Norway Швеція Sverige ЄДНАННЯ АСКОЛЬД І ДІР НОРВЕЗЬКО-ШВЕДСЬКИЙ ФОНД РАДА ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Аналітична записка

Прогалини у кіберсанкціях: формування єдиного фронту

Короткий виклад

Документ окреслює необхідність посилення глобальних кіберсанкцій у відповідь на ескалацію кіберзагроз, особливо в контексті гібридної війни у 2025 році. Він висвітлює зростання рівня кібератак, зокрема спрямованих проти критичної інфраструктури, та аналізує санкції, введені США, ЄС, Великою Британією та Австралією. Необхідною складовою для ефективних кіберсанкцій є державно-приватні партнерства, які використовують досвід приватного сектору в галузі технологій, відкритих джерел інформації та інновацій для покращення виявлення загроз та забезпечення дотримання санкцій. Для вирішення нових викликів у документі пропонується створити єдиний онлайн-реєстр кіберсанкцій, вдосконалити платформи багатосторонньої координації та перейти до секторальних санкцій щодо передових технологій. Документ пропонує безпосередньо спрямовувати санкції проти держав-порушниць, застосовувати асиметричні санкції та інтегрувати кіберсанкції з активними кібероперaціями і заходами самооборони відповідно до міжнародного права. Такі кроки мають сприяти формуванню узгодженої та адаптивної глобальної відповіді на кіберзагрози, забезпечуючи підзвітність і стійкість міжнародної системи.

Загальний контекст та огляд останніх кіберсанкцій

Перші два квартали 2025 року відзначилися різким зростанням цифрової агресії. За даними CheckPoint [1] [2] середня кількість кібератак на одну організацію збільшилася на 47% у I кварталі та на 21% у II кварталі порівняно з аналогічними періодами 2024 року, що свідчить про структурне підвищення базового рівня загроз. Кількість випадків використання програм-вимагачів зросла ще стрімкіше, збільшившись на 126% у порівнянні з аналогічним періодом минулого року. У цьому рейтингу Північна Америка зазнала найбільшої кількості подібних атак – 62%, а на другому місці опинилась Європа – 21%.

Щодо цілей атак, Африка посідала перше місце за кількістю щотижневих інцидентів в обох кварталах, далі – країни Азійсько-Тихоокеанського регіону та Латинська Америка. Європа, хоча й не зафіксувала найбільшого загального обсягу атак, продемонструвала найбільше зростання у порівнянні з аналогічним періодом минулого року – 22%. Найбільш ураженими секторами стали:

Освіта
(+71% у I кв.; +31% у II кв.)

Державне управління
(+51% у I кв.; +26% у II кв.)

Телекомунікації
(+94% у I кв.; +38% у II кв.)

Масштабні кіберінциденти охопили всі критично важливі сектори. Державні та пов'язані із ними актори з Росії, Китаю та Ірану здійснювали атаки на критичну інфраструктуру й урядові системи по всьому світу. Цього року відбулася одна з наймасштабніших операцій кіберрозвідки в історії США – злам телекомунікаційних мереж групою Salt Typhoon з КНР[3]; у вересні було зафіксовано масштабні атаки програм-вимагачів на європейські аеропорти[4], а також цілеспрямовані кібератаки на платформи SalesForce [5] , системи охорони здоров'я[6], федеральні установи[7]...

1.https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/

2.https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/

3.https://www.theregister.com/2025/08/28/fbi_cyber_cop_salt_typhoon

4.https://www.securityweek.com/european-airport-cyberattack-linked-to-obscure-ransomware-suspect-arrested/

5.https://cybernews.com/news/stellantis-jeep-dodge-automaker-data-breach-salesforce-shiny-hunters/

6.https://cybernews.com/news/pacific-healthworks-everest-ransomware-attack-la-perouse-data-leak-physician-groups/

7.https://www.nytimes.com/2025/08/12/us/politics/russia-hack-federal-court-system.html

У цьому середовищі санкції залишаються одним із небагатьох інструментів, здатних змінити баланс вигод і витрат для держав, що здійснюють або толерують кіберзлочини. На відміну від суто оборо- нних заходів, скоординовані санкції забезпечують політичну атрибуцію, накладають репутаційні та матеріальні витрати на ворожі екосистеми, виконують функцію колективного стримування, коли військові заходи є непропорційними. По суті, вони перетворюють цифрові збитки на економічний і дипломатичний тиск, трансформуючи віртуальну агресію на реальну відповідальність.

