УДК 341.1
DOI https://doi.org/10.32782/2524-0374/2021-9/81

ЗАХИСТ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ В КОНТЕКСТІ МІЖНАРОДНОГО МИРУ ТА БЕЗПЕКИ

PROTECTION OF CRITICALLY IMPORTANT INFRASTRUCTURE FACILITIES IN THE CONTEXT OF INTERNATIONAL PEACE AND SECURITY

Громовенко К.В., доктор юридичних наук,
професор кафедри міжнародного та порівняльного правознавства
Міжнародного гуманітарного університету

У статті розглядається діяльність Групи урядових експертів щодо заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки, а також зміст прийнятих нею норм, що увійшли до тексту Резолюції Генеральної Асамблеї ООН A/76/135 від 14 липня 2021 року. З урахуванням того, що доповіді Групи урядових експертів приймаються Генеральною Асамблею, вони мають нормативний вплив на практику та позицію держав щодо застосування норм міжнародного права в кіберпросторі. Водночас низка норм доповіді 2021 року безпосередньо стосується критичної інфраструктури держав, яка часто стає об'єктом нападу з боку державних і недержавних акторів.

На підставі аналізу даних норм робиться висновок про важливі кроки та новації, запропоновані Групою урядових експертів задля захисту критично важливих об'єктів держави та інформаційно-комунікаційних технологій (ІКТ) від зловмисної діяльності в кіберпросторі. В статті встановлено, що попри спеціальний характер розроблені норми є відображенням норм та принципів міжнародного права, закріплених в Статуті Організації Об'єднаних Націй, що полегшує процес формування і застосування звичаєвих норм в кіберпросторі.

Проаналізовано два паралельні процеси вироблення норм відповідальної поведінки в кіберпросторі – в рамках Групи урядових експертів та Відкритої робочої групи, які входять до Першого комітету Генеральної Асамблеї ООН. В статті встановлено, що робота Відкритої робочої групи відкриває нові горизонти для залучення зацікавлених сторін, але Група урядових експертів є більш традиційним механізмом і наразі, в силу важливих висновків, представлених в доповідях 2013, 2015 та 2021 років, заслуговує на особливу увагу.

Серед основних висновків даної статті – важливість розробки норм відповідальної поведінки держав в кіберпросторі. Лише досягнення цієї цілі сприятиме формуванню розуміння у держав щодо того, як потрібно діяти у випадку коли їх об'єкти важливої критичної інфраструктури стали об'єктом нападу або коли їх інфраструктура використовується в зловмисній ІКТ-діяльності проти інфраструктури інших держав. В подальшому таке розуміння дозволить не тільки сформувати звичаєві норми міжнародного права стосовно ІКТ та їх використання, а й розробити юридично обов'язкові, кристалізовані в міжнародному інструменті, зобов'язання.

Ключові слова: інформаційно-комунікаційні технології, ІКТ, відповідальна поведінка в кіберпросторі, об'єкти критичної інфраструктури, Група урядових експертів.

The article examines the activity of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, as well as the content of the norms adopted by them and thereafter included in the UN General Assembly Resolution A/76/135 dated on 14 July 2021. Although reports of the Group of Governmental Experts are adopted by the General Assembly, they do have normative impact on the practice of states and their position on the application of international law in cyberspace, despite the lack of legally binding force.

Based on the analysis of these norms, article concludes about the important steps and innovations proposed by the Group of Governmental Experts to protect information and communication technologies (ICT) from malicious activity and their use against critical objects of the state. Despite these rules are voluntary and non-binding, they reflect the norms and principles of international law enshrined in the Charter of the United Nations, and they are important for the formation of customary rules in the cyber domain.

The article also establishes the existence of two parallel processes within the First Committee of the UN General Assembly. The existence and work of the Open-Ended Working Group opens new horizons for stakeholder engagement, but the Group of Governmental Experts is a more traditional mechanism and for now, due to the important findings presented in the 2013, 2015 and 2021 reports, merits special consideration.

Finally, among the main conclusions of this article is the importance of developing norms of responsible behavior in cyberspace. This fosters countries` understanding of what to do when their critically important infrastructure is attacked or their infrastructure is used in malicious ICT activities against other countries` infrastructure. Thus, in the future, this understanding will contribute not only to the formation of customary rules of international law on ICT and their use, but also to the development of legally binding, crystallized in the international treaties, obligations.

Key words: information and communication technologies, ICT, responsible behavior in cyberspace, critical infrastructure, Group of Governmental Experts.

