УДК 340.12.
DOI: https://doi.org/10.21564/2663-5704.67.342243

***Трофименко Володимир Анатолійович***, кандидат юридичних наук, доцент, доцент кафедри філософії, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
*e-mail: v.a.trofymenko@nlu.edu.ua*
*ORCID iD: 0000-0003-2240-3727*

# КІБЕРКОНФЛІКТ ТА ПРАВОВЕ ПОЛЕ ЙОГО ІСНУВАННЯ: СПРОБА ФІЛОСОФСЬКО-ПРАВОВОГО ОСМИСЛЕННЯ

*Публікацію присвячено кіберконфлікту і правовому полю його існування. Наголошується, що головною науковою проблемою є відсутність єдиного розуміння кіберконфлікту та його характерних рис. У свою чергу це створює певну проблему створення правового поля його існування. Головною причиною цього є специфічність кіберконфлікту. Таким чином, показується, що проблема правового поля кіберконфлікту залишається відкритою й потребує нагального вирішення.*

***Ключові слова:*** *кіберконфлікт, кіберпростір, міжнародне право, міжнародне гуманітарне право, кіберлегалізм.*

***Постановка проблеми.*** Усе нове, що відкриває людина, завжди має дві сторони: позитивну та негативну. Негативна сторона може розглядатись не тільки як така, що завдає прямої шкоди, а й як така, що розширює, нехай поза правовим полем, можливості суб'єкта. Одним з історичних прикладів може слугувати грошова система. Гроші та інші засоби платежу є полегшувальним механізмом в системі обміну, але винахід кожного нового такого засобу (гроші, облігації тощо) завжди породжував певну схему зловживання[1]. Сучасним прикладом наведеної ситуації може служити кіберпростір. Позитивним боком кіберпростору є полегшення життя людини: багато операцій і дій робляться не виходячи з дому та за малі проміжки часу, інтернет став однією з провідних сфер інформування та спілкування та ін. Негативними його проявами є кіберзлочинність, кіберконфлікт і кібервійна. І якщо кіберзлочин переважно завдає шкоди окремій людині, то останні дві форми можуть завдати шкоду великим групам людей, окремій державі чи взагалі міжнародній спільноті. А збитки можуть мати не тільки грошовий, а й інші виміри.

[1] Див.: Фергюсон Н. Еволюція грошей. Фінансова історія світу. Київ : Наш формат, 2017. 384 с.

Тому кіберконфлікт сьогодні є однією з «найгарячіших» тем для наукової спільноти. Досліджуються суб'єкти та об'єкти цієї проблеми, мотиви, способи та методи ведення, а також можливості протидії.

Зважаючи, що розвиток кіберпростору все ще набирає обертів, розширюються і сфери застосування кіберконфлікту, породжуючи нові напрямки для наукових досліджень. Цьому сприяє також підвищення рівня небезпечності кіберконфлікту, що також можна пояснити стрімкістю розвитку інтернету. Усе це зберігає важливість і необхідність наукового розгляду сутності кіберконфлікту, метою якого є протидія йому й профілактика.

***Аналіз останніх досліджень і публікацій.*** Досліджуючи кіберпростір, колектив учених із Канади, США, Великої Британії та Нідерландів ставить питання його віднесення до об'єктів критичної інфраструктури. На початку 2020 р., відмічають вони, швидке впровадження інструментів дистанційної роботи та зв'язку урядами, компаніями та окремими особами в усьому світі збільшило залежність від кіберінфраструктури для нормального функціонування держав, підприємств і суспільств. Оскільки ці інструменти міцно впроваджуються в повсякденне життя в усьому світі, виникає питання, чи слід їх вважати критично важливою інфраструктурою, чи, можливо, навіть чимось важливішим. Науковці зазначають, що в низці держав критична важливість навколишнього середовища для збереження людського життя була визнана шляхом поширення правосуб'єктності – а отже, і юридичних прав – на екологічні суб'єкти. Такі країни, як Колумбія, Еквадор, Нова Зеландія, Індія, надали юридичні права на різні річки, озера, парки та природу загалом. У своїй статті вчені досліджують майбутні можливості й випадки, коли держави можуть розглянути можливість надання юридичних прав іншим нечутливим, але критично важливим суб'єктам. Дивлячись у майбутнє, де людське життя стає дедалі залежнішим від взаємозалежних систем у кіберпросторі, чи існує ймовірність того, що цим системам буде надано правосуб'єктність? На думку дослідників, дистанційна робота та її наслідки для кібербезпеки можуть призвести до абсолютно нового визнання важливості залежностей кіберпростору та, як наслідок, до нового правового трактування. На тлі тривалих дебатів щодо правового регулювання кіберпростору, включаючи право збройних конфліктів, це викличе ще складніші правові міркування, особливо з огляду на транскордонні залежності й системи, що впливають на численні юрисдикції. Вчені, таким чином, формують перспективний концептуальний підхід до вивчення політичних міркувань і потенційних наслідків, якщо високо взаємозалежним кіберсистемам у далекому майбутньому буде надано такий самий захист, як і елементам навколишнього середовища [1].

Такий підхід може змінити ставлення і до кіберконфлікту в бік констатації його більш великої небезпечності.