Однак на практиці глобальна архітектура кіберсанкцій залишається фрагментованою. За перші три квартали 2025 року США 8 , ЄС 9 , Велика Британія10 та Австралія11 колективно внесли до санкційних списків 40 осіб та 24 організації за кіберзлочинну діяльність. Із них лише троє осіб одночасно фігурують у списках ЄС і Великої Британії – ба більше, ЄС запровадив санкції приблизно на сім місяців раніше. Інших збігів не було зафіксовано. Це свідчить про системну неузгодженість у визначенні, атрибуції та пріоритизації кіберзагроз різними юрисдикціями.

Випадок Garantex – російської криптовалютної біржі – ілюструє цю невідповідність. Цю компанію було внесено до санкційних списків США у серпні 2025 року за пов'язаною із кібером програмою; Великою Британією – ще у квітні 2022 року в межах заходів, пов'язаних із Росією; а Європейським Союзом – у лютому 2025 року в межах санкцій, запроваджених у зв'язку з агресією проти України. Попри те, що всі три санкційні режими спрямовані проти одного й того ж суб'єкта, вони посилаються на різні обґрунтування та терміни, причому в списках немає офіційного пояснення таких розбі- жностей. Існує ще одна перешкода, а саме непослідовність у включенні до списків та непрозорість атрибуції. Наприклад, у національному реєстрі санкцій України часто не наводяться детальні обґрунтування або доказова база для включення до списків, що ускладнює взаємну сумісність санкційних режимів і знижує юридичну визначеність.

Нерівномірність темпів і мотивів застосування санкцій, пов'язаних із кіберзлочинами у провідних західних юрисдикціях, засвідчує відсутність єдиної санкційної доктрини у цифровій сфері. Хоча всі чотири розглянуті приклади держав формально декларують мету стримування ворожих кібера- ктивностей, практична реалізація їхніх заходів має переважно реактивний характер і до того ж є суттєво фрагментованою. Частину рішень класифіковано за категорією «Росія», інші — за «кібер», «права людини» чи «Україна», але координація між ними майже відсутня.

Попри це, простежуються певні закономірності. У всіх юрисдикцій основним обмежувальним заходом є замороження активів, що відображає обмеженість інструментів, доступних для боротьби з цифровими загрозами, оскільки фінансові та транзакційні обмеження залишаються найбільш ефективною формою екстериторіального тиску. Переважна більшість підсанкційних суб'єктів походять з Росії, Китаю та Південно-Східної Азії, що відображає як геополітичну концентрацію наступальних кіберспроможностей, так і відносно вищий рівень упевненості у встановленні їхньої причетності. Також більшість підсанкційних осіб, пов'язаних із РФ, є співробітниками Головного управління Генерального штабу ЗС РФ (ГРУ).

Разом з тим, обґрунтуванню цих заходів часто бракує аналітичної чіткості. У більшості країн санкці- йні оголошення містять лише загальні формулювання на кшталт «зловмисна кіберактивність, що загрожує національній безпеці або громадянам». Винятками є США та ЄС, де запровадження санкцій супроводжується офіційними пресрелізами з детальними поясненнями та посиланнями на конкретні хакерські групи, кампанії чи елементи інфраструктури, що зазнали удару.

Загалом, сучасна динаміка свідчить про фрагментовану і при цьому динамічну архітектуру кіберстримування. Кіберсанкції частіше використовуються не як узгоджений стратегічний інструмент, а як політичний сигнал – спосіб продемонструвати позицію. Зростаюча тенденція до замороження активів та обмежена деталізація публічних обґрунтувань

вказують на те, що, попри зростання згоди щодо того, кого карати, спільного бачення щодо як і чому досі бракує. Це створює інституційні прогалини, якими можуть скористатися суб'єкти під санкціями, та обмежує потенціал санкційної політики як цілісного режиму стримування у цифровому просторі.