Об'єкти критичної інфраструктури завжди відігравали ключову роль в забезпеченні добробуту населення та безпеки держави. Історія свідчить про те, що розуміння важливості таких об'єктів сформувалося задовго до самого поняття. Ще за часів античності спартанський полководець Лісандр зупинив функціонування транспортного сполучення через Геллеспонт (Дарданелли), щоб спровокувати голод серед населення Стародавньої Греції та без супротиву захопити їх. Яскравим прикладом цілеспрямованих атак проти об'єктів критичної інфраструктури також є Директива Касабланки, що вимагала від командирів повітряних сил США та Великої Британії здійснювати атаки по об'єктам військової, промислової та економічної систем Третього Рейху під час Другої світової війни [1, с. xvi].

З появою та швидким розвитком інформаційно-комунікаційних технологій загроз стало ще більше, а напади проти них вийшли на новий рівень. В першу чергу, мова йде про кібероперації проти об'єктів критичної інфраструктури, але це лише один із прикладів того, як ІКТ можуть застосовуватись проти критично важливих об'єктів держави. Така зловмисна діяльність в кіберпросторі створює ряд загроз, зокрема для забезпечення міжнародного миру, безпеки та стабільності, та потребує уваги міжнародної спільноти.

Вперше питання щодо «інформаційної безпеки» на міжнародну рівні підняла Російська Федерація, за ініціативи якої у 1998 році була прийнята Резолюція «Розвиток у сфері інформації та телекомунікацій у контексті міжнародної безпеки». Дану Резолюції було прийнято в рамках роботи Першого комітету Генеральної Асамблеї Організації Об'єднаних Націй, до мандату якого відносяться питання роззброєння та міжнародної безпеки. В ній зазначалось, що сучасні технології можуть використовуватися таким чином, що це використання може «негативно впливати на безпеку держав» [5]. Варто відзначити, що лише в XIX столітті прийшло усвідомлення того, наскільки негативно технології можуть впливати на безпеку держав. При найгіршому сценарії мова йде про настання гуманітарної кризи, серйозні порушення прав людини і навіть втрату державності, особливо якщо зловмисна ІКТ-діяльність застосовується спільно з агресивними збройними діями. При цьому, використання руйнівного потенціалу ІКТ проти одного об'єкта критичної інфраструктури чи його систем цілком достатньо, щоб завдати

значної шкоди національній безпеці держави та добробуту населенню. Якщо ж мова йде про об'єкти технічної інфраструктури, які використовуються декількома державами, то успішні деструктивні атаки проти них, можуть мати вирішальне значення і влив на функціонування фінансових ринків, роботу глобального транспорту, зв'язку, міжнародної торгівлі та охорони здоров'я.

Резолюція 1998 року заклала основи розуміння важливості інформаційної безпеки. Резолюція одразу знайшла підтримку серед держав-учасниць ООН, проте лише через чотири роки Група урядових експертів була уповноважена Генеральною Асамблеєю «розглядати наявні та потенційні загрози у сфері інформаційної безпеки та можливі спільні заходи для їх вирішення…» [9]. Серед основних досягнень Групи урядових експертів – визнання того, що міжнародне право застосовується до кіберпростору (2013) і запровадження необов'язкових добровільних норм відповідальної поведінки держав (2015). Однак робота групи в 2016-2017 роках зайшла в глухий кут. Переговори провалилися, коли зайшла мова про застосування міжнародного гуманітарного права, контрзаходів та невід'ємного права на самооборону в кіберпросторі [6]. Невдача Групи урядових експертів призвела до того, що в 2018 році Генеральна Асамблея схвалила резолюцію, представлену Російською Федерацією, із закликом створити Відкриту робочу групу та нову Групу урядових експертів. Важливо підкреслити, що мандати обох груп дублюються і вони фактично займаються питаннями регулювання поведінки держав в кіберпросторі [10].

До складу новоствореної Групи урядових експертів, мандат якої триватиме з 2019 по 2021, увійшло 25 експертів на основі справедливого географічного розподілу, включаючи п'ять постійних членів Ради Безпеки. Мандат Групи полягає у розгляді питання застосування міжнародного права до кіберпростору, норм, правил і принципів, заходів зміцнення довіри та розвитку потенціалу держав в кіберпросторі. На відміну від Групи урядових експертів, до роботи Відкритої робочої групи може увійти будь-яка зацікавлена держава [4, с. 2]. Формат роботи цієї групи теж максимально відкритий: якщо Група урядових експертів проводить засідання за закритими дверми, то Відкрита робоча група до пандемії COVID-19 була максимально публічною, і держави могли надавати свої пропозиції, заслуховувати пропозиції інших та брати участь в дискусіях [6].

