УДК 341.7
DOI https://doi.org/10.24144/2788-6018.2025.02.180

# КІБЕРПРОСТІР: МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ТА ПРАКТИКА ЗАСТОСУВАННЯ ПРЕЦЕДЕНТНОГО ПРАВА МС ООН

**Карвацька С.Б.,**
*доктор юридичних наук, професор,*
*в.о. завідувача кафедри міжнародного права*
*та порівняльного правознавства*
*Чернівецького національного університету імені Юрія Федьковича*
*ORCID: 0000-0001-9948-4866*

**Маник А.З.,**
*кандидат юридичних наук,*
*асистент кафедри міжнародного права*
*та порівняльного правознавства*
*Чернівецького національного університету імені Юрія Федьковича*
*ORCID: 0009-0005-5667-391*

**Яремчук В.В.,**
*доктор філософії,*
*асистент кафедри міжнародного права*
*та порівняльного правознавства*
*Чернівецького національного університету імені Юрія Федьковича*
*ORCID: 0000-0001-7787-8880*

**Карвацька С.Б., Маник А.З., Яремчук В.В. Кіберпростір: міжнародно-правове регулювання та практика застосування прецедентного права МС ООН.**

Стаття присвячена дослідженню міжнародно-правового регулювання кіберпростору та практики застосування прецедентного права МС ООН (далі – Міжнародний суд ООН) до кібератак. Проаналізовано, що норми міжнародного права є важливою основою міжнародного правопорядку у кіберпросторі, оскільки 1) у ньому складаються відносини, які потребують міжнародно-правового регулювання; 2) зловживання інформаційними технологіями створює значні загрози не лише для окремих осіб, а й для держав і міжнародної спільноти загалом. Важливе значення для урегулювання відносин у кіберпросторі має принцип рівноправності та самовизначення народів: ніхто не може втручатися в інформаційні системи. Доведено, що наразі, офіційне міжнародно-правове визнання інформаційних атак агресією чи інших кіберзасобів зброєю, відсутнє, тож кваліфікація застосування кіберзброї як порушення принципу незастосування сили є проблематичною.

Установлено, що незважаючи на те, що міжнародне право не містить чітких критеріїв щодо застосування стандарту збройного нападу, важливим є аналіз того, якою мірою кібератаки можуть бути кваліфіковані як збройний напад. Кібератаки, які підривають або знищують основні активи безпеки, і належать до найвищої категорії, можуть кваліфікуватися як збройний напад. Доведено, що розслідування кібератак між державами ускладнюється відсутністю у міжнародному праві єдиного зводу правил щодо надання доказів. І хоча немає єдиного стандарту доказування, застосовного до всіх справ, пов'язаних з міжнародною відповідальністю за кібероперації – заяви про самозахист від кібероперацій повинні бути доведені за допомогою переконливих доказів. Зазначено, що при розгляді справ про кібератаки МС ООН надає більшої доказової ваги офіційним документам держав та міжнародних організацій. До формування висновків МС ООН підходить з обережністю: якщо стороні у справі об'єктивно важко виконати обов'язок доказування, оскільки прямі докази знаходяться під територіальним контролем іншої сторони, включаючи її кіберінфраструктуру, допустимим є більш ліберальне використання висновків щодо фактів, за умови, якщо вони не залишають місця для сумнівів.

**Ключові слова:** кіберпростір, кібербезпека, міжнародно-правове урегулювання відносин у кібепросторі, застосування принципів міжнародного права до відносин у кіберпросторі, кіберконфлікти, кібератаки, кібердокази, міжнародно-правового захисту держав від застосування кіберзброї, Міжнародний суд ООН.

**Karvatska S.B., Manyk A.Z., Yaremchuk V.V. Cyberspace: international legal regulation and practice of application of the case law of the UN ICJ.**

The article is devoted to the study of international legal regulation of cyberspace and the practice of applying the case law of the International Court of Justice to cyberattacks. The author analyses that the rules of international law are an important basis for the international legal order in cyberspace, since 1) it is the place where relations requiring international legal regulation are established; 2) misuse of information technologies poses significant threats not only to individuals, but also to States and the international community as a whole. The principle of equality and self-determination of peoples is important for the regulation of relations in cyberspace: no one can interfere with information systems. It is proved that currently, there is no official international legal recognition of information attacks as aggression or other cyber tools as weapons, so the qualification of the use of cyber weapons as a violation of the principle of non-use of force is problematic.

