РАДА
ЕКОНОМІЧНОЇ БЕЗПЕКИ
УКРАЇНИ

КІБЕРАГРЕСІЯ:
САНКЦІЇ ТА ВІДПОВІДАЛЬНІСТЬ

Д-р Ілона ХМЕЛЬОВА, Д-р Богдан ВЕСЕЛОВСЬКИЙ

2024

РЕЗЮМЕ

Кіберагресія є серйозним викликом для глобальної безпеки. Розробка міжнародних правил і політичних стратегій часто не встигає за появою нових кіберзагроз. Кібератаки дедалі частіше інтегруються в стратегії сучасної війни, слугуючи засобом зловмисного впливу з боку окремих держав.

Досвід України у протидії російській кіберагресії є важливим для формування нових підходів – як у політичному, так і у військовому вимірах. Хоча демократичні держави розробили ефективні стратегії для протидії гібридним загрозам і захисту своїх інтересів, сучасний безпековий ландшафт вимагає більшої проактивності та координації. Стримування є недостатнім для захисту суверенітету та національних інтересів. Дедалі більшого значення набуває стратегія позбавлення авторитарних режимів інструментів для здійснення кіберагресії, зокрема через запровадження контрзаходів. Основними викликами є притягнення до відповідальності за кібератаки не лише хакерських груп, а й держав, а також поступове застосування секторальних санкцій та посилення контролю за ланцюгами постачання програмного забезпечення та інших технологій. Відповідальне ставлення приватних компаній та всебічний діалог між урядами та бізнесом відіграватимуть ключову роль.

Солідарність як головний принцип сучасної кібердипломатії має бути спрямованим на дві цілі: по-перше, спільне переслідування порушників за акти кіберагресії та воєнні злочини. По-друге, спільне формування червоних ліній щодо масштабних кібератак на об’єкти критичної інфраструктури. Такі дії мають розглядатися як порушення принципу незастосування сили в міжнародному праві та бути підставою для індивідуальної чи колективної самооборони.

1. КІБЕРАГРЕСІЯ ЯК ЗАГРОЗА ГЛОБАЛЬНІЙ БЕЗПЕЦІ

1.1. Агресія Російської Федерації має декілька вимірів[1]. Конвенційні атаки часто супроводжуються або посилюються кібератаками. Оскільки російська агресія продемонструвала, що кібератаки відбуваються одночасно й скоординовано з іншими видами незаконного втручання, досвід України має бути використаний іншими країнами для підвищення їхньої стійкості.

Серйозні кібератаки[2] на банки та державні установи, включаючи Міністерство оборони, передували повномасштабному вторгненню 2022 року. За кілька годин до того, як російські війська почали обстріл українських міст і вторгнення в країну, була здійснена кібератака на український супутниковий інтернет-сервіс[3].

Кібератаки також посилили страждання цивільного населення. Наприклад, восени та взимку 2022-2023 років, після серії кібератак на енергетичний сектор[4], Росія здійснила кілька хвиль ракетних атак на енергетичну інфраструктуру[5]. Одним з останніх прикладів атак на критичну інфраструктуру стала атака на одного з найбільших українських телекомунікаційних операторів «Київстар», яка призвела до знищення близько 40 відсотків його допоміжної інфраструктури[6]. Більше того, Росія атакує не лише Україну, але й її міжнародних союзників. Інституції ЄС, а також національні уряди та парламенти зазнають постійних кібератак[7]. Згідно зі Спільною доповіддю з кібербезпеки, яку нещодавно опублікувало Федеральне відомство з охорони конституції Німеччини разом з Федеральним бюро розслідувань США, Агентством з кібербезпеки та захисту інфраструктури США, Агентством національної безпеки США та іншими міжнародними партнерами, 161-й навчальний центр спеціального призначення Головного розвідувального управління (ГРУ) ГШ ЗС РФ (в/ч 29155) керує кібергрупою, націленою на об’єкти критично важливої інфраструктури в усьому світі[8]. Таким чином, активізація російської кіберагресії становить загрозу глобальній безпеці.

Аналіз[9] російських кібератак, проведений Радою економічної безпеки України, показав, що існують різні типи кореляцій з конвенційними атаками. Залежно від об’єкта, існують географічні та секторальні кореляції. За часовим критерієм – підготовчі, синхронні та атаки у відповідь. Російська стратегія війни повністю інтегрує гібридні інструменти. Більше того, за даними Державної служби спеціального зв’язку та захисту інформації України[10], у 2024 році кількість російських хакерських атак зросла на 19%. Відбувається зміщення

[1] https://cip.gov.ua/en/news/doslidzhennya-zv-yazok-mizh-kiberatakami-konvenciinimi-ta-informaciinimi-atakami-v-ukrayini-vidpovidaye-rosiiskii-koncepciyi-gibridnoyi-viini
[2] https://www.theguardian.com/world/2022/feb/16/ukraine-accuses-russia-of-cyber-attack-on-two-banks-and-its-defence-ministry
[3] https://www.reuters.com/business/aerospace-defense/satellite-firm-viasat-probes-suspected-cyberattack-ukraine-elsewhere-2022-02-28/
[4] https://www.bbc.com/news/technology-61085480
[5] https://www.iea.org/commentaries/russias-attacks-on-ukraines-energy-sector-have-escalated-again-as-winter-sets-in
[6] https://en.interfax.com.ua/news/general/955839.html
[7] https://www.politico.eu/article/europe-cyberattacks-russia-china-uk-ministry-of-defence-hacks/
[8] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2024/2024-09-05-joint-cyber-security-advisory-3.html
[9] https://reb.org.ua/en/reporting/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi-6yvkk2
[10] https://cip.gov.ua/en/news/russian-hackers-adopting-new-tactics-ssscip-report

фокусу уваги ворожих хакерів на цілі, безпосередньо пов'язані з театром військових дій та ланцюгами постачання.