Аналіз останніх звітів Групи урядових експертів (2015 та 2021) та Відкритої робочої групи (2021) свідчить про підтвердження та конкретизацію деяких положень. Зокрема, у Доповіді Групи від 2021 року підтверджується наявність серйозних загроз, що несуть в собі ІКТ, і підкреслюється серйозне занепокоєння щодо зловмисного використання ІКТ проти критичної інфраструктури (включаючи критичну інформаційну інфраструктуру, інфраструктуру, що забезпечує населення важливими послугами та технічну інфраструктуру задля цілісності та доступності Інтернету, санітарно-медичну інфраструктуру тощо). Доповідь 2021 року також підтверджує позицію щодо того, що низка держав розвиває можливості ІКТ для військових цілей, як це уже зазначалося у доповіді за 2015 рік [7].

В доповідях двох груп зазначається, що норми не мають на меті обмежити чи заборонити дії сумісні з міжнародним правом, вони лише відображають очікування міжнародної спільноти, встановлюючи певні стандарти відповідальної поведінки держав. У звіті Групи урядових експертів від 2021 року підтверджується, що з часом можуть бути розроблені додаткові норми. Щодо доповіді Відкритої робочої групи, то одразу відмітимо той факт, що в ній міститься згадка про можливість подальшої розробки додаткових обов'язкових зобов'язань, яка, попри супротив деяких держав, все ж була включена до фінального тексту доповіді [7; 8].

Незважаючи на наявність двох паралельних процесів в межах Першого комітету Генеральної Асамблеї ООН, увага в даній статті приділяється, в першу чергу, роботі Групи урядових експертів, яка є традиційним механізмом та представила ряд важливих висновків в своїх доповідях. Успіхом доповіді Групи урядових експертів від 2021 року однозначно є уточнення змісту 11 добровільних норм, які виокремили ще в 2015 році:

Відповідно до першої норми або норми 13 (а) щодо міждержавної взаємодії в питаннях безпеки, держави повинні взаємодіяти задля забезпечення використання ІКТ в мирних цілях; утримуватися від використання інформаційно-комунікаційних технологій та їх мереж в цілях здійснення діяльності, що може створювати загрозу для міжнародного миру та безпеки і, звичайно, впорядковувати та поширювати інформацію щодо імплементації всіх норм, що містяться в Доповіді 2021 року [7, с. 8-9].

Важливо, що в формулюванні даної норми містяться прямі посилання на Статут Організації Об'єднаних Націй, серед основоположних цілей якого зазначається підтримання міжнародного миру та безпеки і міжнародна співпраця [11]. Таким чином експерти ще раз підкреслюють те, що кіберпростір не є вакуумом, де відсутні будь-які міжнародні зобов'язання, і те, що існуюче міжнародне право застосовується в кіберпросторі.

В Доповіді також встановлюється зобов'язання щодо проведення консультацій з усіма компетентними представниками влади, взяття до уваги всіх деталей, пов'язаних зі зловмисним використанням ІКТ, а також створення чи посилення національних структур та підходу до розслідування таких ІКТ-інцидентів. Тобто, друга норма стосується релевантної інформації. Важливо, що з позиції експертів слідує, що дана норма покладає на державу обов'язок координувати свою діяльність з компетентними органами на регіональному та міжнародному рівнях для того, щоб посилити їх здатність виявляти та розслідувати інциденти, пов'язані з використанням ІКТ, а також здійснювати обмін релевантною інформацією та кращою практикою [7, с. 9-10].

Норма 13 (с) стосується попередження зловживань ІКТ, що знаходиться в межах території держави. Ця норма фактично відображає обов'язок держав проявляти необхідну обачність в кіберпросторі та поза його межами, оскільки держава не повинна дозволяти використовувати свою територію для здійснення міжнародно-протиправних діянь з використанням можливостей ІКТ. Норма передбачає, що у випадках, коли держава дізналась про зловмисну діяльність, але не може її зупинити, вона повинна звернутись по допомогу до інших держав або до приватного сектору. Крім того, держава, інтереси якої зачіпаються такою діяльністю, мусить повідомити державу, з території якої така діяльність походить, про походження зловмисної ІКТ-діяльності з її території [7, с. 10].