It is established that despite the fact that international law does not contain clear criteria for applying the armed attack standard, it is important to analyse to what extent cyber attacks can be qualified as an armed attack. Cyberattacks that undermine or destroy essential security assets and belong to the highest category may qualify as an armed attack. It is proved that the investigation of cyberattacks between states is complicated by the lack of a single set of rules in international law on the provision of evidence. Although there is no single standard of proof applicable to all cases involving international liability for cyber operations, claims of self-defence against cyber operations must be proved by convincing evidence. It is noted that in considering cases of cyber-attacks, the ICJ gives greater evidentiary weight to official documents of States and international organisations. The ICJ is cautious in formulating its conclusions: if it is objectively difficult for a party to the case to meet the burden of proof because direct evidence is under the territorial control of the other party, including its cyber infrastructure, a more liberal use of findings of fact is permissible, provided that they leave no room for doubt.

**Key words:** cyberspace, cybersecurity, international legal regulation of relations in cyberspace, application of the principles of international law to relations in cyberspace, cyber conflicts, cyber attacks, cyber evidence, international legal protection of states from the use of cyber weapons, International Court of Justice.

**Постановка проблеми.** Кіберпростір відповідно до Підсумкової Декларації 42-саміту G 7 від 26-27 травня 2016 року визначається як «доступне, відкрите, взаємопов'язане, надійне та безпечне середовище» [1]. Власне з появою кіберпростору розпочинається науково-практична дискусія про міжнародно-правове урегулювання відносин у кібепросторі, дослідження застосування принципів міжнародного права до цього процесу, аналіз проблемних питань міжнародно-правового визнання інформаційних атак агресією та аналіз практики розслідування Міжнародним Судом ООН кібератак між державами. Відповідно до Міжнародної Стратегії співробітництва у кіберпросторі, «міжнародне співтовариство має дотримуватися цілей та принципів, закріплених у Статуті ООН, зокрема, незастосування сили та мирного урегулювання спорів, з метою забезпечення миру та безпеки у кіберпросторі. Всі країни повинні протидіяти ворожості та агресії, запобігати нарощуванню озброєнь та конфліктам у кіберпросторі та врегульовувати спори мирним шляхом» [2]. Національний координаційний центр кібербезпеки «вивчає міжнародний досвід щодо застосування міжнародного гуманітарного права до проведення кібероперацій» [3].

**Аналіз останніх досліджень і публікацій**. Проблематику міжнародно-правового урегулювання кіберпростору досліджували такі вітчизняні науковці як І.М. Забара (аналіз правового регулювання міждержавного обміну інформацією), А.В. Пазюк (дисертаційна робота присвячена теоретико-практичним аспектам міжнародно-правово регулювання інформаційної сфери, М.О. Яцишин (використання сили у кіберпросторі у рамках міжнародного права). Варті уваги нові дослідження іноземних науковців таких як Крістофер Уайт, Брайан Мазанець (Whyte Christopher and Brian Mazanec) Майкла Н. Шмітта (Michael N. Schmitt) Марко Роскіні (Roscini Marco) щодо розуміння політики і стратегії кібервійни та доказів у міжнародних спорах, пов'язаних з відповідальністю держав за кібероперації.

**Метою дослідження** є дослідження міжнародно-правового регулювання кіберпростору та практики застосування прецедентного права МС ООН до кібератак.

**Виклад основного матеріалу.** Будь-які пропагандистські дії, спрямовані на викривлення реальності та впливу на самовизначення певної спільноти, є неправомірними. Разом з тим, через неможливість застосовувати «класичну зброю» у кіберпросторі, специфіку має принцип незастосування сили чи погрози силою. У своєму Дорадчому висновку про законність використання ядерної зброї (1996) МС ООН визначає, що ст. 2, 4, 51 і 42 Статуту ООН «не стосуються конкретної зброї

– вони застосовуються до будь-якого застосування сили, незалежно від зброї, що використовується» [4].

«Норми сучасного міжнародного права, як відзначає М. Яцишин, зокрема, основні принципи міжнародного права є чинними і для кіберпростору, і це означає заборону здійснювати акти агресії у кіберпросторі на підставі принципів суверенної рівності держав, незастосування сили і погрози силою, невтручання у внутрішні справи» [5]. Водночас, авторка справедливо зауважує, що очевидною є неузгодженість у формальному консенсусі держав та доктринальна невизначеність з вказаного питання кваліфікації кібервійни за міжнародним правом залишає його відкритим для наукової дискусії. Відсутність міжнародно-правового визнання інформаційних атак агресією ставить під сумнів можливість міжнародно-правового захисту держав від застосування кіберзброї іншими державами чи приватними особами, але за сприяння державних структур. Також варто зауважити, що визначення власне організатора кібератаки теж є доволі складним процесом.