Важливою ланкою наукових досліджень нових сфер є термінологічний апарат. У сфері кіберконфлікту до цієї проблеми звертаються естонські вчені Лоренц П. та Оттіс Р. В останні роки, звертають увагу вони, відбулася низка міжнародних конфліктів, які відобразилися паралельною кампанією ворожих дій у кіберпросторі. Це спонукало до різних спроб проаналізувати таке явище й пояснити загрозу ширшій громадськості. На жаль, констатують автори, звіти й аналіз часто є заплутаними і можуть містити досить довільне використання різних кібермодних слів. З цього випливає, що існує потреба у формальній суворій моделі для опису й аналізу кіберконфліктів. Формальні методи також необхідні для розроблення наступальних і оборонних систем на основі штучного інтелекту для кіберконфліктів. Щоб вирішити цю проблему, вчені пропонують формалізовану систему ключових термінів у кіберконфліктах. Вони починають з перегляду понять «знання», «дані», «інформація». На основі цього науковці переходять до визначення «інформаційної системи» й «інтелектуальної системи». Ними надається формальний опис концепції знищення та фальсифікації інформації й пояснюються поняття конфіденційності, цілісності та доступності як частин системи. Потім вони пропонують визначення кіберзброї, кіберінцидентів, кібератак, кібершпигунства, кіберконфліктів та, нарешті, кібервійни. Їхня структура базується на формальній логіці й дозволяє проводити теоретичні, експериментальні або емпіричні дослідження з математично доведеними результатами. Таким чином, на думку естонських вчених, вона може забезпечити міцну основу для дослідження кіберконфліктів, які часто базуються на менш суворих методах [2].

В етичному аспекті розглядає наведену вище термінологічну проблему англійський вчений П. Корніш. Ідея про те, що вдавання до конфлікту та його ведення можуть і повинні бути обмежені з етичних міркувань, на думку науковця, добре зрозуміла. Чому ж тоді важко застосувати це розуміння до кіберпростору? По-перше, пише П. Корніш, досі не зрозуміло, як визначити «конфлікт», «насильство» та «агресію» в кіберпросторі; що може бути «кібердоменом»; і що може означати безпека в ньому або поза ним. Чи використати розуміння, що існує, та просто ставити перед ним префікс «кібер», чи є щось якісно відмінне в кібербезпеці й поведінці, яку вона дозволяє або якої вимагає? Тоді, констатує вчений, існує набагато глибша, більш структурна проблема, з якою доводиться боротися. Етична проблема кіберпростору полягає в тому, що це штучне середовище, яке пропонує як співпрацю, з одного боку, так і суперечки та конфронтацію, – з іншого. І важко знати ідентифікатори хорошої та поганої поведінки в будь-який момент. Кіберпростір, про-

довжує дослідник, вперто є дополітичним, достратегічним і тому доетичним; він ще не сприйнятливий до форм політичної та стратегічної організації, з якими ми знайомі, і тому стійкий до нормативних обмежень, за допомогою яких ми очікуємо керувати конфліктами й організованим насильством, а також пом'якшувати їх. Як висновок, науковець вважає, що кібербезпеку слід розглядати як арену для людського обміну, на якій дипломатія, переговори, торг, компроміс, поступки та застосування морального судження не лише вважаються належними, а й можливими [3].

Концептуально намагається визначити саме поняття кіберконфлікту французький вчений С. Теллат. Протягом останнього десятиліття, відмічає він, кіберконфлікт став головною рисою міжнародної політики та все більшим занепокоєнням щодо стратегічної стабільності та колективної безпеки. На жаль, вважає дослідник, кіберконфлікт потерпає від відсутності концептуальної ясності щодо його впливу на колективну безпеку та відсутності консенсусу серед міжнародних суб'єктів щодо того, як його інтерпретувати. Вчений пропонує розуміти кіберконфлікт як процес, що розвивається, зумовлений двома факторами: способом конфігурації цифрового простору та способом включення тактичних, організаційних, стратегічних і доктринальних характеристик, пов'язаних із кібербезпекою, до сфери національної та міжнародної безпеки. Обидва фактори, на його думку, заохочують наступальну поведінку, але також демонструють риси, що вказують на стриманість [4].

***Формулювання мети.*** Основна мета публікації – показати специфічність та неоднозначність феномену кіберконфлікту, що впливають на формування його правового поля.

***Викладення основного матеріалу.*** Кіберпростір є особливою нефізичною сферою, тому кіберконфлікт має специфічний характер і вимагає особливого ставлення. На це звертає увагу група канадських вчених К. Лепрехт, Дж. Цеман та Д. Скіллікорн. Кіберпростір, пишуть вони, – це нова сфера діяльності зі своїми власними характеристиками. Кіберзброя якісно відрізняється від кінетичної: вона генерує ефекти некінетичними засобами за допомогою інформації, технологій і мереж. Її властивості, можливості й обмеження порівнянні з якісною різницею між звичайною та ядерною зброєю. Нова зброя та її цілі в новій сфері, продовжують науковці, породжують низку невирішених політичних проблем на внутрішньому, двосторонньому й міжнародному рівнях щодо стримування, атрибуції й реагування. Вони також створюють нові ризики: невизначеність щодо непередбачуваних наслідків, очікування ефективності й невизначеність щодо реакції як цілі, так і міжнародного співтовариства. Кібероперації пропонують значні переваги для держав у досягненні стратегічних цілей як приховано, так і відкрито. Однак, вважають авто-

ри, без стратегічної бази для стримування та, можливо, стримування їхнього використання, підвищення передбачуваності поведінки держав і не держав за відсутності взаємних норм та обмеження їхнього впливу, середовище, де держави стикаються з постійними атаками, які, проте, перебувають нижче порогу збройного конфлікту, створює політичну дилему, яка посилює колективну небезпеку [5].