В контексті цієї норми привертає увагу залучення приватного сектору. Беззаперечним є факт того, що міжнародне право створюється державами. Саме вони є основними суб'єктами міжнародного права, і саме на них покладаються зобов'язання. Проте, досить часто реагування на зловмисну діяльність в кіберпросторі вимагає залучення представників приватного сектору, в розпорядженні яких можуть знаходитись необхідні людські та технічні ресурси для реагування на ІКТ-інциденти [3].

Четверта норма торкається питань співпраці у протидії терористичному та злочинному використанні ІКТ. В рамках цієї норми держави повинні створити та/чи посилити механізми для обміну інформацією та надання допомоги. І найголовніше – посилити універсальні (зокрема в рамках ООН) та регіональні зусилля з метою реагування на використання ІКТ у злочинних та терористичних цілях, а також з цією метою розвивати партнерські відносини для співпраці з міжнародними організаціями, промисловими та науковими колами та громадянським суспільством [7, с. 10-11]. Зокрема, позитивним в цьому плані може стати співпраця третіх держав з Європейським Союзом, Кіберстратегія якого передбачає ряд інструментів для протидії такій діяльності та різні можливості для співпраці [5].

Норма 13 (е) щодо поваги прав людини наголошує на обов'язку держав поважати права та свободи людини і дотримуватися положень Резолюцій Ради з прав людини 20/8 та 26/13 про заохочення, захист та здійснення прав людини в Інтернеті та Резолюцій Генеральної Асамблеї 68/167 та 69/166 про право на недоторканність особистого життя в епоху цифрових технологій. В деталізації змісту цієї норми простежується, що від держав очікується, що вони залучатимуть зацікавлені сторони до процесів розробки

стратегій у сфері інформаційно-комунікаційної безпеки для того, щоб сприяти захисту та здійсненню прав людини в Інтернеті та звести до мінімуму потенційний негативний вплив обмежувальних заходів на людей [7, с. 11-12].

Наступні три норми є ключовими в рамках цієї статті, оскільки вони безпосередньо стосуються критично важливої інфраструктури держави. Норма 13 (f) загалом забороняє завдання шкоди критичній інфраструктурі. Відповідно до цієї норми держави не можуть здійснювати чи підтримувати поведінку, спрямовану проти об'єктів критичної інфраструктури, що забезпечує обслуговування населення. Для цього, на національному рівні держави повинні розробити національну політику та законодавчі заходи, щоб діяльність в сфері ІКТ не суперечила зобов'язанням держав за міжнародним право [7, с. 12-13]. Що стосується норми 13 (g), то вона стосується захисту критичної інфраструктури. Тобто, вимагає від держави позитивних дій. На думку Групи урядових експертів, для захисту важливої критичної інфраструктури та відновлення функціональності у разі інциденту важливо не лише визначити структурні, технічні, організаційні, законодавчі та нормативні заходи, а й заохочувати транскордонне співробітництво [7, с. 13]. Адже саме посилення заходів інформаційно-комунікаційної безпеки та зміцнення існуючих або розробки додаткових процесів та процедур спрятиме виявленню інцидентів у сфері ІКТ.

В Доповіді також міститься положення щодо запитів про допомогу. Аналіз даної норми та коментаря до неї свідчить про чотири відносно самостійні зобов'язання держав, що є нагадуванням про важливість міжнародної співпраці та поваги до суверенітету інших держав, критична інфраструктура яких стала об'єктом неправомірної ІКТ-діяльності, особливо коли така діяльність створює загрози міжнародному миру та безпеці. З урахуванням всіх обставин держави-жертви зловмисного застосування ІКТ повинні, по-перше, звертатися із запитом про допомогу до держав (на двосторонній основі або в рамках діяльності міжнародної організації) або приватного сектору. По-друге, держави мають створювати національні структури та механізми для ідентифікації та пом'якшення наслідків зловмисного використання ІКТ. По-трете, від держав вимагається створювати спільні процедури, які передбачають розгляд запитів про допомогу та реагування на такі запити. Нарешті, створення механізму для співпраці, який дозволяв би здійснювати комунікацію в кризових ситуаціях, систем менеджменту та прийняття рішень також витікає з даної норми [7, с. 13-14].