1.2. Кібератаки також використовуються для підриву глобальної стабільності та демократії. Вони часто посилюють негативний вплив інших гібридних інструментів, таких як масовані дезінформаційні кампанії або акти саботажу, створюючи загрози для критично важливої інфраструктури та економіки. Згідно з останніми дослідженнями WELT AM SONNTAG та «Politico», Росія бере участь у так званій «тіньовій війні», яка включає в себе серйозні кібератаки на європейську інфраструктуру[11]. Наприклад, нещодавно російські хакери порушили роботу щонайменше чотирьох супутників Eutelsat з Франції та одного супутника, що належить люксембурзькій компанії SES[12].

Військові та розвідувальні експерти зазначають, що Росія застосовує повний спектр тактик: від впливу на політичні дискусії та здійснення кібератак на об'єкти критичної інфраструктури до широкомасштабних диверсій і вбивств.

Незалежні дослідники демонструють, що кількість кібератак, організованих державами, неухильно зростає[13]. І хоча держави традиційно не поспішають давати політичну оцінку кібератакам, нові виклики безпеці змінюють цю практику.

Наприклад, у травні 2024 року ЄС зробив офіційну заяву щодо продовження зловмисної поведінки Російської Федерації в кіберпросторі[14], рішуче засудивши зловмисну кампанію, проведену підконтрольною Росії організацією Advanced Persistent Threat Actor 28 (APT28) проти Німеччини та Чехії. Європейські країни підкреслили постійну безвідповідальну поведінку Росії в кіберпросторі, спрямовану проти демократичних інститутів, урядових установ і критичної інфраструктури в Європейському Союзі і за його межами. Одночасно НАТО опублікувало аналогічну заяву, в якій звинуватило Росію в активізації своєї кампанії, що включає саботаж, акти насильства, кібернетичне та електронне втручання, дезінформацію та інші гібридні операції[15].

Ще один яскравий приклад мав місце в серпні 2024 року, коли урядовці США звинуватили іранських хакерів у зламі президентської кампанії Дональда Трампа[16].

Згідно зі звітом Міжнародного валютного фонду[17], глобальна фінансова стабільність також перебуває під загрозою через зростання частоти та витонченості кібератак. За останні два десятиліття майже п'ята частина зареєстрованих кіберінцидентів вплинула на світовий фінансовий сектор, завдавши прямих збитків фінансовим компаніям на суму 12 мільярдів доларів США. Ця тенденція створює ще один виклик: кібератаки можуть бути використані для

[11] https://www.welt.de/politik/deutschland/plus254516486/Russlands-Kampf-gegen-den-Westen-Wie-Putin-in-Europa-zuendelt.html
[12] https://nos.nl/nieuwsuur/collectie/13903/artikel/2544559-rusland-saboteert-zes-europese-satellieten-ook-nederlandse-tv-geraakt
[13] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[14] https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/
[15] https://www.nato.int/cps/uk/natohq/official_texts_225230.htm
[16] https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts
[17] https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/

руйнування національних економік держав-супротивників. Наприклад, атаки на об'єкти критичної інфраструктури можуть завдати економічної шкоди, погіршити інвестиційний клімат і паралізувати нормальну роботу державних установ і служб.

1.3. Кіберсолідарність як принцип сучасної дипломатії трансформує підходи до безпеки. Оскільки гібридні загрози розмивають державні кордони, національний суверенітет потребує більш ефективного захисту. Координація всіх зусиль – єдина запорука успіху.

У новому оборонному звіті Microsoft[18] зазначається, що кількість кібератак зростає, а темпи атак, що фінансуються державами, збільшилися до такої міри, що зараз у кіберпросторі фактично ведеться постійна боротьба.

Таким чином, політичні рекомендації передбачають більш скоординоване реагування:

- запровадження жорстких контрзаходів у відповідь, включаючи, серед іншого, цільові санкції;
- робота над законними колективними контрзаходами;
- роз'яснення «червоних ліній» і забезпечення того, щоб підтримувані державою кібервторгнення не залишалися безкарними.

Чудовим прикладом таких підходів є Стратегія міжнародного кіберпростору та цифрової політики США[19]. Цей документ фокусується на розбудові широкої цифрової солідарності. У класичному розумінні це готовність працювати разом над досягненням спільних цілей, допомагати партнерам розбудовувати потенціал та надавати взаємну підтримку. Однак ця стратегія також включає ще один елемент солідарності – скоординовані дії для притягнення до відповідальності злочинних суб'єктів.

