia’s Vaunted Cyber Capabilities Were Frustrated in Ukraine / David Ignatius // The Washington Post. 21 June 2022. URL: https://www.washingtonpost.com/opinions/2022/06/21/russia-ukraine-cyberwar-intelligence-agencies-tech-companies/ (дата звернення: 15.05.2026).
35. Information Practices of Resistance During the 2022 Russian Invasion of Ukraine / I. Kouper // Proceedings of the 85th Annual Meeting of the Association for

Information Science & Technology. Pittsburgh, Pennsylvania, 29 October – 1 November 2022. P. 157–168.

36. Information Security Management: American Experience / Sarancha Viktor, Shabunina Viktoriia, Tur Oksana // Law and Public Administration.
37. International Law and the Use of Force: The Jus Ad Bellum / Michael N. Schmitt // International Law Studies.
38. International Law Applied to Operations in Cyberspace. — Paris : Ministry of the Armed Forces of France, 2019. URL: https://documents.unoda.org/wp-content/uploads/2021/12/French-positionon-international-law-applied-to-cyberspace.pdf (дата звернення 15.05.2026)
39. Iran and Israel Cyber Warfare and Interference of US / Muhammad Umar // Strategic Review of Asia. 2024. Vol. 3, № 2. DOI: 10.70670/sra.v3i2.824.
40. Israel Defense Forces and National Cyber Defense / Lior Tabansky // Connections. 2020. Vol. 19, № 1. DOI: 10.11610/Connections.19.1.05.
41. Israel's National Cybersecurity and Cyberdefense Posture Policy and Organizations / Jasper Frei. Zürich : ETH Zurich, 2020. DOI: 10.3929/ethz-b-000438397.
42. ICTY, Prosecutor v. Tadić, Appeals Chamber Judgment / International Criminal Tribunal for the Former Yugoslavia. 1999.
43. International Journal of Communication 4 (2010), Book Review 1144–1146. Martin C. Libicki “Cyberdeterrence and Cyberwar” / Negar Kahen // International Journal of Communication. 2010. Vol. 4. P. 1144–1146.
44. “Lessons from Stuxnet.” / T. M. Chen, S. Abu-Nimeh // Computer. — 2011. — Vol. 44. — P. 91–93.
45. Machine Learning and Deep Learning Methods for Cybersecurity. Yang Xin, Mingcheng Gao, Haixia Hou. URL: https://www.researchgate.net/publication/325159145 (дата звернення 15.05.2026)
46. Military and Paramilitary Activities in and against Nicaragua : Judgment of the Court, 27 June 1986. — The Hague : International Court of Justice, 1986. — (I.C.J. Reports 1986, p. 14)
47. Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law / Kubo Mačák // International Review of the Red Cross. DOI: 10.1017/S0021223714000260.

48. Military Objectives in International Humanitarian Law / Robert Kolb // Yearbook of International Humanitarian Law.
49. Multilingualism and Universal Access to Cyberspace, UNESCO, електронне видання. URL: https://www.unesco.org/en/communication-information/multilingualism-cyberspace#:~:text=Recommendation%20concerning%20the%20Promotion%20and,Paris%20on%2015%20October%202003 (дата звернення 15.05.2026)
50. Narrative Battles: The Impact of Open-Source Intelligence on the Framing of Russia's War on Ukraine / A. Brantly // Paper presented at the Danyliw Seminar on Contemporary Ukraine. 2022.
51. National Cyber Strategy of the United States of America: Experience for Ukraine / V. Shemchuk // Information and Law. DOI: 10.33270/0119113.
52. Nation-State Cyber Operations Legal Considerations: An Estonian Case Study / Agata Małecka // Security and Defence Quarterly. DOI: 10.37105/sd.139.
53. NATO Allies Condemn Russia's Invasion of Ukraine in the Strongest Possible Terms. 24 February 2022. URL: https://www.nato.int/en/news-and-events/articles/news/2022/02/24/nato-allies-condemn-russias-invasion-of-ukraine-in-the-strongest-possible-terms (дата звернення: 15.05.2026).
54. NATO Cooperative Cyber Defence Centre of Excellence: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by Michael N. Schmitt. Cambridge : Cambridge University Press, 2017.
55. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual. URL: https://ccdcoe.org/research/tallinn-manual/ (дата звернення 15.05.2026)
56. „Od ofiary do światowego lidera. Estonia po cyberatakach z 2007 roku", Agnieszka Warchoł, Politeja, t. 20, nr 5(86), 2023, s. 307–327, DOI: https://doi.org/10.12797/Politeja.20.2023.86.14
57. Offensive Cyberspace Operations for Cyber Security / Gazmend Huskaj // Journal of Information Security.
58. Oxford Public International Law / Christine D. Gray. Oxford : Oxford University Press.
59. Personal Data Breaches Are Falling – Except in Russia / Claudia Glover // Techmonitor. 15 April 2022. URL:

https://techmonitor.ai/technology/cybersecurity/personal-data-breaches-are-falling-except-in-russia (дата звернення 15.05.2026)

60. Problematic Issues of Communicating Cyberattacks in Ukraine: Possible Ways to Solve the Problem. URL: http://www.niss.gov.ua/content/articles/files/CyberCommunication-e06b5.pdf (дата звернення: 15.05.2026).
61. Proportionality in Cyberwar and Just War Theory / Fredrik D. Hjorthen, James Pattison // Ethics and Information Technology. 2023. DOI: 10.1080/16544951.2023.2179244.
62. "Proportionality in the Morality of War." / Hurka T. // Philosophy & Public Affairs. — 2005. — Vol. 33, No. 1. — P. 34–66. — DOI: 10.1111/j.1088-4963.2005.00024.x.
63. "Proportionality and Necessity in Jus in Bello." / J. McMahan // The Oxford Handbook of the Ethics of War / ed. by H. Frowe, S. Lazar. — Oxford : Oxford University Press, 2018. — P. 418–439.
64. "Proportionate Defense." / J. McMahan // Journal of Transnational Law and Policy. — 2013–2014. — Vol. 21. — P. 1–36.
65. Reno v. American Civil Liberties Union, 521 U.S. 844 (1997). URL: https://supreme.justia.com/cases/federal/us/521/844/ (дата звернення 15.05.2026)
66. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses / Stephen Herzog // Journal of Strategic Security. DOI: 10.5038/1944-0472.4.2.3.
67. "Rights, Goods, and Proportionate War." / C. Eberle // The Monist. — 2016. — Vol. 99, No. 1. — P. 70–86. — DOI: 10.1093/monist/onv030.
68. Russia Unexpectedly Poor at Cyberwar: European Military Heads // Defense Post. 9 June 2022. URL: https://www.thedefensepost.com/2022/06/09/russia-poor-cyberwar/ (дата звернення: 15.05.2026).
69. Satellite Outage Caused "Huge Loss in Communications" at War's Outset – Ukrainian Official / Raphael Satter // Reuters. 15 March 2022. URL: https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/?utm_source=chatgpt.com (дата звернення: 15.05.2026).

70. Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations / Irène Couzigou // International Review of Law, Computers & Technology.
71. Six Books of the Commonwealth / Jean Bodin.
72. Special Report: Ukraine / Microsoft Digital Security Unit. 27 April 2022. P. 3. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (дата звернення: 15.05.2026).
73. Statement by NATO Heads of State and Government on Russia's Attack on Ukraine. 25 February 2022. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/02/25/statement-by-nato-heads-of-state-and-government-on-russias-attack-on-ukraine (дата звернення: 15.05.2026).
74. "Stuxnet, the Real Start of Cyber Warfare?" / T. Chen // IEEE Network. — 2010. — Vol. 24. — P. 2–3. — DOI: 10.1109/MNET.2010.5634434.
75. Stuxnet Facts Report: A Technical and Strategic Analysis / M. De Falco. — Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2012.
76. "Stuxnet Attackers Used 4 Windows Zero-Day Exploits." / R. Naraine. — 2010.
77. Territorial Integrity of Ukraine : Resolution adopted by the General Assembly on 27 March 2014 № 68/262 // United Nations General Assembly.
78. The Cyber Defense Review // Army Cyber Institute at West Point.
79. The Cyber Dimension of the Russia–Ukraine War / M. Willett // Survival. 2022. Vol. 64, № 5. P. 7–26.
80. The Department of Defense Law of War Manual. Washington : U.S. Department of Defense, 2015 (updated July 2023).
81. The Inadequacy of International Humanitarian Law in Regulating Cyber Warfare: A Critical Analysis of the Geneva Conventions and Additional Protocols / Bonaventure Kirumbe Ambrose // East African Journal of Law and Ethics. DOI: 10.37284/eajle.8.1.3873.
82. The Israeli Unit 8200 – An OSINT Based Study. Trend Analysis / Sean Cordey. Zürich : ETH Zurich. DOI: 10.3929/ethz-b-000389135.
83. The Evolution of the IT Army of Ukraine / Stefan Soesanto // Survival. 2023. DOI: 10.1080/00396338.2023.2218701.
84. The Law of Cyber Warfare: Quo Vadis? / Michael N. Schmitt // Stanford Law & Policy Review.

85. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation / Erica D. Lonergan // Journal of Cybersecurity. 2023. DOI: 10.1093/cybsec/tyad006.
86. The Right of Legitimate Defense Against Cyberattacks in Public International Law / Dr. Amr Ezzat Mahmoud Elhaw // Journal of Law and Emerging Technologies.
87. The Israeli Cyber Emergency Response Team (CERT) Principles of Operation // Israel National Cyber Directorate.
88. “The Cousins of Stuxnet: Duqu, Flame, and Gauss”, Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, Márk Félegyházi, Future Internet, vol. 4, no. 4, 2012, pp. 971–1003, DOI: https://doi.org/10.3390/fi4040971
89. The Functions of Social Conflict / Lewis A. Coser. New York : Free Press, 1956.
90. United Nations Security Council Resolution 678 : UN Doc. S/RES/678, para. 2. — 29 November 1990
91. US Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command / Alexander Martin // Sky News. 1 June 2022. URL: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (дата звернення: 15.05.2026).
92. U.S. Sends Top Security Official to Help NATO Brace for Russian Cyberattacks / David E. Sanger // The New York Times. 1 February 2022. URL: https://www.nytimes.com/2022/02/01/us/politics/russia-ukraine-cybersecurity-nato.html (дата звернення: 15.05.2026).
93. War with Shadows: Persistent Engagement and the Power-Topologies of US Military Cyberspace Operations / Tim Stevens // Contemporary Security Policy.
94. War, Aggression and Self-Defence / Yoram Dinstein. Cambridge : Cambridge University Press.
95. Where is the SIMNET for Cyberspace? / Scott D. Lathrop // Simulation & Gaming. 2023. DOI: 10.1177/15485129231169781.
96. Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations / Michael N. Schmitt // International Review of the Red Cross.
97. World Wide Warfare: Jus ad Bellum and the Use of Cyber Force / Marco Roscini. Cambridge : Cambridge University Press.