На специфічності дослідження конфліктів у кіберпросторі наголошують американські дослідники Р. Шандлер і Д. Канетті. Дослідження кіберконфліктів, наголошують автори, надзвичайно складне. Ця галузь є непростою, якісних даних мало, міжнародні відносини оповиті таємницею, і, незважаючи на свою уявну повсюдність, кіберсила лише нещодавно вийшла на поле бою. Зіткнувшися з цими викликами, на думку науковців, потрібно піднятися, щоб відповідати на виклики досліджень у галузі кібербезпеки, застосовуючи креативні методи, які збирають перевірені та доказові дані, а також дозволяють створювати прогностичні моделі кіберповедінки. На цьому тлі вони пропонують бачення досліджень у галузі кібербезпеки, яке охоплює культуру ретельного дослідження, заснованого на теоретично обґрунтованих і політично релевантних дослідженнях. Учені виділяють дві ключові особливості. По-перше, дослідження на перетині кібербезпеки й політології повинні враховувати людський вимір кіберконфлікту. Підхід до кібербезпеки, заснований на людській безпеці, ставить людей як основні об'єкти безпеки та визнає, що аналіз на індивідуальному рівні може пролити світло на тенденції макрорівня. По-друге, кібердослідження повинні використовувати суворі, емпіричні методи. Науковці пропонують застосовувати широкий спектр методів збирання емпіричних даних, що охоплюють якісні й кількісні, експериментальні та спостережні дослідження. Невід'ємною частиною є те, що всі наукові дослідження повинні дотримуватись найвищих стандартів відтворюваності й фальсифікації [6].

Про непридатність традиційного мислення, зокрема військового, у кіберпросторі, пишуть вчені з США Дж. Калберг і Т. Кук. Вчені відмічають, що комплексних теорій конфлікту в кіберсвіті ще не розроблено, але використання традиційної військової стратегії та оперативних концепцій замість стратегій, що існують у цій сфері, може вводити в оману, призводячи до помилкових оцінок та несприятливих результатів. На їхню думку, чотири принципи кіберсвіту створюють серйозні проблеми для застосування традиційних військових стратегій у кіберконфліктах. Кіберсвіт характеризується таким: 1) відсутність сталості об'єкта, що підриває концепцію маневру; 2) обмежене або відсутнє вимірювання ефективності в наступальній кібератаці; 3) конфлікти, що виконуються з обчислювальною швидкістю, що усуває

часове вікно для змістовного стратегічного лідерства; 4) анонімність, що робить сторони конфлікту невідомими. Як результат, роблять висновки вчені, використання традиційного військового мислення і поведінки, що залежить від шляху, в кіберпросторі, ймовірно, призведе до неправильних висновків щодо стратегічних досягнень і можливостей на доконфліктній стадії, а також збільшить ризик стратегічної невдачі під час конфлікту та надасть можливість для стратегічного сюрпризу противника [7].

Просторово-часовим характеристикам та рушійним силам кіберконфлікту приділяє увагу колектив китайських вчених: Дж. Донг, С. Чен та ін. Останніми роками, звертають увагу автори, безперервно з'являються зловмисні кіберактивності, які спонсоруються державами, що призводить до дедалі складнішого міжнародного ландшафту кібербезпеки. Щоб відповісти на цей виклик, проведено масштабні дослідження. Але, на жаль, ці дослідження рідко кількісно аналізують характеристики і фактори, що впливають на кіберконфлікти, з геополітичної точки зору. У цьому контексті, на основі набору даних, що охоплює інциденти кіберконфліктів, національні внутрішні характеристики і двосторонні відносини, вчені використовують такі методи, як аналіз соціальних мереж і статистичний регресійний аналіз, щоб дослідити еволюційні тенденції, структуру мережі, моделі зв'язку й рушійні сили кіберконфліктів. Результати їхньої роботи показують, що, з одного боку, кіберконфлікти між країнами відображають геополітичну динаміку фізичного світу й демонструють характеристики регіоналізму, подібні до традиційної геополітичної конкуренції. З іншого боку, на міждержавні кіберконфлікти впливають внутрішні особливості й зовнішня політика з вираженими регіональними відмінностями. Підсумовуючи, вчені застосовують комплексний та багатовимірний підхід з метою надання аналітичних даних і посилань для відповідних досліджень [8].

Кіберконфлікту без війни присвячується дослідження французького дослідника Т. Лібетро. Кіберконфлікт без війни, зазначає він, відіграє дедалі важливішу роль у сучасній політиці безпеки. Присвячуючи дослідження трьом європейським членам НАТО – Нідерландам, Франції та Норвегії, автор статті розширює фокус дослідження кіберконфлікту без війни за межі його домінантного контексту в США. Вчений порівнює та оцінює, як країни сприймають і як реагують на зміни стратегічного середовища, що характеризуються зростанням кіберконфлікту без війни. Аналіз французького дослідника демонструє, що всі три країни визнають, що кібероперації без війни змінюють стратегічне середовище і ставлять під сумнів ідею розгортання наступальних кіберможливостей виключно як питання війни. Однак автор також визначає стратегічний вакуум, оскільки жодна з них не сформулювала стратегій, які

б детально описували, як військові та розвідувальні структури повинні підходити до нового стратегічного середовища й керувати ним. У статті стверджується, що нинішня відсутність стратегічного керівництва є фундаментальним викликом, який ставить під загрозу європейські суспільства й підриває демократичне управління, оскільки орієнтування в новому просторі стратегічної кіберконкуренції є значним викликом для сучасного європейського державного управління [9].