Україна також займає провідні позиції у формуванні нових підходів до архітектури безпеки. Протидія кіберагресії включена до багатьох нещодавно підписаних двосторонніх угод у сфері безпеки. Наприклад, Угода про співробітництво у сфері безпеки між Україною та Францією[20] передбачає, що «Учасники працюватимуть разом, щоб дати можливість Україні виявляти, стримувати і перешкоджати будь-якій кіберагресії, кібершпигунству, зокрема шляхом посилення кіберстійкості та захисту критичної інфраструктури від кібератак».

Двостороння угода про безпеку між Україною та Сполученими Штатами Америки[21] формально пов'язує класичні та гібридні атаки проти України, заявляючи про необхідність підвищення кіберстійкості її критичної інфраструктури, особливо енергетичних об'єктів, до повітряних ударів. Документ також передбачає посилення кіберзахисту від зловмисних кібератак з боку Росії та інших ворожих державних і недержавних суб'єктів, підкреслюючи таким чином глобальний характер цього виклику.

[18] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
[19] https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/.
[20] https://www.president.gov.ua/en/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-89005
[21] https://www.president.gov.ua/en/news/dvostoronnya-bezpekova-ugoda-mizh-ukrayinoyu-ta-spoluchenimi-91501

Визначивши кібероборону одним зі своїх основних завдань, держави-члени НАТО також зробили кілька важливих геополітичних кроків[22]:

- На саміті НАТО 2023 року у Вільнюсі члени Альянсу ухвалили нову концепцію посилення внеску кіберзахисту в загальну систему стримування і оборони НАТО і започаткували нову структуру на підтримку національних зусиль з пом'якшення наслідків атак у відповідь на значну зловмисну кіберактивність.
- На саміті НАТО 2024 року у Вашингтоні, округ Колумбія, члени Альянсу домовились про створення Центру інтегрованого кіберзахисту НАТО.

[22] https://www.nato.int/cps/en/natohq/topics_78170.htm

2. КІБЕРСАНКЦІЇ ТА ІНШІ ОБМЕЖУВАЛЬНІ ЗАХОДИ

2.1. Кіберсанкції розвинулися як новий інструмент безпеки. Автономні кіберрежими забезпечують стійкість санкцій та уможливлюють появу унікальних підходів.

Європейський Союз розробив чіткий та уніфікований підхід до протидії зловмисній кібердіяльності, яка загрожує його безпеці. У червні 2017 року ЄС створив Інструментарій кібердипломатії, що стало важливим кроком на шляху до спільної відповіді ЄС на кіберзагрози. Ця ініціатива дозволяє ЄС та його державам-членам використовувати низку інструментів Спільної зовнішньої та безпекової політики (СЗБП), включаючи санкції, для реагування на зловмисні кібератаки проти ЄС та його членів. Для того, щоб ввести в дію цей інструментарій, у травні 2019 року ЄС ухвалив два правові заходи – Регламент Ради (ЄС) 2019/796 та Рішення Ради (СЗБП) 2019/797, які створюють основу для санкцій проти осіб та організацій, відповідальних за значні кібератаки, що загрожують безпеці ЄС.

Санкції в межах цього механізму можуть застосовуватися до тих, хто планує, підтримує або заохочує значні кіберінциденти, особливо ті, що порушують критично важливу інфраструктуру або економічну стабільність. Заходи можуть включати заморожування активів та заборону на в'їзд для причетних осіб. Санкції накладаються одноголосним рішенням Ради за пропозицією будь-якої держави-члена або Високого представника, і ЄС веде оновлений список фізичних та юридичних осіб, на яких поширюються санкції. У травні 2022 року Рада продовжила дію цього механізму до 2025 року[23], підкресливши прихильність ЄС до кіберстійкості. У червні 2024 року ЄС запровадив санкції проти шести осіб, пов'язаних з кібератаками, зокрема проти тих, хто розгортав загрози на кшталт «Conti» і «Trickbot». Підхід ЄС, як правило, спрямований на недержавних суб'єктів, щоб уникнути прямого приписування атак державам, поважаючи суверенітет держав-членів[24] і лишаючи їм можливість здійснювати атрибуцію.

Сполучені Штати також мають режим кіберсанкцій, встановлений виконавчими наказами 13694 (2015) і 13757 (2016)[25]. Він спрямований на окремих осіб і групи, відповідальні за кібердіяльність, що загрожує національній безпеці або економічній стабільності. Санкції США можуть застосовуватися до осіб, причетних до хакерських атак, атак з вимогою викупу або крадіжки інтелектуальної власності. Підсанкційні особи можуть зіткнутися з заморожуванням активів, фінансовими обмеженнями та заборонами на в'їзд, що фактично перекриває їм доступ до фінансової системи США. Помітні санкції були спрямовані проти таких груп, як північнокорейська Lazarus Group і російське ГРУ за атаки з використанням програм-вимагачів, таких як NotPetya і WannaCry. США часто координують ці санкції з міжнародними союзниками, посилюючи стримуючий ефект, і розглядають можливість запровадження секторальних обмежень, таких як блокування доступу до критично важливих технологій, особливо для пов'язаних з державою кіберакторів.