Хоча стаття 51 Статуту ООН вказує на те, що «збройний напад» може спричинити невід'ємне право держави на індивідуальну або колективну самооборону. Для вдосконалення поняття самооборони та сприяння *jus ad bellum* міжнародному праву щодо застосування транснаціональної сили необхідно більше роз'яснень щодо того, що є збройним нападом у кіберпросторі [6]. Поріг збройного нападу, коли він застосовується в кіберпросторі, може бути використаний у процесах прийняття політичних рішень державами, які розглядають можливість ініціювання кібератаки [7]. Розуміння параметрів порогу збройного нападу у кіберпросторі допоможе державам-жертвам у процесі прийняття рішень у відповідь на кібератаки: якщо поріг збройного нападу буде досягнутий, це дасть державі-жертві правову базу у міжнародному праві для застосування транснаціональної сили, тобто самооборони [8].

Незважаючи на те, що міжнародне право не містить чітких критеріїв щодо застосування стандарту збройного нападу, при аналізі того, якою мірою кібератаки можуть бути кваліфіковані як збройний напад, інші джерела можуть надати додаткові вказівки. На запрошення Центру передового досвіду з кіберзахисту НАТО Міжнародна група експертів розробила Талліннський механізм (міжнародний формат підтримки стійкості цивільної інфраструктури України перед кіберзагрозами, учасниками якого є 11 країн [9]), який охоплює норми щодо застосування міжнародного права до «кібероперацій» [10]. Щодо збройних нападів, експерти погодилися з тим, що окремі кібероперації «достатньо серйозні», щоби кваліфікуватися як збройний напад, що відповідає консультативному висновку МС ООН щодо ядерної зброї, у якому стверджується, що «вибір засобів нападу не має значення для питання про те, чи кваліфікується операція як збройний напад» [11]. І хоча, чинне міжнародне право надає мало відчутних критеріїв для оцінки масштабу та наслідків, тим не менш, Міжнародна група експертів погодилася з тим, що «кібероперація, у результаті якої серйозно поранено, або вбито багато людей, або завдано значної шкоди чи знищено майно», досягає порогу збройного нападу [12].

Крім того, існують деякі особливі позиції окремих держав. До прикладу, Великобританія заявляє, що «якщо ворожа держава втручається в роботу одного з наших ядерних реакторів, що призводить до масової загибелі людей, то цей акт-кібероперація, може розглядатися як незаконне застосування сили або збройний напад», а також «такі дії, як націленість на основні медіа-сервіси, є забороненими втручаннями або навіть збройними нападами, коли вони здійснюються за допомогою кіберзасобів» [13]. У Франції кібератака може бути кваліфікована як збройний напад, якщо вона спричиняє «значні людські жертви або значну фізичну чи економічну шкоду», тобто, якщо операція у кіберпросторі «призвела до виходу з ладу критично важливої інфраструктури зі значними наслідками або наслідками, здатними паралізувати цілі сфери діяльності країни, спричинити технологічні або екологічні катастрофи та призвести до численних жертв» [14, 8]). У правовому висновку Нідерландів («Лист до парламенту щодо міжнародного правопорядку в кіберпросторі») зазначено, що кваліфікація кібератаки як збройного нападу «залежить від масштабу і наслідків відповідного інциденту», а також, що «кібератака повинна мати транскордонний характер, щоб її можна було кваліфікувати як збройний напад» [15, 8-9].

Американські дослідники – Крістофер Уайт (доктор філософії з програми безпеки та готовності до надзвичайних ситуацій Університету Співдружності штату Вірджинія (США) та Брайан Мазанець (доктор філософії з міжнародної безпеки, ад'юнкт-професор в Університеті Джорджа Мейсона та Університеті штату Міссурі (США) наголошуютть, що «через великі масштаби, в яких відбувається сучасне «кібершпигунство», яке також називають витоком інформації, цей перший тип став справжнім занепокоєнням і своєрідним вторгненням, яке занадто тривожне і занадто велике, щоб його ігнорувати» [16]. Показовим прикладом є «інформація про креслення винищувача F-35, яка, згідно з витоками Сноудена, була серед більш ніж 50 ТБ інформації, яку Китай викрав у уряду Сполучених Штатів Америки (США) в ході багаторічної операції з викрадення» [17, 120].