8.https://home.treasury.gov/news/press-releases?title=cyber+&publication-start-date=&publication-end-date=
9.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32025D0171
10.https://www.bvifsc.vg/sites/default/files/31jul25-uk-sanctions-update-cyber-russia-regime.pdf
11.https://www.opensanctions.org/entities/NK-XQyqxmZPMezqQiDeHoGQjf/

Роль державно-приватного партнерства

Санкції та експортний контроль у сфері кіберу не можуть бути ефективно розроблені або впроваджені без тісної співпраці з приватним сектором. Приватні компанії, особливо ті, що працюють у сфері технологій та кібербезпеки, володіють критично важливими знаннями, ресурсами та даними в режимі реального часу, необхідними для виявлення та протидії кіберзагрозам. Уряди покладаються на інновації приватного сектору для відстеження зловмисних суб'єктів, розробки захисних технологій та ефективного застосування санкцій.

Громадські організації та бізнес зарекомендували себе як надійні партнери у розробці традиційних санкцій, про що свідчить досвід України у протидії російській агресії. Ця співпраця відіграла ключову роль у таких сферах, як розслідування на основі відкритих джерел інформації (OSINT), збір приватної розвідувальної інформації та постійний моніторинг підсанкційних суб'єктів. Успіх цих зусиль підкреслює необхідність розширення таких практик для реалізації кіберсанкцій. Завдяки партнерству з приватним сектором держава може отримати доступ до спеціалізованих навичок і технологій, які покращують її здатність відстежувати незаконну кібердіяльність, виявляти тактики ухилення від санкцій та посилювати механізми їхнього виконання. Розширення цих партнерських відносин має вирішальне значення для створення стійкої системи санкцій, здатної адаптуватися до мінливих кіберзагроз.

Приватний сектор є не менш важливим у формуванні регуляторних підходів до санкцій та пов'язаних з ними інструментів, таких як експортний контроль та перевірка інвестицій у високотехнологічних галузях. Приватні компанії часто працюють на передовій технологічних інновацій, що дає їм унікальне розуміння ризиків та можливостей, пов'язаних з новими технологіями. Без їхнього внеску уряди ризикують створити регуляторні норми, які будуть або надто обмежувальними, гальмуючими інновації, або надто м'якими, не здатними усунути вразливості.

Україна має цінний досвід у сприянні державно-приватному партнерству, який може слугувати зразком для наслідування. Національна санкційна коаліція, яку координує Рада економічної безпеки України, є прикладом того, як партнерство між урядом, громадянським суспільством та бізнесом може сприяти просуванню політики санкцій. Крім того, РЕБ працює над запуском Trusted Tech Caucus в парламенті України у співпраці з Інститутом технологічної дипломатії (США) та Асоціацією народних депутатів України. Ця ініціатива має на меті залучити приватний сектор до розробки нормативних актів щодо передових технологій, щоб політика ґрунтувалася на галузевому досвіді та відповідала найкращим світовим практикам.

Рекомендації

Рекомендація 1:
Створити єдиний онлайн-реєстр кіберсанкцій

Створення єдиного онлайн-реєстру кіберсанкцій є необхідним кроком для підвищення ефективності міжнародних заходів реагування на кіберзагрози. Об'єднані реєстри виявилися надзвичайно цінними для швидкої перевірки підсанкційних суб'єктів з огляду на досвід існуючих санкційних режимів проти Росії від ЄС і США. Ці системи дозволяють зацікавленим сторонам, зокрема урядам, підприємствам та фінансовим установам, швидко перевіряти, **чи підпадає особа, організація або суб'єкт під обмеження, тим самим зменшуючи ризики недотримання вимог та спрощуючи процес їх виконання.** У контексті кіберсанкцій подібний глобальний реєстр централізував би інформацію про визначених кіберсуб'єктів, що полегшило б транско- рдонне відстеження та атрибуцію зловмисних дій.