Цікавою стосовно кіберконфлікту є проблема, озвучена американськими науковцями Дж. Брауном і Т. Фазалем. Це проблема підтвердження / заперечення участі держави в кіберконфлікті. Держави, звинувачені у здійсненні кібероперацій, зазначають автори, зазвичай не підтверджують і не заперечують відповідальність. Вони роблять «заперечення без заперечення» або відмовляються коментувати звинувачення. Ці неоднозначні сигнали поширені, але вони значною мірою нині ігноруються в кіберлітературі, яка схильна трактувати заяву про визнання заслуг як бінарний вибір. Неоднозначність «заперечень без заперечення» та «відмовлення від коментарів», на думку науковців, дозволяє державам досягати двох, здавалося б, протилежних цілей: підтримки кризової стабільності й залишення відкритою можливості своєї участі в атаці. Навмисно залишаючись підозрюваною, держава може маніпулювати сприйняттям суперниками своїх кіберможливостей і рішучості. Відмова заперечувати відповідальність також може формувати сприйняття суперниками можливостей союзників, підвищуючи довіру до стримування. Усього цього можна досягти без ризиків ескалації, які виникли б у разі явного визнання відповідальності. У той час як попередні дослідження зосереджувалися на небезпеці ескалації та обмеженнях дорогої сигналізації за допомогою кібербезпеки, американські вчені показують, що заперечення без заперечення та відмовлення від коментарів роблять кібероперації значно кориснішими, ніж оцінюється в літературі [10].

Ролі відкритості інформації про кіберконфлікти й участі в них держави присвячено публікацію інших американських дослідників – К. Джайлса і К. Хартмана. Безпрецедентна прозорість, зазначають вони, яку продемонстрували нідерландські розвідувальні служби, викривши російських офіцерів ГРУ в жовтні 2018 р., свідчить про низку нових тенденцій у державному врегулюванні кіберконфліктів. Публічні звинувачення США проти посадовців іноземних державних розвідок і навмисне надання Великою Британією інформації, що дозволяє світовим ЗМІ «доксінгувати» офіцерів ГРУ, причетних до отруєння в Солсбері на початку 2018 р., створили прецедент для розкриття інформації, яка раніше була б конфіденційною.

Вчені відмічають, що це суттєве відхилення від попередньої практики, коли деталі кібератак, спонсорованих державою, можна було розкрити лише завдяки тривалим журналістським розслідуванням (як у випадку зі Stuxnet) або завдяки зусиллям корпорацій із кібербезпеки (як у випадку з Red October). У своїй роботі вони використовують тематичні дослідження, щоб проілюструвати характер цього відхилення та розглянути його вплив, включаючи потенційно суттєві наслідки для державного врегулювання кіберконфліктів. У статті вони відмічають певні наслідки, зокрема:

1. Вплив прозорості на сприйняття конфлікту. Більша обізнаність громадськості про атаки, вважають науковці, приведе до більшої громадської згоди щодо необхідності вжиття контрзаходів. Це може поширюватися на готовність громадськості визнати, що існує стан оголошеної або неоголошеної війни з кіберагресором.

2. Результативний вплив на законність. Це додає новий елемент, констатують дослідники, до тривалих дебатів щодо законності кібератак або контратак, впливаючи на момент, коли стан конфлікту політично й соціально, навіть якщо не юридично, вважається таким, що існує.

3. Подальший результативний вплив на дозволи й повноваження щодо проведення кібератак у формі адаптації до очевидного дисбалансу між засобами й методами, доступними агресорам (особливо тим, хто вважає себе вже в конфлікті) та захисникам. Більша відкритість уже посилила публічні й політичні сумніви щодо стриманості, яку демонструють країни НАТО та ЄС у відповідь на дії Росії; ця тенденція продовжиться [11].

Впливу ще одного сучасного технологічного винаходу – штучного інтелекту – на кіберконфлікти присвячено дослідження англійських вчених К. Хартмана і К. Джайлса. Упровадження машинного навчання та потенційно штучного інтелекту (ШІ), пишуть автори, значно розширить можливості автоматизації охоплення масової аудиторії за допомогою адаптованого і правдоподібного контенту. Як наслідок, вони зроблять зловмисників ще потужнішими.

Інструменти для використання машинного навчання в інформаційних операціях розвиваються надзвичайно швидкими темпами і стають все більш доступними для набагато ширшого кола користувачів. До початку 2018 р., зазначають вчені, вважалося, що використання методів штучного інтелекту кіберзлочинцями не очікується найближчим часом, оскільки ці методи спираються на величезні набори даних, відповідно величезну обчислювальну потужність або і те, й інше, вимагають вузькоспеціалізованих навичок і знань. Однак у 2019 р. ці припущення виявилися недійсними, оскільки набори даних і обчислювальна потужність були демократизовані, а вільно доступні інстру-

менти усунули потребу в спеціальних навичках. Цілком розумно припустити, що цей процес продовжиться, трансформуючи ландшафт обману, дезінформації та впливу в інтернеті.

Вчені оцінюють стан кібер- та інформаційних операцій, посилених штучним інтелектом, наприкінці 2019 р. й досліджують, чи може це бути початком суттєвих і небезпечних тенденцій протягом наступного десятиліття. Серед сфер, які вони вважають за необхідне врахувати: кампанії в соціальних мережах із використанням діпфейків; шахрайство з боку генеральних директорів за допомогою діпфейків; машинно генерований політичний астротурфінг; комп'ютери, що реагують на емоційний стан тих, хто з ними взаємодіє, що дозволяє проводити автоматизовані, штучні гуманоїдні дезінформаційні кампанії [12].