98. Who’s Behind Cyber Attacks?, Anna Fleck, електронне видання, URL: https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/ (дата звернення 15.05.2026)
99. Актуальні проблеми держави і права : збірник наукових праць. Вип. 103 / Національний університет «Одеська юридична академія». Одеса, 2024.
100. Актуальні проблеми сучасних міжнародних відносин : матеріали Всеукраїнської науково-практичної конференції, 17–18 листопада 2023 р., м. Дніпро / ред. кол.: І. В. Іщенко, І. К. Головко, П. Г. Петров. Дніпро : ПрінтДім, 2023. 290 с.
101. Види збройних конфліктів та їх правове регулювання / С. Я. Бескоровайний // Юридична наука. – 2014. – № 3. – С. 116–126.
102. Виявлення кібератак та підвищення інформаційної безпеки на основі технології нейронних мереж в умовах кібервійни / Олександр Васильович Лебідь, Світлана Сергіївна Кіпоренко, Валерія Юріївна Вовк // Наукові перспективи. 2023. DOI: 10.52058/2786-6025-2023-1(15)-238-256.
103. Гібридна війна та її вплив на захист прав людини та демократичні цінності в Україні / Д. С. Коротков // Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Питання політології». – 2017. – Вип. 31. – С. 97–101.
104. Державець / Нікколо Макіавеллі. — Київ : Основи, 1998. — 84 с.
105. Додатковий протокол I до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів : міжнародний документ від 08.06.1977 р.
106. Додатковий протокол II до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв неміжнародних збройних конфліктів : міжнародний документ від 08.06.1977 р.
107. Женевська конвенція про захист цивільного населення під час війни : міжнародний документ від 12.08.1949 р.
108. Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни / Я. С. Мануїлов // Інформація і право. – 2023. – № 1(44). – С. 154–167.
109. Заборонені засоби ведення кібервійни / Микола Камчатний. – Київ : Юридична думка, 2021. – 214 с.

110. Зміст та практичне застосування принципу пропорційності в міжнародному праві / Б. А. Тоцький // Альманах міжнародного права. – 2019. – Вип. 22. – С. 95–102.

111. ESET спільно з представником ДССЗЗІ України розповіли про загрозу Industroyer2 на конференції Black Hat : електронне видання. 25.08.2022. URL: https://www.eset.com/ua/about/newsroom/press-releases/company/eset-sovmestno-s-predstavitelem-dsszi-ukrainy-predstavili-issledovanie-ugrozy-industroyer2/?srsltid=AfmBOoqJw9eidmoM6nu_uBFKsVeW0SXVp4LypEVn6ImrRaAEzwihdsmW (дата звернення: 15.05.2026).

112. Історія становлення кібервійни як складової політичного процесу / Ю. В. Завгородня // Актуальні проблеми політики. 2023. DOI: 10.32782/app.v72.2023.6.

113. Кібератака на українську енергетику: як це було : електронне видання. 04.03.2016. URL: https://texty.org.ua/fragments/65835/Kiberataka_na_ukrajinsku_jenergetyku_jak_ce_bulo-65835/ (дата звернення: 15.05.2026).

114. Кібервійна як різновид інформаційних війн. Захист кіберпростору України / Яна Вікторівна Дмитрук, Тетяна Олександрівна Гришанович, Людмила Ярославівна Глинчук, Оксана Костянтинівна Жигаревич // Молодий вчений. – 2022. – № 5(105). – С. 248–252.

115. Кібервійна як сучасний метод ведення збройних конфліктів / І. Воєводін // Юридичний науковий електронний журнал. – 2023. – № 4. – С. 382–385.

116. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – Київ : НІСД, 2014. – 328 с.

117. Конвенція про кіберзлочинність (ETS № 185) : міжнародний документ від 23.11.2001 р. // База даних «Законодавство України» / Верховна Рада України.

118. Конфліктологія: курс лекцій, енциклопедія, програма, таблиці : навчальний посібник / Віктор Петрінко. – Ужгород : Видавництво УжНУ «Говерла», 2020. – 360 с.

119. Крок до стандартів НАТО та посилення цифрової безпеки / Дмитро Забзалюк, Іванна Соловей // Юридична газета online. – 2023. – 15 червня.

120. Матеріали круглого столу «Філософія війни та миру: від античності до сьогодення». Інститут філософії імені Г. С. Сковороди НАН України. 28 березня 2023 р.

121. Міжнародні кібернавчання Locked Shields – 2022. Проблемні питання в підготовці складових сил оборони та безпеки України / Євген Олександрович Живило, Олександр Олександрович Черноног // Сучасні інформаційні технології у сфері безпеки та оборони. – 2022. – № 3(45). – С. 123–130.

122. Міжнародний кримінальний трибунал щодо колишньої Югославії // United Nations International Criminal Tribunal for the Former Yugoslavia.