Крім того, єдиний реєстр полегшив би **відстеження кібероперацій**, які часто діють через проксі-сервери. Шляхом об'єднання даних з різних юрисдикцій, він забезпечив би комплексне уявлення про зв'язки, тактики та операційні схеми, сприяючи обміну розвідданими між партнерами. Це особливо важливо з огляду на спільний характер кіберзагроз, коли атаки на одну країну можуть мати побічні ефекти для інших, наприклад, порушення роботи критичної інфраструктури або викрадення конфіденційних даних. Централізована платформа сприятиме узгодженню атрибуцій та допоможе запобігти широковживаним тактикам ухилення, таким як ребрендинг або перенесення операцій.

Важливо розуміти, що для впровадження такого реєстру та забезпечення точності і захисту даних потрібна міжнародна співпраця. Партнери повинні надавати пріоритет стандартам взаємодії для інтеграції існуючих національних баз даних та сприяти створенню колективного механізму захисту.

Рекомендація 2:
Посилити ефективну співпрацю за допомогою синхронізованих платформ

Попри те, що спільні заяви про кіберсанкції демонструють готовність до колективних дій, відсутність синхронізації між режимами підриває їхній вплив. Різні країни часто встановлюють різні рівні обмежень, через що утворюються вигідні для зловмисників прогалин. Для вирішення цієї проблеми існує потреба у створенні спеціальних платформ для постійної координації, до прикладу багатосторонні форуми або цифрові портали, де союзники можуть узгоджувати списки санкцій, обмінюватися доказами та координувати стратегії їхнього застосування.

Більше того, уніфікація обмежень передбачає стандартизацію критеріїв для визначення та накладення санкцій. Наприклад, прийняття спільних порогових визначень кіберінцидентів може запобігти розбіжностям, які дозволяють правопорушникам шукати притулок у юрисдикціях з менш суворими вимогами. Ці платформи також можуть сприяти **обміну інформацією в режимі реального часу**, що дозволить швидше реагувати на нові загрози. Завдяки окремому середовищу для співпраці, союзники можуть об'єднати ресурси для проведення розслідувань та нарощування потенціалу, особливо для країн з обмеженим досвідом у сфері кібербезпеки.

Зрештою, ефективна співпраця вимагає політичної волі та інституційної підтримки для подолання перешкод, як от розбіжності в законодавчих базах. Створення спільних робочих груп могло б інституціоналізувати ці зусилля, задля формування більш згуртованого міжнародного фронту проти кіберагресії. Такий синхронізований підхід не тільки посилив би тиск на порушників, але й продемонстрував би спільну рішучість дотримуватися кібернорм.

Рекомендація 3:
Перехід до секторальних санкцій щодо передових технологій

Перехід до секторальних санкцій має вирішальне значення для обмеження доступу авторитарних режимів до передових технологій, які сприяють кібератакам. Такі технології, як хмарні сервіси, новітні мережеві інструменти та платформи для аналізу даних, часто мають подвійне призначення та дозволяють здійснювати як законні операції, так і зловмисні кіберкампанії. Застосовуючи широкі обмеження до цілих секторів, а не до конкретних суб'єктів, санкції можуть порушити ланцюги постачання хакерам, що фінансуються державою, тим самим зменшуючи їхню спроможність здійснювати складні вторгнення, як операції з використанням програм-вимагачів або шпигунства.

Крім того, до цих санкцій необхідно інтегрувати нормативно-правові рамки для нових технологій, таких як штучний інтелект (ШІ). Системи ШІ можуть автоматизувати кіберзагрози, що робить їх стратегічним активом для ворожих держав. Санкції повинні бути пов'язані з експортним контролем та забороною інвестицій в обладнання та програмне забезпечення, пов'язані з ШІ, щоб авторитарні режими не могли безконтрольно здобувати та розвивати ці можливості. Така проактивна позиція запобігатиме поширенню загроз, пов'язаних із ШІ, та сприятиме впровадженню етичних глобальних стандартів у розвитку технологій.

Загалом, така зміна вимагає ретельного підходу, щоб мінімізувати небажані економічні наслідки для світових ринків і водночас максимізувати вигоди в галузі безпеки. **Зосередившись на технологіях з високим рівнем ризику**, секторальні санкції слугуватимуть потужним інструментом для стримування кіберагресії та створення безпечнішого цифрового середовища.