Окремою проблемою розгляду кіберконфлікту є його правове врахування. До цієї проблеми звертається дослідник з США М. Хусингтон. Він цікавиться питанням: чи входить кіберконфлікт (кібероперація) у рамки міжнародного права. Багато написано, відмічає автор, про міжнародно-правове регулювання кібероперацій щодо застосування сили (jus ad bellum), у ситуаціях збройного конфлікту (jus in bello) та в мирний час. Міжнародні юристи запропонували свій досвід щодо того, як і яким чином міжнародне право повинне реагувати на виклики й можливості, що виникають. Підходи загалом, хоча й не виключно, поділяються на дві окремі категорії. Або основні проблеми, що виникають у зв'язку з кіберопераціями, можна вирішити за допомогою правил, що існують, та міжнародно-правових структур, або кібероперації являють собою щось настільки принципово нове, що потрібен цілий новий набір правил і структур. Третій підхід передбачає, що наявні структури можуть насправді відповідати викликам кібероперацій, але для того, щоб бути ефективною, дисципліна повинна відкинути ті частини себе, які несумісні з цією новою темою, – фактично суперечачи нинішній доктрині, намагаючись урахувати пред'явлені регуляторні вимоги. Вчений ставить питання: який із цих трьох підходів – «всередині», «поза» або «проти» – є правильним [13]?

Впливу права кіберконфлікту (кібервійни) на міжнародне право присвячено роботу англійського автора К. Мацака. Історично склалося так, пише англійський вчений, що міжнародно-правовий аналіз кібероперацій виник і розвивався саме крізь призму права війни. У своїй статті він аналізує вплив, який розвиток права війни мав і може мати на «ядро» міжнародного права, інакше кажучи, на загальне міжнародне право. У ній аналізуються три ключові виміри взаємозв'язку між правом війни та загальним міжнародним правом: системний, концептуальний і телеологічний. Науковцем стверджується,

що, по-перше, у дискурсі відбувся зсув на системному рівні, у результаті якого академічні дебати та зосередження уваги держав перемістилися з питань права війни на питання загального міжнародного права, включаючи суверенітет, невтручання й відповідальність держав. Краще розуміння цієї тенденції має розвіяти побоювання щодо фрагментації міжнародного права і вплинути на дебати щодо взаємозв'язку між правом війни та «основним» міжнародним правом. По-друге, цей розвиток створив сприятливий ґрунт для міграції певних концепцій із права війни, де вони виникли, розвинулися або закріпилися, у загальне міжнародне право. Показовим прикладом є тест функціональності, який виник як компромісне рішення для визначення того, чи є кібероперація «атакою» згідно з правом війни, але який може запропонувати додаткову корисність в інших галузях міжнародного права, включаючи право державного суверенітету і право контролю над озброєннями та роззброєнням. По-третє, однак, вкрай важливо враховувати унікальну телеологічну основу права війни, перш ніж упроваджувати його правила і принципи в різні нормативні контексти. Як не парадоксально, повне перенесення цих норм може на практиці поставити під загрозу основні гуманітарні міркування [14].

Кібератакам у межах міжнародного права приділяє увагу австралійський дослідник С. Хаатайя. У роботі вченим розглядається використання автоматичних хакерських атак згідно з міжнародним правом на підставі необхідності. Хакерські атаки, визначає він, – це форма активного оборонного заходу, що застосовується у відповідь на кіберзагрози, що включають вплив поза системами або мережами жертви, призначений для пом'якшення кіберзагрози або запобігання їй. Автоматичні хакерські атаки – це системи, які після активації здатні виконувати ці функції без прямого людського контролю. Аргумент необхідності згідно з міжнародним правом щодо відповідальності держав надає підставу, на якій держави можуть вживати заходів, які в іншому випадку були б незаконними, для реагування на кібероперації, що становлять серйозну й неминучу загрозу їхнім суттєвим інтересам. Вчений стверджує, що використання автоматичних хакерських атак може бути виправдано на підставі необхідності, проте система повинна бути здатною проводити низку складних оцінок, щоб забезпечити її відповідність до суворих критеріїв, що вимагаються міжнародним правом. Складність систем, здатних проводити ці оцінки, несе ризик непередбачуваних наслідків та ескалації конфлікту зі швидкістю машини [15].

Проблемі впливу кіберконфлікту на міжнародне гуманітарне право присвячено роботу пакистанського вченого Х. Сухаїла. Динаміка ведення військових дій, зазначає він, змінилася від звичайних війн, що ведуться на полі

бою, до віртуальної війни, оскільки держави були залучені в гонку кіберозброєнь. Від простих розподілених атак типу «відмова в обслуговуванні» (DDoS) до потужних Stuxnet і Flame – кіберзброя різниться за своїми потенційними людськими втратами. Закони про збройні конфлікти (ЗЗК) розроблені гнучко, щоб адаптуватися до змінних обставин. Автор ґрунтується на припущенні, що чинне договірне право є достатнім у багатьох аспектах, проте в деяких сферах також необхідне укладення договорів. Передбачуваним рішенням є комплексна державна практика тлумачення чинних правил (lex lata), що регулюють збройний конфлікт у кіберконтексті. Це вчений пояснює тим, що збройні конфлікти в кіберпросторі відрізняються від кінетичної війни за багатьма вимірами. Світова спільнота ще не досягла консенсусу щодо того, як ЗЗК захищає під час кібервійни. Від визначення основних термінів, таких як атака й об'єкт, до необхідності вирішення питання про атрибуцію. З огляду на таку неоднозначність, робить висновок вчений, міжнародне гуманітарне право (МГП, що використовується як взаємозамінне з ЗЗК) частіше порушуватиметься в конфліктах, що відбуваються в кіберпросторі, ніж у фізичному просторі. Зусилля держав щодо щирого використання чинного законодавства є неодмінною умовою для розвитку МГП у кіберконтексті [16].