123. Міноборони ініціювало роботу над законодавчим визначенням поняття «кібервійна» / [Електронний ресурс] : офіц. вебсайт Міністерства оборони України. 2024. URL: https://mod.gov.ua/news/minoboroni-inicziyuvalo-robotu-nad-zakonodavchim-viznachennyam-ponyattya-kibervijna (дата звернення: 15.05.2026)

124. Мілітаризація викликів та загроз в кіберпросторі як операційному середовищі / Євген Олександрович Живило // Сучасні інформаційні технології у сфері безпеки та оборони. – 2021. – № 1(40). – С. 95–102.

125. Нюрнберзькі принципи : електронне видання. URL: https://www.un.org/ru/documents/decl_conv/conventions/principles.shtml (дата звернення: 15.05.2026).

126. Оборона як ефективний засіб забезпечення безпеки суспільства та держави / Валерій Сокуренко // Право і безпека. – 2022. – № 2(85). – С. 13–19.

127. Оборона / П. А. Мінєєв // Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г.Железняк [та ін.] ; НАН України, НТШ. — К. : Інститут енциклопедичних досліджень НАН України, 2022. — Режим доступу: https://esu.com.ua/article-74633 (дата звернення: 15.05.2026)

128. Політична енциклопедія / редкол.: Ю. Левенець, Ю. Шаповал та ін. Київ : Парламентське видавництво, 2011. 808 с. ISBN 978-966-611-818-2.

129. Правове регулювання здійснення кібероборони / В. М. Роллер // Інформація і право. – 2021. – № 2(37). – С. 87–94.

130. Правове регулювання кібератак під час збройних конфліктів / О. Р. Пасешник // Юридичний науковий електронний журнал. – 2023. – № 7. – С. 456–459.

131. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України від 29 груд. 2021 р. № 1426 // Офіційний вісник України. – 2022. – № 10. – Ст. 523.

132. Про оборону України : Закон України від 06.12.1991 № 1932-XII // Відомості Верховної Ради України. 1992. № 9. Ст. 106.

133. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 403.

134. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021 // Офіційний вебпортал Верховної Ради України.

135. Проєкт Закону України № 12349 «Про Кіберсили Збройних Сил України».

136. Про сутність кібероборони як виду воєнних дій / П. М. Сніцаренко // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ ім. Івана Черняховського. – 2021. – № 2(72). – С. 114–120.

137. Протокол спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти, а також при усуненні їх наслідків / Є. О. Живило, І. В. Ромашко // Сучасний захист інформації. – 2023. – № 1. – С. 52–59.

138. Специфіка порушення прав людини в умовах військових конфліктів: постановчо-концептуальний характер і особливості / А. О. Білоус, А. О. Пастернак // Юридичний науковий електронний журнал. – 2022. – № 10. – С. 54–58.

139. Структуризація аналізу міжнародних конфліктів та загроз / Олександр Цвєтков // Politicus. – 2021. – № 4. – С. 23–29.

140. Сутність кібероборони України: визначення та протиріччя правових та теоретичних засад / Світлана Анатоліївна Паламарчук, Наталія Анатоліївна Паламарчук, Роман Михайлович Штонда, Тетяна Василівна Побережець // Інформація і право. – 2023. – № 4(47). – С. 98–107.

141. Теоретико-методологічні засади дослідження поняття «війна» / Світлана Матвієнків, Назар Головчинський // Політичне життя. – 2020. – № 3. – С. 18–24.

142. Трактат про військове мистецтво / Нікколо Макіавеллі. — Київ : Основи, 1998. — 472 с.

143. Україна в умовах російської агресії. Виклики та відповіді : монографія / І. В. Букрєєва, І. Г. Верховцева, В. В. Гулай та ін. – Київ : Видавництво Ліра-К, 2023. – 404 с.

144. Усунення Україною одного з компонентів "ядерної тріади" Російської Федерації: подробиці спецоперації "Павутина", електронне видання, URL: http://pravotoday.in.ua/content/znischennya-ukrayinoyu-elementu-yadernoyi-triadi-rosiyi-detali-specoperaciyi-pavutina/ (дата звернення 15.05.2026)