Загалом, кібератаки щодо держав розділяють на три типи: «кібершпигунство», «маніпулювання інформаційним середовищем» і «знищення основних активів безпеки» [17,100-101]. Кібершпигунство фахівці пропонують розглядати розвідувальну або контррозвідувальну операцію [18,287-288] як збройний напад. Використання соціальних мереж для масового впливу на окремих виборців продемонструвало, що сучасні технології можуть маніпулювати інформаційним середовищем і завдавати шкоди демократичній цілісності західних країн [19]. Третій тип стосується «підриву, деградації або знищення основних засобів безпеки» – кібератака, спрямована на об'єкти критичної інфраструктури, у тому числі на атомну електростанцію, або на станцію управління дамбою, може підпадати під цю категорію [20, 444].

Франція та Велика Британія розробили систему класифікації кібератак, у якій визначено, зокрема, Рівень 5: Надзвичайна ситуація – який може бути кваліфікований як збройний напад відповідно до статті 51 Статуту ООН. Міністерство юстиції та безпеки Нідерландів визначило категорію А (найвищий рівень) кібератак щодоовні активи безпеки», які можуть бути порушені, погіршені або знищені кібератаками, можна згрупувати в такі категорії, як виробництво, зберігання і переробка ядерних матеріалів, виробництво, розподіл і транспортування електроенергії, газу і нафти, Інтернет, аероуправління, великомасштабне виробництво/переробка та/або зберігання (нафто) хімічних речовин, фінансові системи, мережі зв'язку, а також військовий потенціал (що унеможливлює розгортання збройних сил) [21]. Виходячи з того, що кібератаки підривають, погіршують або знищують основні активи безпеки, а також що кібератаки, які належать до найвищої (надзвичайної) категорії, можуть (потенційно) кваліфікуватися як збройний напад.

Проблеми з доказовою базою в міждержавних судових процесах, зокрема, у зв'язку з кваліфікацією відповідної протиправної поведінки, не є специфічними для кібероперацій. Задовго до настання «кібернетичної ери» МС ООН у рішенні у справі Нікарагуа проти США (1986) визнав, що «проблема полягає не в юридичному процесі приписування діяння конкретній державі, а в попередньому процесі відстеження матеріальних доказів, що підтверджують особу порушника» [22]. Розслідування кібератак між державами ускладнюється відсутністю у міжнародному праві єдиного зводу правил щодо надання доказів. Що стосується подання доказів у міждержавних судових процесах, то некримінальні міжнародні суди визначають свої власні стандарти у кожному конкретному випадку. МС ООН є головним судовим органом ООН, який розглядає, якщо залучені у судовий процес держави визнали ійого юрисдикцію, позови про відповідальність держав, що випливають із порушення норми міжнародного права [23].

Постає питання про те, щоби установити, чи можна визначити правила доказування, які б застосовувалися до позовів у міждержавних судових провадженнях, спрямованих на відшкодування шкоди, завданої кіберзлочинами. Слід, однак, зазначити, що висновки, зроблені МС ООН, стосуються лише його діяльності, і не можуть бути автоматично поширені на інші міжнародні суди. Правила надання доказів у МС ООН містяться у його Статуті та Регламенті. Одним із доречних прикладів може слугувати рішення МС ООН у справі між Східним Тимором і Австралією (2014). Східний Тимор стверджував, що Австралія направила своїх агентів у офіс австралійського адвоката, який виступав юридичним радником у Східному Тіморі для збору конфіденційної інформації, що стосується судових процесів між двома державами. Цей офіс був фізично розташований в Австралії. Східний Тимор звернувся до МС ООН, заявивши, що «Австралія, захопивши документи та дані, порушила суверенітет Східного Тимора», і що «Австралія повинна негайно повернути до призначеного представника Східного Тимора всі вищезазначені документи, а також знищити кожну копію таких документів, що знаходяться у володінні, або контролі Австралії» [24]. Вирішуючи справу, МС ООН зазначив, що «на цьому етапі розгляду справи потрібно лише вирішувати, чи дійсні права, на які претендує Східний Тимор у позові, та для яких він вимагає захист». МС ООН визнав права Східного Тимору «дійсними» і видав тимчасову постанову про те, що «Австралія не повинна жодним чином втручатися у зв'язки між Східним Тимором та його юридичними радниками» [24].