Взаємозв'язку національного законодавства й міжнародного права у сфері кіберконфлікту присвячено дослідження австралійського вченого А. Леггата. Талліннський посібник із міжнародного права, що застосовується до кібервійни (2013 р.), пише автор, визначає 95 «основних правил», що регулюють конфлікти, та основу для кожного з них у договірному та звичайному праві. Але чи існує достатня основа на рівні національного законодавства для встановлення норм прийнятної поведінки на міжнародному рівні? Пропозиція вченого полягає в тому, що настав час для нового виду міжнародної співпраці щодо кібервійни та прийнятних норм поведінки в кіберпросторі. Він наводить деталі з різних національних статутів, щоб проілюструвати, як національне законодавство застосовується до кіберпростору. Ним розглядається застосовність чинного національного кримінального й деліктного законодавства, використовуючи гіпотетичні сценарії щодо самооборони, змови і корпоративної відповідальності у приватному секторі. Мета полягає в тому, щоб заохотити експертів до міжнародної співпраці для визнання національних правил, еквівалентних роботі Талліннського суду [17].

Взаємозв'язок національного й міжнародного аспектів у сфері кіберконфліту оновлює бачення ролі держави в цій галузі. На це звертають увагу південнокорейські вчені І. Чо і Дж. Чанг. Вони аналізують обмеження співпраці й розширення конфліктів між державами в кіберпросторі. Як і традицій-

ні простори безпеки по всьому світу, глобальний кіберпростір також є анархічною системою без абсолютної влади чи інституційного статусу. У такій ситуації, вважають вчені, спираючись на кіберсуверенітет і кіберсилу, держава намагається створити інституцію, що застосовується до внутрішнього та міжнародного кіберпростору, щоб зробити кіберсистему сприятливою для самої держави. Оскільки, на відміну від традиційної сили, кіберсила має як матеріальні, так і нематеріальні елементи, держава не може знати рівень кіберсили іншої держави. З цієї причини конфлікти між державами в кіберсфері загострюються. Найактивнішими державами, що конкурують за перевагу в кіберпросторі, є Сполучені Штати і Китай. Вони призводять до різних рівнів визнання та стратегій щодо кіберсфери. Хоча конкуренція між Сполученими Штатами й Китаєм провокує конфлікти, вона також провокує тимчасову співпрацю між державами. Діяльність ООН у сфері кібербезпеки також фрагментована різними міжурядовими установами та управлінськими організаціями. Однак відмінності в стратегії між Сполученими Штатами й Китаєм впливають на інші держави. Зрештою, констатують науковці, хоча напрямок дискусій щодо кібербезпеки було визначено на основі діяльності Групи урядових експертів в ООН, а необхідність міждержавної співпраці була визнана, така співпраця буде лише тимчасовою, оскільки держави вважають внутрішню політику та стратегію важливішими, ніж міжнародні чи регіональні організації співпраці [18].

Але держава може не тільки захищатись, а й нападати. Що робити в цьому випадку? На цю проблему звертає увагу японський вчений Дж. Осава. Протягом останнього десятиліття, зазначає він, національні держави почали використовувати кіберсферу як засіб для задоволення своїх національних інтересів. Огляд тенденцій кібератак за останнє десятиліття, на думку автора, показує, що кібератаки часто трапляються після інцидентів міжнародних розбіжностей або конфліктів. Деякі національні держави вдавалися до кібератаки з метою втручання у внутрішні справи сусідньої країни. Тому кібербезпека стала головним пріоритетом у національній та міжнародній безпеці. Тому, констатує науковець, щоб зупинити потенційних державних супротивників, які здійснюють кібератаки проти національних інтересів, необхідно вживати сильних заходів національної політики безпеки, таких як кіберстримування, колективна кібербезпека та обмін інформацією, щоб запобігти катастрофам, спричиненим серйозною кібератакою [19].

Проблемі правового покарання в кіберсфері як наслідку кіберконфлікту присвячено роботу англійського науковця Л. Келло. Західні країни, пише автор, стикаються з кричущою проблемою покарання в кіберсфері. Інші