[23] https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/

[24]https://www.consilium.europa.eu/en/press/press-releases/2024/06/24/cyber-attacks-six-persons-added-to-eu-sanctions-list-for-malicious-cyber-activitiescyberattacks-against-eu-member-states-and-ukraine/

[25] https://www.state.gov/cyber-sanctions/

Ці санкції підірвали фінансові мережі, що підтримують кіберзлочинну діяльність, зменшивши ресурси, доступні цим суб'єктам, і обмеживши їхню здатність проводити масштабні кібероперації. Кіберсанкції США часто координуються з міжнародними союзниками, включаючи Європейський Союз та Велику Британію[26]. Останні тенденції вказують на потенційний перехід від персональних санкцій до ширших секторальних обмежень, таких як обмеження доступу до технологій, критично важливих для кіберпотужностей, особливо для пов'язаних з державою суб'єктів, причетних до шпигунства або атак на американську інфраструктуру.

У відповідь на ескалацію кіберзагроз Сполучене Королівство запровадило Регламент про кіберсанкції 2020 року[27], який створив надійну основу для стримування та реагування на зловмисну кібердіяльність, що ставить під загрозу національну безпеку, економічну стабільність та ефективне функціонування міжнародних організацій. Це законодавство після Брекзиту узгоджується з глобальними зусиллями, відображаючи підходи Європейського Союзу та Сполучених Штатів і водночас враховуючи специфічні проблеми безпеки Великої Британії. Положення уповноважують Державного секретаря визначати фізичних або юридичних осіб, причетних до зловмисної кібердіяльності, і накладати на них санкції, включаючи заморожування активів, заборону на поїздки і заборону на фінансові операції.

Британський офіс впровадження фінансових санкцій (OFSI) відповідає за застосування фінансових санкцій, надаючи рекомендації[28] для забезпечення їх дотримання та ведення переліку визначених осіб. Британська система кіберсанкцій доповнює міжнародні зусилля, узгоджуючись з інструментарієм кібердипломатії ЄС і режимом кіберсанкцій США.

У грудні 2021 року Австралія запровадила власний автономний режим кіберсанкцій, що дозволяє застосовувати цільові санкції до осіб або груп, відповідальних за великі кіберінциденти. В рамках цього режиму міністр закордонних справ може накладати фінансові обмеження та заборони на поїздки на тих, хто бере участь або підтримує значні кіберінциденти, що впливають на Австралію або інші країни. Австралійський режим є широким і застосовується до кіберзагроз з будь-якої точки світу. Наприклад, у жовтні 2024 року Австралія запровадила санкції проти трьох лідерів російського кіберзлочинного угруповання Evil Corp, відомого своїми атаками з вимогами викупу, що завдавали значних фінансових збитків.

«Кіберінцидент» визначається як подія з використанням кібертехнологій, яка призводить до заподіяння шкоди або має на меті заподіяння шкоди Австралії або іншій країні. Цей режим застосовується у найбільш кричущих ситуаціях, що викликають міжнародне занепокоєння. Відповідне законодавство включає Закон про автономні санкції 2011 року та Положення про автономні санкції 2011 року. На відміну від санкцій проти конкретних країн, цей тематичний режим застосовується до поведінки, що підлягає санкціям, у всьому світі. Режим накладає фінансові санкції, включаючи заморожування активів і заборону на в'їзд для визначених фізичних та юридичних осіб. Перш ніж внести до переліку або зробити заяву в межах цього режиму, міністр закордонних справ повинен отримати письмову згоду від Генерального

[26] https://www.state.gov/taking-joint-action-against-cybercriminals/
[27] https://www.legislation.gov.uk/uksi/2020/597/made
[28] https://www.gov.uk/government/publications/cyber-sanctions-guidance/cyber-sanctions-guidance

прокурора та проконсультуватися з іншими відповідними міністрами. Департамент закордонних справ і торгівлі здійснює нагляд за впровадженням і дотриманням цих санкцій. Юридичні та фізичні особи зобов'язані дотримуватися санкцій, а порушення можуть призвести до значних штрафів[29].

Таким чином, ці країни створили механізми для застосування санкцій до фізичних та юридичних осіб, які займаються шкідливою кібердіяльністю, з метою підриву та стримування кіберзагроз. Координуючи свої дії на міжнародному рівні, ЄС, США, Велика Британія та Австралія посилюють кіберзахист, захищаючи інфраструктуру та економіку від все більш масштабних кібератак.