Аналізуючи практику застосування до кібероперацій правил та прецедентного права МС ООН щодо доказів Марко Роскіні (професор міжнародного права у Вестмінстерській школі права, науковий співробітник Центру передового досвіду НАТО з питань кіберзахисту (CCDCOE)) робить важливі зауваження. По-перше, тягар доказування не зміщується в кіберконтексті і продовжує лежати на стороні, яка стверджує певний факт. По-друге, хоча немає упевненості в тому, що можна визначити як єдиний стандарт доказування, що є застосовним до всіх справ, пов'язаних з міжнародною відповідальністю за кібероперації, видається, що заяви про самозахист від кібероперацій, повинні бути доведені за допомогою чітких і переконливих доказів. З іншого боку, для доведення того, що сторона у судовому процесі проводила кібероперації, які є міжнародними злочинами, необхідні переконливі докази [25, 272]. По-третє, МС ООН може взяти до офіційного відома відмову сторони надати засекречені кібердокументи, але може утриматися від того, щоби робити негативні висно-

вки з факту ненадання документів. По-четверте, МС ООН надає більшої доказової ваги офіційним документам держав та міжнародних організацій, таких як ООН. Інші документи, як-то, Звіти НУО та наукові чи публіцистичні статті про кіберінциденти є лише вторинними джерелами доказів, які можуть бути корисними для підтвердження інших джерел або для встановлення обізнаності громадськості з певними фактами, за умови, що вони є достатньо ретельними і лише тоді, коли вони «повністю узгоджуються між собою щодо основних фактів та обставин справи» [25, 272]. По-п'яте, до формування висновків МС ООН підходить з великою обережністю: якщо стороні у справі об'єктивно важко виконати обов'язок доказування, оскільки прямі докази знаходяться під виключним територіальним контролем іншої сторони, включаючи її кіберінфраструктуру, допустимим є більш ліберальне використання висновків щодо фактів за умови, якщо вони не залишають місця для обґрунтованих сумнівів. По-шосте, навіть якщо сторона у судовому процесі отримує докази незаконно, наприклад, шляхом несанкціонованого втручання у комп'ютерні системи іншої держави, отримані таким чином докази можуть бути взяті до уваги МС ООН, хоча мета збору доказів не виключає незаконності такої поведінки [25, 273].

**Висновки.** Норми міжнародного права є важливою основою міжнародного правопорядку у кіберпросторі, оскільки 1) у ньому складаються відносини, які потребують міжнародно-правового регулювання; 2) зловживання інтернетом та інформаційними технологіями створює значні ризики та загрози не лише для окремих осіб, а й для держав і міжнародної спільноти загалом. Важливе значення для урегулювання відносин у кіберпросторі має принцип рівноправності та самовизначення народів: ніхто не може втручатися в інформаційні системи чи здійснювати пропаганду. Наразі, офіційне міжнародно-правове визнання інформаційних атак агресією чи інших кіберзасобів зброєю, відсутнє, тож кваліфікація застосування кіберзброї як порушення принципу незастосування сили є досить проблематичною.

Незважаючи на те, що міжнародне право не містить чітких критеріїв щодо застосування стандарту збройного нападу, при аналізі того, якою мірою кібератаки можуть бути кваліфіковані як збройний напад, інші джерела можуть надати додаткові вказівки. Так як кібератаки підривають, погіршують або знищують основні активи безпеки, а також що кібератаки, які належать до найвищої (надзвичайної) категорії, можуть (потенційно) кваліфікуватися як збройний напад. Разом з тим, розслідування кібератак між державами ускладнюється відсутністю у міжнародному праві єдиного зводу правил щодо надання доказів. І хоча немає упевненості у тому, що можна визначити як єдиний стандарт доказування, застосовним до всіх справ, пов'язаних з міжнародною відповідальністю за кібероперації, видається, що заяви про самозахист від кібероперацій, повинні бути доведені за допомогою чітких і переконливих доказів.