країни неодноразово порушують їхні політичні та економічні інтереси. Західні лідери неодноразово попереджають про серйозність таких дій. І все ж жертви неодноразово не карали, щоб стримати правопорушників. У своїй статті науковець розглядає, чому і як виникла ця ситуація та що з цим робити. Західний підхід до запобігання кіберконфліктам підкреслює центральне значення чинного міжнародного права та норм. Однак правова й нормативна база не є адекватною для цієї мети, оскільки вона не забезпечує достатніх підстав для переконливого реагування на дії, що не є війною. Отже, західний підхід зазнав разючої невдачі. Він, констатує вчений, не враховує центральної істини щодо сучасних питань безпеки: значна частина сучасного міждержавного суперництва не відповідає ні руйнівним критеріям війни, ні прийнятним межам мирного суперництва. Швидше, саме немиролюбність або суперництво середнього спектра є більш руйнівним, ніж традиційна діяльність у мирний час, але не фізично насильницьким, як війна. Країни використовують кіберпростір для досягнення деяких політичних та стратегічних цілей війни без жодного пострілу. Відсутність ефективної відповіді Заходу свідчить не про толерантність до агресії, а про нездатність розробити стратегію реагування, яка б відповідала правовим і доктринальним неоднозначностям немиролюбності. Чинне законодавство та норми, робить висновок японський дослідник, є джерелом проблеми, а не її вирішенням. Тимчасове рішення має бути знайдено в розробленні нової доктрини – у консеквенціалістській стратегії, яка впливає на матеріальні інтереси супротивників, щоб стримувати дії, які міжнародне право та стратегія безпеки зазвичай не визнають такими, що заслуговують на рішучу відповідь [20].

***Висновки.*** Наведені вище джерела показують, що кіберконфлікт залишається в призмі зацікавленостей наукової спільноти. Варто відмітити певну складність наукових досліджень із причини швидкого розвитку кіберпростору і неможливості повної прогнозованості розвитку способів і напрямків кіберконфлікту в цьому розрізі.

Констатується теза, що кіберконфлікт все важче врегульовується традиційними способами та методами. Доволі таки вагома частина кіберконфліктів не потрапляє до сфери національного законодавства чи міжнародного права. Більше того, сам кіберконфлікт є вектором впливу та зміни правових норм. Але головною проблемою є питання притягнення до відповідальності за вчинення кіберконфлікту та його негативні наслідки.

У подальшому дослідження кіберконфлікту та його різновидів буде однією з провідних тем наукових розробок.

## ЛІТЕРАТУРА


1. Kushwaha N., Giles K., Singer T., Watson B. Cyber Personhood. *13th International Conference on Cyber Conflict (CyCon) – Going Viral.* Proceeding's 13th International Conference on Cyber Conflict (CyCon) – Going Viral. Tallinn, 2021. P. 275–289.
2. Lorents P., Ottis R. Knowledge based framework for cyber weapons and conflict. *International Conference on Cyber Conflict 2010.* Proceeding's Conference on cyber conflict. Tallinn, 2010. P. 129–142.
3. Cornish P. Deterrence and the Ethics of Cyber Conflict. *Ethics and Policies for Cyber Operations. Philosophical Studies Series.* 2019. Vol. 124. P. 1–16.
4. Taillat S. Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. *Contemporary Security Policy*. 2019. №40 (3). P. 368–381.
5. Leuprecht C., Szeman J., Skillicorn D. The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary security policy*. 2019. №40 (3). P. 382–407.
6. Shandler R., Canetti D. Introduction: Cyber-conflict – Moving from speculation to investigation. *Journal of Peace Research.* 2024. №61 (1). P. 3–9. doi: https://journals.sagepub.com/doi/10.1177/00223433231219441.
7. Kallberg J., Cook T. The Unfitness of Traditional Military Thinking in Cyber. *IEEE ACCESS*. 2017. №5. P. 8126–8130.
8. Dong J., Chen S., Ding F., Zhuo J., Hao M. Spatiotemporal characteristics and drivers of global cyber conflicts. *Humanit Soc Sci Commun.* 2025. №12. URL: https://www.nature.com/articles/s41599-025-04897-7 (дата звернення: 18.07.2025).
9. Liebetrau T. Cyber conflict short of war: a European strategic vacuum. *European Security.* 2022. №31 (4). P. 497–516. URL: https://www.tandfonline.com/doi/citedby/10.1080/09662839.2022.2031991?scroll=top&needAccess=true (дата звернення: 19.07.2025).
10. Brown J., Fazal T. "SorryNotSorry": Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security.* 2021. №6 (4). P. 401–417.
11. Giles K., Hartmann K. «Silent Battle" Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. *11th Annual International Conference on Cyber Conflict (CyCon) – Silent Battle.* Proceeding's 11Th international conference on cyber conflict (CyCon) – Silent Battle. Tallinn, 2019. P. 23–25.
12. Hartmann K., Giles K. The Next Generation of Cyber-Enabled Information Warfare. *12th International Conference on Cyber Conflict (CyCon)*. 2020. P. 233–250.
13. Hoisington M. Regulating Cyber Operations Through International Law: In, Out or Against the Box? *Ethics and Policies for Cyber Operations. Philosophical Studies Series.* 2017. Vol. 124. P. 87–98.
14. Macák K. From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law. *9th International Conference*

*on Cyber Conflict -Defending the Core (CyCon)*. Proceeding's 9th International conference on cyber conflict: defending the core (CyCon). Tallinn, 2017. P. 135–148.
15. Haataja S. Cyber operations and automatic hack backs under international law on necessity. *Computer law & security review*. 2024. № 53. URL: https://www.sciencedirect.com/science/article/pii/S0267364924000591?via%3Dihub (дата звернення: 20.07.2025).
16. Sohail H. Fault Lines In The Application Of International Humanitarian Law To Cyberwarfare. *Journal of digital forensics security and law*. 2022. № 17 (1). URL: https://commons.erau.edu/jdfsl/vol17/iss1/8 (дата звернення: 20.07.2025).
17. Leggat H. Cyber Warfare: An Enquiry Into the Applicability of National Law to Cyberspace. *17th Australian Cyber Warfare Conference (CWAR).* Proceeding's 17th Australian Cyber Warfare Conference (CWAR). Tallinn, 2020. P. 28–46.
18. Cho Y., Chung J. Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity. *Pacific focus*. 2017. № 32 (2). P. 290–314.
19. Osawa J. The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review*. 2017. № 24 (2). P. 113–131.
20. Kello L. Cyber legalism: why it fails and what to do about it. *Journal of Cybersecurity. 2021.* Vol. 7 (1).URL: https://academic.oup.com/cybersecurity/article/7/1/tyab014/6343244?login=false (дата звернення: 21.07.2025).