Можна зробити такий порівняльний огляд вищезгаданих національних режимів:

Критерій	США	ЄС	Британія	Австралія
Правова база	Виконавчі накази 13694 та 13757	Інструментарій кібердипломатії; Регламент (ЄС) 2019/796; Рішення 2019/797	Регламент про кібербезпеку (санкції) 2020	Закон про автономні санкції 2011 року; Положення про автономні санкції 2011 року
Сфера застосування	Глобальний режим; націлений на фізичних / юридичних осіб, які займаються зловмисною кібердіяльністю	Глобальний режим; націлений на фізичних / юридичних осіб, відповідальних за кібератаки, що загрожують ЄС або його країнам-членам	Глобальний режим; націлений на фізичних / юридичних осіб, причетних до кібердіяльності, що підриває безпеку Великої Британії або міжнародних організацій	Глобальний режим; націлений на фізичних / юридичних осіб, причетних до значних кіберінцидентів
Санкційні заходи	Заморожування активів, фінансові обмеження, заборони на поїздки	Заморожування активів, заборона на поїздки, заборона на надання коштів	Заморожування активів, заборона на поїздки, заборона на надання коштів	Цільові фінансові санкції, заборони на в'їзд
Державні органи	Управління з контролю за іноземними активами	Європейська служба зовнішньої діяльності; Рада ЄС	Британський офіс впровадження фінансових санкцій (OFSI)	Міністерство закордонних справ і торгівлі

[29] https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/significant-cyber-incidents-sanctions-regime

Останні події	Санкції проти північнокорейських та російських осіб за кампанії з вимагання викупу, такі як NotPetya та WannaCry	Регламент (ЄС) 2024/2642 та Рішення 2024/2643, ухвалені в жовтні 2024 року щодо обмежувальних заходів у зв'язку з гібридною дестабілізуючою діяльністю Росії	Імплементація Регламенту щодо кібербезпеки (санкцій) 2020 року	Створення автономного режиму кіберсанкцій у грудні 2021 року

2.2 Більше того, санкції за деякі кібератаки тепер є частиною комплексних санкційних режимів. Гарним прикладом є система санкцій ЄС проти осіб, відповідальних за підривну діяльність проти ЄС та його держав-членів. Це дозволяє системно реагувати на гібридні атаки.

8 жовтня 2024 року ЄС ухвалив Регламент (ЄС) 2024/2642[30] та Рішення (СЗБП) 2024/2643[31], що встановлюють рамки обмежувальних заходів у зв'язку з підривною діяльністю Росії. Ці правові інструменти забезпечують основу для запровадження санкцій проти фізичних та юридичних осіб, відповідальних за дії, що загрожують ЄС та його країнам-членам, включаючи кібератаки. Ці нові рамки ґрунтуються на Стратегічному компасі з безпеки і оборони[32], затвердженому Радою у 2022 році, який закликав до створення Гібридного інструментарію ЄС для виявлення та реагування на гібридні загрози. Інструментарій, що діє з грудня 2022 року, підкреслює прихильність ЄС до протидії складним кібероперація м за допомогою узгоджених заходів. Нова система ЄС спрямована на фізичних і юридичних осіб, які несуть відповідальність за дії або політику уряду Російської Федерації, що підривають або загрожують демократії, верховенству права, стабільності або безпеці в Союзі, одній або декількох його державах-членах, в міжнародній організації або третій країні, або які підривають або загрожують суверенітету або незалежності однієї або декількох держав-членів або третьої країни шляхом участі в кібератаках, що мають значний вплив на критично важливу інфраструктуру, основні послуги або громадську безпеку, а також здійснюють такі дії або політику, або отримують від них вигоду.

Обмежувальні заходи включають заборони на в'їзд і заморожування активів. Комплексна система санкцій ЄС може слугувати моделлю для інших країн, які прагнуть протистояти гібридним загрозам, включно з кібератаками. Встановивши чіткі правові інструменти та критерії для запровадження санкцій, країни можуть підвищити свою стійкість до дестабілізуючих дій. Прийняття подібних заходів передбачає:

- розробку правових інструментів, що визначають сферу застосування та критерії санкцій;
- створення механізмів ідентифікації та визначення фізичних та юридичних осіб, відповідальних за підривну діяльність;

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2642
[31] https://eur-lex.europa.eu/eli/dec/2024/2643/oj
[32] https://www.consilium.europa.eu/en/policies/strategic-compass

- забезпечення координації з міжнародними партнерами для підвищення ефективності санкцій[33].

Розширення режиму санкцій ЄС на діяльність інших держав, зокрема на Китайську Народну Республіку, вимагатиме ретельного аналізу геополітичної динаміки та міжнародних відносин. Раніше ЄС вже висловлював занепокоєння щодо зловмисної кібердіяльності, яка походить з території КНР. Наприклад, у липні 2021 року ЄС опублікував декларацію, в якій закликав владу КНР вжити заходів проти зловмисної кібердіяльності, що здійснюється з його території[34].

Таким чином, цей новий режим може бути розширений двома способами:
- ЄС може використовувати його проти інших країн, а не лише проти Росії.
- Інші західні країни можуть перейняти цю практику.

2.3. На майбутнє кіберсанкцій впливають щонайменше три тенденції.

По-перше, західні країни, ймовірно, застосовуватимуть двоступеневу атрибуцію під час оголошення нових санкцій – до хакерської групи та до держави. Нещодавнє дослідження продемонструвало[35], що ЄС використовував більш прямі заяви щодо причетності Росії. Наприклад, у липні 2022 року було оприлюднено декларацію, яка оголошує про засудження кібератак у січні та приписує Російській Федерації атаки KA-SAT у травні 2022 року[36]. Однак ЄС так і не згадав про те, що його члени постраждали. Тим не менш, цю публічну заяву можна інтерпретувати як оголошення прямої державної відповідальності за кібероперацію. Це позитивний крок, оскільки він уможливлює всебічну відповідальність держави.