Рекомендація 4:
Розширити санкції та атрибуцію для безпосереднього включення держав

Санкції та заходи з встановлення відповідальності повинні виходити за межі кіберугруповань і бути спрямовані безпосередньо на держави-спонсори, з огляду на те, що багато кібероперацій здійснюються за вказівкою держави. Хоча технічне встановлення відповідальності зосереджується на цифровій криміналістиці: відстеження IP-адрес або ознак шкідливого програмного забезпечення, політичне встановлення відповідальності стає актуальним у багатогранних збройних конфліктах, де кібератаки є частиною більш широкої гібридної війни. Цей подвійний підхід дозволяє притягнути уряди до відповідальності, навіть коли прямі зв'язки приховані за допомогою проксі-серверів, тим самим усуваючи прогалини в чинних режимах, які часто захищають державних акторів.

Приписування відповідальності державам дозволяє застосовувати більш комплексні санкції, зокрема **дипломатичні, економічні або ж обмеження на пересування**, що виходять за межі заходів, спрямованих виключно на кіберпростір. Наприклад, у випадках, коли кіберінцидент пов'язаний з розвідувальним апаратом держави, санкції можуть передбачати заморожування активів або заборону на участь посадових осіб у міжнародних форумах. Таке розширення сфери застосування санкцій запобігає ескалації конфлікту, оскільки змушує потенційних агресорів відчути наслідки кібератак на національному рівні.

Для ефективної реалізації цього союзники повинні розробити спільні протоколи для визначення відповідальності, об'єднавши розвіддані з різних джерел для побудови надійних кейсів. Це підвищить легітимність санкцій і зменшить ризик помилкової атрибуції. В кінцевому підсумку, націлення на держави безпосередньо зміцнює міжнародне верховенство права в кіберпросторі, сприяючи підзвітності та стабільності.

Рекомендація 5:
Застосовувати асиметричні санкції у відповідь на кібератаки

Санкції, введені у відповідь на кібератаки, не повинні обмежуватися лише кіберпростором; натомість вони можуть охоплювати ширший спектр обмежень прав і можливостей держави-порушника. Така гнучкість дозволяє застосовувати **асиметричні заходи, спрямовані на вразливі місця в інших секторах**, таких як фінанси, торгівля або дипломатія, що посилює бажаний ефект. Наприклад, кібервтручання в критичну інфраструктуру може спричинити санкції щодо експорту енергії або культурних обмінів, порушуючи більш широкі інтереси агресора без ескалації до прямої кібервідповіді.

Такий підхід враховує, що **кібератаки часто слугують стратегічним цілям за межами цифрової сфери**, таким як економічний саботаж або

політичний вплив. Відокремлюючи відповідь від характеру атаки, санкції стають універсальним інструментом у зовнішньополітичному арсеналі держави, призначеним для максимального стримування та мінімізації ризиків взаємної кіберескалації. Це також дозволяє вживати пропорційних заходів, що відповідають міжнародному праву, забезпечуючи обґрунтованість та ефективність відповідних дій.

На практиці особи, які приймають рішення, повинні **оцінювати контекст кожного інциденту**, щоб вибрати відповідні, недзеркальні санкції, та консультуватись із союзниками для координації дій. Ця стратегія не тільки передбачає покарання за безпосереднє правопорушення, але й сигналізує, що кіберагресія матиме багатогранні наслідки, що сприятиме створенню більш безпечного глобального середовища.

Рекомендація 6:
Розробити автономні режими кіберсанкцій із накопичувальним застосуванням

Кіберсанкції можуть діяти як самостійний автономний режим, для протидії унікальній природі цифрових загроз. Ця незалежність дозволяє вживати спеціалізованих заходів, таких як блокування доступу до глобальних мереж або заморожування хакерських криптовалютних активів без переплетення їх з не пов'язаними геополітичними питаннями. Автономний режим спрощує впровадження та дозволяє швидко приймати рішення на основі доказів, що стосуються кіберпростору, а також зменшувати бюрократичні перешкоди в конфліктах, що охоплюють кілька сфер.