## REFERENCES

1. Kushwaha, N., Giles, K., Singer, T., Watson, B. (2021). Cyber Personhood. *13th International Conference on Cyber Conflict (CyCon) – Going Vira:* proceeding's 13th International Conference on Cyber Conflict (CyCon) – Going Viral. Tallinn, *275–289.*
2. Lorents, P., Ottis, R. (2010). Knowledge based framework for cyber weapons and conflict. *International Conference on Cyber Conflict:* proceeding's International Conference on cyber conflict. Tallin, *129–142.*
3. Cornish, P. (2019). Deterrence and the Ethics of Cyber Conflict. *Ethics and Policies for Cyber Operations. Philosophical Studies Series, 124, 1–16.*
4. Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. *Contemporary Security Policy*, *40(3), 368–381.*
5. Leuprecht, C., Szeman, J., Skillicorn, D. (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary security policy*, *40(3), 382–407.*
6. Shandler, R., Canetti, D. (2024). Introduction: Cyber-conflict – Moving from speculation to investigation. *Journal of Peace Research, 61(1), 3–9.* doi: https://journals.sagepub.com/doi/10.1177/00223433231219441
7. Kallberg, J., Cook, T. (2017). The Unfitness of Traditional Military Thinking in Cyber. *IEEE ACCESS*, *5, 8126–8130.*

8. Dong, J., Chen, S., Ding, F., Zhuo, J., Hao, M. (2025). Spatiotemporal characteristics and drivers of global cyber conflicts. *Humanit Soc Sci Commun, 12.* URL: https://www.nature.com/articles/s41599-025-04897-7
9. Liebetrau, T. (2022). Cyber conflict short of war: a European strategic vacuum. European Security, *31 (4), 497–516.* URL: https://www.tandfonline.com/doi/citedby/10.1080/09662839.2022.2031991?scroll=top&needAccess=true
10. Brown, J., Fazal, T. (2021). "SorryNotSorry": Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security, 6(4), 401–417.*
11. Giles, K., Hartmann, K. (2019). "Silent Battle" Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. *11th Annual International Conference on Cyber Conflict (CyCon) – Silent Battle:* proceeding's 11Th international conference on cyber conflict (CyCon) – Silent Battle. Tallinn, *23–25.*
12. Hartmann, K., Giles, K. (2020). The Next Generation of Cyber-Enabled Information Warfare. *12th International Conference on Cyber Conflict (CyCon)*, *233–250.*
13. Hoisington, M. (2017). Regulating Cyber Operations Through International Law: In, Out or Against the Box? *Ethics and Policies for Cyber Operations. Philosophical Studies Series, 124, 87–98.*
14. Macák, K. (2017). From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law. *9th International Conference on Cyber Conflict – Defending the Core (CyCon):* proceeding's 9th International conference on cyber conflict: defending the core (CyCon). Tallinn, *135–148.*
15. Haataja, S. (2024). Cyber operations and automatic hack backs under international law on necessity. *Computer law & security review*, *53*. URL: https://www.sciencedirect.com/science/article/pii/S0267364924000591?via%3Dihub
16. Sohail, H. (2022). Fault Lines In The Application Of International Humanitarian Law To Cyberwarfare. *Journal of digital forensics security and law*, *17 (1)*. URL: https://commons.erau.edu/jdfsl/vol17/iss1/8
17. Leggat, H. (2020). Cyber Warfare: An Enquiry Into the Applicability of National Law to Cyberspace. *17th Australian Cyber Warfare Conference (CWAR);* proceeding's 17th Australian Cyber Warfare Conference (CWAR). Tallinn, *28–46.*
18. Cho, Y., Chung, J. (2017). Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity. *Pacific focus, 32(2), 290–314*.
19. Osawa, J. (2017). The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review*, *24(2), 113–131*.
20. Kello, L. (2021). Cyber legalism: why it fails and what to do about it. *Journal of Cybersecurity, 7(1).*URL: https://academic.oup.com/cybersecurity/article/7/1/tyab014/6343244?login=false

***Trofymenko Volodymyr Anatoliovych***, candidate of Legal Sciences,
Assistant Professor, Department of Philosophy,
Yaroslav Mudryi National Law University,
Kharkiv, Ukraine

# CYBERCONFLICT AND THE LEGAL FIELD OF ITS EXISTENCE: AN ATTEMPT AT PHILOSOPHICAL AND LEGAL UNDERSTANDING

*The publication is devoted to cyber conflict and the legal field of its existence. It is emphasized that the main scientific problem is the lack of a unified understanding of cyber conflict and its characteristic features. In turn, this creates a certain problem of creating a legal field of its existence. The main reason for this is the specificity of cyber conflict. Thus, it is shown that the problem of the legal field of cyber conflict remains open and requires an urgent solution.*

***Keywords:*** *cyber conflict, cyberspace, international law, international humanitarian law, cyber legalism.*