По-друге, відбудеться поступовий перехід від виключно персональних санкцій до секторальних. Очевидною метою є обмеження доступу до західних технологій, які дозволяють здійснювати кібератаки на об’єкти критичної інфраструктури. Крім того, розгляд кібератак як невід’ємної частини гібридних операцій призведе до запровадження міжсекторальних обмежень. Такий підхід особливо актуальний у сучасних умовах, коли передові технології – такі як високопродуктивні обчислення, штучний інтелект і засоби шифрування – є критично важливими інструментами для зловмисної кібердіяльності.

По-третє, очікуються більш скоординовані дії. Наприклад, у жовтні 2024 року Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) визначило сім фізичних та дві юридичні особи, пов’язані з російським кіберзлочинним угрупованням, у межах тристоронніх дій з Великою Британією та Австралією[37]. Це позитивний приклад спільних заходів.

[33] https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/russia-eu-sets-up-new-framework-for-restrictive-measures-against-those-responsible-for-destabilising-activities-against-the-eu-and-its-member-states/
[34] https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/
[35] https://eurepoc.eu/wp-content/uploads/2024/02/Right-Thoughts-Right-Words-Right-Actions-February-2024.pdf
[36] https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/
[37] https://home.treasury.gov/news/press-releases/jy2623

У липні 2024 року Австралія, США і шість інших країн-членів Альянсу опублікували спільну рекомендацію, в якій визначили хакерську групу КНР, що фінансується державою, як значну загрозу для їхніх мереж. Ця безпрецедентна співпраця підкреслює необхідність об’єднання міжнародних зусиль для боротьби з кіберзагрозами.

3. ПРОТИДІЯ КІБЕРАГРЕСІЇ: ВІДПОВІДАЛЬНІСТЬ ТА ЗАПОБІГАННЯ

3.1. Відповідальність за агресію має бути багатовимірною і передбачати персональну кримінальну відповідальність та міжнародно-правову відповідальність держав.

Кіберагресія складається з двох компонентів: міжнародних протиправних дій Російської Федерації та міжнародних злочинів, скоєних російським військово-політичним керівництвом. Слід особливо підкреслити, що кіберагресія порушує зобов'язання erga omnes. Як визначив Міжнародний суд ООН[38], це зобов'язання, у виконанні яких мають юридичний інтерес усі держави, оскільки їхній предмет має важливе значення для міжнародного співтовариства в цілому. Таким чином, кожна держава, а не лише Україна, може притягнути Росію до відповідальності за порушення цих правил.

Незалежно від того, якої форми набуде правова база, розширення визначення поняття «агресія» для адекватного реагування на кіберзагрози є ключовим імперативом. Чинне визначення «агресії» в міжнародному праві є застарілим. У свою чергу, не кожна кібератака може вважатися актом агресії, навіть якщо її безпосередньо організовує держава. Оцінюються два критерії: по-перше, масштаб кібератаки, по-друге, намір завдати шкоди суверенітету іншої держави.

Хоча рішення про те, коли кібератака призведе до застосування статті 5 Договору НАТО[39] буде прийматися Північноатлантичною радою в кожному конкретному випадку, НАТО стверджує[40], що кібератака «може завдати такої ж шкоди сучасному суспільству, як і звичайний напад», і що «кіберзахист є частиною основного завдання НАТО з колективної оборони».

Масштаб атаки можна виміряти за конкретними наслідками, наприклад за людськими жертвами або матеріальними збитками. Що стосується атак на критичну інфраструктуру, то при аналізі агресії слід враховувати не лише руйнування самої інфраструктури, але й виведення її з ладу на тривалий час. Намір порушити суверенітет має стосуватися політичної волі здійснити напад з метою заподіяння шкоди політичній незалежності або територіальній цілісності іншої держави.

Так само, як недружні інциденти на фізичних кордонах відрізняються від повномасштабної війни, ізольовані невеликі кібератаки відрізняються від кіберагресії. Однак навмисне заподіяння відчутної шкоди іншій державі за допомогою кібератаки слід розглядати як агресію, подібно до обстрілу суверенної території[41].

Важливо адвокувати модернізоване визначення агресії в міжнародному праві, яке б відображало унікальну природу кібервійни. Одним із перших кроків може стати включення кіберпростору до юрисдикції спеціального трибуналу щодо злочину агресії проти України,

[38] https://www.icj-cij.org/case/50
[39] https://www.nato.int/cps/en/natolive/official_texts_17120.htm
[40] https://www.nato.int/cps/en/natohq/official_texts_112964.htm
[41] https://ukraineverstehen.de/cyberaggression-braucht-das-voelkerrecht-ein-update/

здатного здійснювати правосуддя шляхом притягнення до відповідальності організаторів агресії у всіх вимірах[42].

Агресія може супроводжуватися іншими міжнародними злочинами з використанням кіберелементів. Подальший розвиток технологій створює нові можливі загрози:

- Геноцид: нові технології та ШІ можуть бути використані для вчинення геноцидних актів, (насамперед, підбурювання до геноциду).
- Екоцид: кібератаки на об'єкти критичної інфраструктури потенційно можуть призвести до значної шкоди навколишньому середовищу.
- Злочини проти людяності: комбіновані гібридні дії можуть призвести до широкомасштабного нападу на цивільне населення.