Однак, коли кібератака є частиною збройного або гібридного нападу, ці санкції повинні застосовуватися комплексно разом з іншими обмеженнями. Наприклад, якщо кібероперація підтримує військову агресію, це може спричинити багаторівневі санкції як за режимом кібервійни, так і за режимом звичайної війни, що посилить тиск на порушника. Такий комплексний підхід забезпечує всебічне охоплення, не даючи агресорам можливості розділити свої дії на окремі частини, щоб уникнути повної відповідальності.

Щоб збалансувати ці елементи, міжнародні угоди повинні визначати критерії для автономії та інтеграції, сприяючи ясності та послідовності. Така система підвищила б адаптивність санкцій, зробивши їх більш потужним інструментом протидії новим гібридним кіберзагрозам.

Рекомендація 7:
Сприяти спільній атрибуції для підвищення точності та стримування

Спільні процеси атрибуції значно підвищують точність виявлення виконавців кібератак, використовуючи колективний інтелект декількох країн. Об'єднуючи технічні дані, такі як зразки шкідливого програмного забезпечення та мережеві журнали, союзники можуть підтвердити висновки та зменшити кількість помилок, які можуть виникнути в результаті

ізольованих аналізів. Ця спільна робота не тільки вдосконалює базу доказів, але й формує спільне розуміння методології зловмисників, що дозволяє вживати більш цілеспрямованих та ефективних контрзаходів.

Більше того, спільне визнання легітимізує подальші дії, такі як санкції або дипломатичні звинувачення, демонструючи міжнародний консенсус. Коли кілька країн публічно атрибують атаку, це підриває правдоподібність заперечень агресора та посилює моральну та юридичну вагу відповіді. Така єдність сигналізує потенційним порушникам, що кібератаки зустрінуть скоординовану реакцію, тим самим посилюючи стримуючий ефект та запобігаючи майбутнім інцидентам.

Для сприяння цій практиці слід створити такі механізми, як центри обміну інформацією або спільні кіберцентри, щоб полегшити безпечну співпрацю. З часом спільна атрибуція сприятиме формуванню норм у кіберпросторі, сприяючи прозорості та підзвітності між державами.

Рекомендація 8:
Сприяти кращій співпраці з приватним сектором у сфері нерозповсюдження технологій

Покращення співпраці з приватним сектором є вкрай важливим для запобігання поширенню передових технологій серед авторитарних режимів, які можуть використовувати їх для кібератак. Компанії у сфері технологій, телекомунікацій та програмного забезпечення відіграють ключову роль у ланцюгах постачання і повинні застосовувати стандарти корпоративної відповідальності для ретельного контролю експорту та партнерських відносин. Це включає процедури належної перевірки для виявлення ризиків зловживання технологіями, наприклад у сфері спостереження або наступальних кіберзасобів, тим самим приводячи ділові практики у відповідність до глобальних інтересів безпеки.

Державно-приватне партнерство може сприяти цьому завдяки механізмам обміну інформацією про загрози та передовим досвідом. Така синергія допомогла б запобігти заволодінню зловмисними державами такими інструментами, як алгоритми штучного інтелекту або хмарна інфраструктура, що зменшило б загальний рівень загроз.

Зрештою, така співпраця вимагає заходів з побудови довіри, включаючи правовий захист спільних даних та створення спільних робочих груп. Включаючи корпоративну відповідальність у боротьбу проти поширення кіберзлочинності, союзники можуть створити більш надійний бар'єр проти авторитарного використання технологій, підвищивши колективну кіберстійкість.

Рекомендація 9:
Адаптувати підходи до приватних військових компаній з урахуванням появи кібернайманців

Поява кібернайманців – приватних суб'єктів, найнятих для проведення наступальних кібероперацій – вимагає кардинальних змін у регулюванні діяльності приватних військових компаній (ПВК). Попри традиційну зосередженість на кінетичній війні, ПВК все частіше залучаються до цифрової сфери, що суттєво стирає межі між державними та недержавними суб'єктами. Шляхом визнання кібернайманців продовженням традиційних ПВК, регуляторні органи можуть запровадити ліцензійні вимоги, механізми нагляду та заходи відповідальності, щоб запобігти нерегульованому поширенню кіберможливостей.