При розгляді справ кібератаки МС ООН надає більшої доказової ваги офіційним документам держав та міжнародних організацій. До формування висновків МС ООН підходить з великою обережністю: якщо стороні у справі об'єктивно важко виконати обов'язок доказування, оскільки прямі докази знаходяться під виключним територіальним контролем іншої сторони, включаючи її кіберінфраструктуру, допустимим є більш ліберальне використання висновків щодо фактів за умови, якщо вони не залишають місця для обґрунтованих сумнівів.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**


1. G7 Ise-Shima Leaders' Declaration G7 Ise-Shima Summit, 26-27 May 2016: http://www.mofa.go.jp/files/000160266.pdf; G7 Principles and Actions on Cyber. Ise-Shima, Japan, May 27, 2016. URL: http://www.g8.utoronto.ca/summit/2016shima/cyber.html.
2. International Strategy of Cooperation on Cyberspace. 2017. URL: http://www.chinadaily.com.cn/opinion/201703/02/content_28401127.ht.
3. Рада національної безпеки і оборони України. Річний аналітичний огляд. 2023-2024 роки. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf.
4. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996. URL: http://www.icj-cij.org/files/caserelated/95/095-19960708-ADV-01-00-EN.pdf.
5. Яцишин М.Ю. Використання сили у кіберпросторі в рамках міжнародного права. *Інформація і право*. 2018. № 4(27). С. 22–32.
6. Schmitt Michael N. Taming the Lawless Void: Tracking the Evolution of International Law. *Texas National Security Review.* 2020. N 3 (3). P. 32–47.
7. Mačák Kubo. From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers. *Leiden Journal of International Law*. 2017. N 30 (4). P 877–899. doi:10.1017/S0922156517000358.
8. Gill Terry D. Legal Basis of the Right of Self-Defence under the UN Charter and under Customary International Law. In The Handbook of the International Law of Military Operations, edited by Terry D. Gill and Dieter Fleck, 2015. P. 213–224. Oxford: Oxford University Press.

9. МЗС України. Рік роботи Талліннського Механізму: 200 мільйонів євро для кіберзахисту цивільної інфраструктури України. 20 грудня 2024 року. URL: https://mfa.gov.ua/news/rik-roboti-tallinskogo-mehanizmu-200-miljoniv-yevro-dlya-kiberzahistu-civilnoyi-infrastrukturi-ukrayini.
10. Oorsprong F., Ducheine P., & Pijpers P. Cyber-attacks and the right of self-defense: a case study of the Netherlands. *Policy Design and Practice*. 2023. N 6/2. P. 217–239.
11. ICJ. Case concerning the Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion). ICJ Reports. 1996.
12. Schmitt Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge Cambridge University Press. 2017.
13. Attorney General's Office. Speech: Cyber and International Law in the 21st Century. 2018. May 23. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
14. Ministère des Armées. International Law Applied To Operations In Cyberspace. République Française, 2019. September 9. URL: https://www.defense.gouv.fr/content/ download/567648/9770527/ file/international+law+applied+to+operations+in+cyberspace.pdf.
15. Minister of Foreign Affairs. Letter to the Parliament on the International Legal Order in Cyberspace. Government of the Netherlands, 2019. July 5. URL: https://www.government.nl/ documents/ parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.
16. Maurer Tim. Cyber Mercenaries: The State, Hackers and Power. Cambridge: Cambridge University Press. 2018.
17. Whyte Christopher and Brian Mazanec. Understanding Cyber Warfare: Politics, Policy and Strategy. London; New York, NY: Routledge Taylor & Francis Group. 2019.
18. Ducheine P.A.L., and B.M.J. Pijpers. The Notion of Cyber Operations. *In Research Handbook on International Law and Cyberspace*, 2nd ed., Cheltenham: Edward Elgar Publishing. 2021. P. 271–295.
19. Pijpers B.M.J. Influence Operations in Cyberspace: On the Applicability of Public International Law during Influencing Operations in a Situation below the Threshold of the Use of Force. PhD thesis, University of Amsterdam. 2022.
20. Gill Terry D., and Paul A.L. Ducheine. Anticipatory Self-Defense in the Cyber Context. *International Law Studies*. 2013. N 89: 438–471.
21. Nationaal Coördinator Terrorismebestrijding en Veiligheid. Overzicht Vitale Processen. Ministerie van Justitie en Veiligheid. 2020. URL: https://www.nctv.nl/ onderwerpen/vitale-infrastructuur/ overzicht-vitale-processen.
22. I.C.J. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986. 14, para. 57 (June 27).
23. Clemons H. Vern. The Ethos of the International Court of Justice is Dependent Upon the Statutory Authority Attributed to its Rhetoric: A Metadiscourse, *Fordham INT'L L.J.* 1997.N 20. P. 1479, 1486, 1490–91.
24. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia). URL: http://www.icj-cij.org/en/case/156.
25. Roscini Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal.* Vol. 50, p. 233, 2015. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2611753.