3.2. Деякі російські кібератаки можна кваліфікувати як воєнні злочини. Це означає, що західні компанії, які уможливлюють ці атаки, сприяють вчиненню міжнародних злочинів.

Відповідно до статті 25 Римського статуту[43] особи можуть нести кримінальну відповідальність і підлягати покаранню, якщо вони сприяють вчиненню злочинів і надають засоби для їх вчинення. Цей принцип також закріплений у національному законодавстві багатьох країн.

Прокурори Міжнародного кримінального суду вже розслідують ймовірні російські кібератаки на українську цивільну інфраструктуру як можливі воєнні злочини. Таким чином, ймовірно, будуть створені правові прецеденти. Прокурор МКС Карім Хан прямо заявив, що «злочини, скоєні за допомогою кібертехнологій, можуть підпадати під юрисдикцію МКС, якщо будуть дотримані вимоги Римського статуту»[44]. За даними ЗМІ[45], команда МКС вивчає атаки на інфраструктуру, які ставили під загрозу життя людей, порушуючи постачання електроенергії та води, перериваючи зв'язок з аварійними службами або виводячи з ладу мобільні сервіси передачі даних, які надають попередження про повітряну небезпеку. Зусилля Росії, спрямовані на руйнування енергетичної інфраструктури України, підкреслили зростаючу інтеграцію кібератак з класичними військовими операціями, спрямованими на об'єкти критичної інфраструктури.

Оскільки атрибуція є найбільшою проблемою, доцільніше класифікувати ті кібератаки на цивільну інфраструктуру, які є частиною більшої атака (коли конвенційна атака і кібератака відбуваються одночасно або послідовно), як воєнні злочини. Водночас контекст має важливе значення. Міжнародний кримінальний суд має юрисдикцію щодо воєнних злочинів, особливо коли вони вчиняються як частина плану чи політики або як частина широкомасштабного вчинення таких злочинів. Тобто доведення логічного зв'язку між різними атаками полегшить атрибуцію та кваліфікацію (кібератаки на цивільну інфраструктуру не є ізольованими, а є частиною ширшого плану). Водночас це убезпечує українську хакерську спільноту. Україна не має політики чи плану вчинення широкомасштабних воєнних злочинів. А для Росії це спосіб ведення бойових дій.

[42] https://www.coe.int/en/web/portal/-/justice-for-crimes-committed-in-ukraine-ministers-of-justice-discuss-legal-cooperation-and-a-special-tribunal-for-the-crime-of-aggression
[43] https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf,
[44] https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through
[45] https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/

У свою чергу, нещодавнє розслідування Reuters демонструє вражаючу тенденцію[46]: незважаючи на російську гібридну війну, приватні суб'єкти підривають стратегії національної безпеки. Західні технологічні компанії, зокрема Cisco, IBM і SAP, погоджувалися на вимоги Росії отримати доступ до ретельно охоронюваних деталей безпеки продуктів. Російська влада звернулася до західних технологічних компаній з проханням переглянути вихідний код продуктів безпеки, таких як брандмауери, антивірусне програмне забезпечення та засоби шифрування, перш ніж дозволити імпорт і продаж цих продуктів в Росії. Ці запити формулюються як частина політики безпеки. Однак такі перевірки дають можливість російському уряду вивчити вихідний код – по суті, набір інструкцій, які керують основними операціями програмного забезпечення. Це може дозволити Росії виявити і використати вразливості в коді, створюючи можливості для шпигунства або кібератак на західні об'єкти. У цих перевірках беруть участь Федеральна служба безпеки Росії і Федеральна служба з технічного та експортного контролю, які були причетні до кібератак проти західних країн. Більше того, багато російських приватних суб'єктів, які проводять ці перевірки, мають задокументовані зв'язки з військовим або розвідувальним секторами. Наприклад, «Ешелон» – один з кількох акредитованих ФСБ випробувальних центрів. На його веб-сайті підкреслюється, що він визнаний Міністерством оборони Росії за «захист державної таємниці». Ситуація ще гірша, оскільки «Ешелон» потрапив під санкції західних урядів[47]. Росія використовує свої регуляторні механізми для доступу до критично важливих технологій, потенційно використовуючи їх для отримання стратегічної переваги.

Необхідно посилити діалог з приватними компаніями. Компанії повинні запобігати неправомірному використанню їхньої продукції, особливо у спосіб, що уможливлює кібератаки та придушення демократичних рухів. Невиконання зобов'язань має призводити до чітких наслідків, зокрема втрати основних привілеїв – доступу до державних контрактів або дипломатичної підтримки на міжнародних ринках. Запроваджуючи такі заходи, уряди можуть сигналізувати, що порушення санкцій не будуть толеруватися.

3.3. Правосуддя – це важливо. Але ще важливіше запобігти майбутнім злочинам. Саме тому слід винести уроки з російської агресії та позбавити авторитарні режими інструментів для ведення гібридних війн.