Санкції повинні застосовуватися до ПВК, які порушують міжнародне право у кіберпросторі. Наприклад, якщо ПВК здійснює системні кібератаки, що зачіпають цивільне населення, вона може зіткнутися із заморожуванням активів, забороною на пересування або забороною на укладення контрактів. Такий підхід відповідає принципам Женевських конвенцій, адаптованим до цифрової війни. Застосування санкцій до тих ПВК, що не дотримуються вимог, стримуватиме їх участь у незаконній діяльності та тиснутиме на держави, що їх приймають.

Адаптація нормативно-правової бази вимагає багатосторонньої співпраці з метою визначення поняття «кібернайманець» та створення органів контролю. Інтегруючи санкції в більш широку нормативно-правову екосистему, союзники можуть зменшити ризики, пов'язані з приватизованими кіберзагрозами та сприяти створенню більш відповідального та безпечного глобального кіберсередовища із забезпеченням дотримання гуманітарних стандартів.

Рекомендація 10:
Поєднувати санкції з іншими заходами впливу, включаючи наступальні кібероперації та самооборону

Для досягнення максимального ефекту кіберсанкції повинні бути інтегровані з цілим спектром заходів впливу аби створити багатогранну стратегію проти агресорів. Це стосується дипломатичного тиску, економічних стимулів для дотримання вимог та інформаційних кампаній з викриття зловмисних дій. Завдяки поєднанню санкцій з цими інструментами, відповідні заходи стають більш адаптивними, стійкими, та спрямованими не тільки на усунення безпосередніх загроз, але й на довгострокову зміну поведінки. Наприклад, поєднання заморожування активів з публічним викриттям може посилити репутаційний збиток, а економічна допомога постраждалим союзникам зміцнює колективну стійкість.

Ключовим елементом є перехід до наступальних кібероперацій як допоміжного заходу, що проводиться правомірно з метою проактивного підриву можливостей супротивників. Замість того, щоб покладатися виключно на оборонні позиції, держави повинні розробити доктрини цілеспрямованих кіберзаходів, таких як нейтралізація серверів управління та контролю, що використовуються в атаках. Ця зміна вимагає чітких правил застосування сили, щоб уникнути ескалації і гарантує пропорційність операцій та можливість атрибуції в разі стратегічної вигоди. Наступальні дії в поєднанні з санкціями можуть спричинити негайні витрати, що ефективніше запобігає майбутнім інцидентам, ніж самі санкції.

Крім того, більш активне застосування права на самооборону відповідно до статті 51 Статуту ООН є необхідним у разі серйозних кіберінцидентів, які прирівнюються до збройних нападів. Це положення дозволяє вживати необхідних і пропорційних заходів реагування, в тому числі й кінетичні, якщо кіберзагрози перевищують певний поріг. Включаючи кіберзахист до цієї правової бази, держави зможуть легітимізувати свої дії та координувати їх з союзниками через організації, як НАТО. Цей підхід, що поєднує санкції, наступальні дії та самооборону, посилює стримуючий ефект, сприяє дотриманню міжнародних норм та підвищує глобальну стабільність у кіберпросторі.

Автори:

Д-р Ілона Хмельова, секретар Ради економічної безпеки України, позаштатний науковий співробітник Університету Джорджа Вашингтона, khmeleva@escu.ua

Соломія Вибрановська, експерт Ради економічної безпеки України, s.v@escu.ua

Рекомендації були підготовлені у консультаціях з Міністерством закордонних справ України

Публікацію створено Радою економічної безпеки України за підтримки Фонду “Аскольд і Дір”, що адмініструється ICAP Єднання в межах проєкту “Сильне громадянське суспільство України – рушій реформ і демократії” за фінансування Норвегії та Швеції. Зміст публікації є відповідальністю Ради економічної безпеки України та не є відображенням поглядів урядів Норвегії, Швеції або ICAP Єднання.