Група урядових експертів також не оминула увагою канали поставок обладнання та систем ІКТ. Згідно з нормою 13 (i) щодо цілісності каналів поставки продуктів ІКТ, держави повинні:

а) створювати на національному рівні всеосяжні, прозорі, об'єктивні та неупереджені правові рамки та механізми для управління ризиками щодо каналів поставки згідно зі своїми міжнародними зобов'язаннями;

б) розробляти стратегії та програми, спрямовані на заохочення впровадження постачальниками обладнання та систем ІКТ передових методів та кращих практик;

в) приділяти підвищену увагу у національній політиці та у діалозі з державами та відповідними учасниками в Організації Об'єднаних Націй та на інших майданчиках питанню про те, як забезпечити всім державам можливість здорової конкуренції та впровадження інновації,

г) вдаватися до спільних заходів, зокрема обміну передовим досвідом на двосторонньому, регіональному та багатосторонньому рівнях щодо управління ризиками, а також розробляти та впроваджувати загальні правила та стандарти безпеки на міжнародному рівні [7, с. 14-15].

Позитивним також є включення та конкретизація змісту норми стосовно подання інформації про вразливості, фактори вразливостей у сфері ІКТ та існуючі методи боротьби з ними. З метою досягнення цієї мети від держав очікується створення національних рамок та стратегій щодо інформування про ідентифіковані вразливості ІКТ. Аналогічно цьому, на міжнародному рівні мають бути прийняті глобальні рамки щодо ідентифікації та повідомлення про фактори уразливості ІКТ. На думку експертів, такі рамки сприятимуть обмеженню комерційного поширення вразливостей, а значить – стануть засобом захисту від будь-якого неналежного використання, яке створює потенційні ризики для міжнародного миру та безпеки або реалізації та захисту прав людини та основних свобод [7, с. 15-16]. Показовою в цьому плані є практика приватних компаній, які не тільки повідомляють про виявлені вразливості, а й класифікують такі вразливості залежно від потенційних наслідків та характеристик [12].

Нарешті, остання одинадцята норма або норма 13 (j) стосується незавдання шкоди групам екстреного реагування (групам реагування на комп'ютерні інциденти або групам реагування на інциденти інформаційної безпеки). Загалом ця норма є публічним свідченням особливого статусу таких груп. Тому, на думку Групи урядових експертів, позитивними з боку держави може стати надання публічних заяв або вжиття заходів стосовно підтвердження того, що держави не будуть використовувати такі групи для участі в зловмисній міжнародній діяльності, а навпаки – визнаватимуть та поважатимуть сфери діяльності та етичні засади груп екстремального реагування [7, с. 16-17].

Підсумовуючи аналіз згаданих норм, зазначимо, що їх статус з часом цілком ймовірно може змінитися. На підставі цих норм, які деталізують, якою має бути поведінка держав в кіберпросторі, може сформуватися практика держав та їх *opinio juris* щодо обов'язковості такої практики. В свою чергу, практика та *opinio juris* є конститутивними елементами міжнародних звичаїв, а формування звичаїв сприятиме їх подальшій кристалізації в міжнародних договорах, положення яких, на відміну від положень резолюцій Генеральної Асамблеї, є обов'язковими для держав-учасниць договору.

ЛІТЕРАТУРА

1. Brown K.A. Critical Path: A Brief History of Critical Infrastructure Protection in the United States. Spectrum Publishing Group, Inc. 198 p.
2. Final OEWG Report dated on 21 March 2021. URL: https://www.un.org/disarmament/open-ended-working-group/.
3. Greiman V.A. Public/Private Partnerships in Cyberspace. *Journal of Information Warfare*. Vol. 14, No. 3 (2015). P. 30-42.
4. Meyer P. Norms of Responsible State Behaviour in Cyberspace. In: Christen M., Gordijn B., Loi M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. 2020. URL: https://link.springer.com/chapter/10.1007/978-3-030-29053-5_18.
5. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. European Commission Press Release. 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.
6. Ponta A. Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes. American Society of International Law Insight. Volume 25, Issue 14. 2021. URL: https://www.asil.org/insights/volume/25/issue/14#_edn4. 6
7. Report of the GGE on Advancing responsible State behaviour in cyberspace in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf 3
8. UN GA Resolution adopted by the General Assembly on 31 December 2020, A75/240, Developments in the field of information and telecommunications in the context of international security, A/RES/75/240. URL: https://undocs.org/en/A/RES/75/240. 9
9. UNGA, Developments in the field of information and telecommunications in the context of international security A/RES/57/53, dated on 30 Dec 2002. 8
10. UNIDIR Report of the International security cyber issues workshop series. 2016. URL: www.unidir.org. 2
11. United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI. URL: https://www.un.org/en/about-us/un-charter/full-text. 7
12. What Do the Different Alert Level Colors Indicate? CISEcurity website. URL: https://www.cisecurity.org/cybersecurity-threats/alert-level/.