Залежність Росії від західних технологій є її слабкістю, яку можна використати для перемоги в гібридній війні. Наприклад, російська влада зробила кілька спроб змусити державні установи та приватні компанії перейти на альтернативні іноземним технології російського виробництва. Урядові рішення іноді ігнорувалися, оскільки компанії та установи воліють використовувати більш надійні та якісні рішення, навіть якщо це призводить штрафних санкцій або юридичних наслідків[48] . Нездатність Росії адаптуватися може призвести до подальшої ізоляції та зниження конкурентоспроможності країни в найближчі роки. Це означає, що подальший тиск на Росію можна розглядати як інвестицію в глобальну безпеку. Зусилля мають бути зосереджені на

[46] https://www.reuters.com/article/technology/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB/
[47] https://home.treasury.gov/news/press-releases/jy2204
[48] https://www.business-humanrights.org/fr/latest-news/opinion-how-to-exploit-russias-addiction-to-western-technology/

запобіганні кібершпигунству, яке дозволяє Росії красти західні технології та обходити існуючі санкції.

Іншим важливим кроком є блокування доступу Росії до західного програмного забезпечення та новітніх технологій без розмежування на військові та цивільні. Такий підхід запобігає використанню технологій подвійного призначення для кібератак або шпигунства. Крім того, слід запровадити повну заборону на російське програмне забезпечення, оскільки багато продуктів можуть бути використані для кібератак і стеження. З цією метою ланцюжок постачання програмного забезпечення має бути під більшим контролем і пильним наглядом. Важливо також не допустити, щоб країни потрапляли в залежність від російського програмного забезпечення, оскільки це посилює «м'яку силу» авторитарних режимів і збільшує залежність від них. Міжнародна спільнота може ще більше ізолювати російські компанії від глобальних ланцюгів постачання, що перешкоджатиме їхньому технологічному прогресу.

Нарешті, вкрай важливо не допустити використання Росією кібердипломатії для досягнення своїх геополітичних цілей. Практика міжнародних відносин показує, що Росія часто намагається ініціювати розробку нових міжнародних правил для кіберпростору. Не маючи наміру дотримуватися цих норм у майбутньому, Росія намагається в односторонньому порядку обмежити потенційні відповіді на свої зловмисні дії. Тому західні держави повинні зайняти лідерську позицію в розробці нових міжнародно-правових норм, одночасно посилюючи інструменти відповідальності та примусу. Крім того, не можна допустити використання нових міжнародних договорів для потенційного порушення прав людини авторитарними режимами[49].

[49]https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Кіберпростір є невід'ємною частиною російської агресії – не лише проти України, але й проти всіх демократичних держав. Більше того, кібератаки використовуються Китаєм, Іраном та Північною Кореєю для досягнення своїх національних цілей та підриву глобальної безпеки. Таким чином, міжнародна архітектура має бути перебудована відповідно до сучасних викликів:

- Нинішньої політики стримування, що базується на покаранні, недостатньо. Всі інструменти мають бути більш скоординованими та проактивними. Необхідно розробити нові обмежувальні заходи, щоб позбавити авторитарні режими сучасних технологій та інструментів для запуску і підтримки кіберагресії. Проактивна стратегія має полягати не лише в каральних заходах, а й у побудові надійного захисту в рамках інфраструктури, інституцій та міжнародної співпраці. Постійний обмін розвідданими, транскордонні навчання та оцінка загроз у реальному часі мають стати пріоритетами для створення справді превентивної системи кіберзахисту.
- Західні країни повинні повністю координувати і синхронізувати режими санкцій, запроваджені для протистояння кіберагресії. Крім того, кібератаки повинні атрибуватися державам у більш стійкий спосіб.
- Принаймні деякі кібератаки повинні розглядатися як частина більших загроз – конвенційних або гібридних. Санкції мають бути спрямовані не лише на кібервимір, але й забезпечувати комплексний вплив на здатність вести війну або здійснювати незаконне втручання (сфера застосування може бути розширена, щоб націлитися на ланцюги постачання, фінансові системи та логістичні мережі, які опосередковано підтримують кіберагресію).
- Слід запровадити нові міжнародно-правові підходи. Юридичне визначення агресії має включати кіберпростір, що уможливить відповідальність російського керівництва за його злочини. Крім того, національні та міжнародні суди, включно з Міжнародним кримінальним судом, повинні розглянути питання про правову кваліфікацію деяких кібератак як воєнних злочинів.
- Сучасні стратегії безпеки та оборонні угоди повинні враховувати кіберзагрози. Західні країни повинні розробити чітке бачення колективної самооборони для протидії кіберагресії. Воно повинно включати конкретні тригери для реагування, такі як застосування статті 5 Договору НАТО у відповідь на кібератаки, що загрожують національній безпеці. Спільні групи з кібербезпеки можуть бути розміщені в країнах-членах для швидкого реагування на транснаціональні кіберінциденти.
- Для глобального підходу життєво важливим є вихід за межі західних країн і включення країн з економікою, що розвивається, в Азії, Африці та Латинській Америці. Авторитарні режими часто використовують вразливості цих регіонів для проведення кібероперацій або використовують їх як непрямі центри для кібератак. Розбудова партнерських відносин з цими регіонами через програми посилення потенціалу, передачу технологій та спільні ініціативи з розвідки загроз зменшить ризики кіберагресії.