ТЕРМІНОЛОГІЧНА ТА НОРМАТИВНО-ПРАВОВА НЕВИЗНАЧЕНІСТЬ У СФЕРІ КІБЕРБЕЗПЕКИ

Муравська (Якубівська) Ю. Є.
к.е.н., доц., доцент кафедри економічної безпеки та фінансових розслідувань
Тернопільський національний економічний університет

Категорія «кібертероризм» та дослідження в науковій та юридичній літературі імовірних наслідків його проявів містить помітну ідеологічну складову, що обумовлено глобальною боротьбою з тероризмом. На дану проблему як одну з першорядних звернули увагу автори професійної доповіді «Мінімізація системних ризиків у сфері кібербезпеки», що була підготовлена на замовлення ОЕСР. У даній доповіді, наприклад, зазначається, що аналіз реального ступеня загроз від кібератак фактично унеможливлюється врезультаті відсутності цілісної термінології та частого розуміння під кібервійнами та кібератаками заходів, які можуть мати принципово протилежне значення [1].

Проте на практиці майже неможливо доказати, що ті акти, які зазвичай відносять до кібертерактів, відповідають якимось конкретно визначеним критеріям. Характерним даному поняттю можна відзначити активність вірусу Stuxnet у Ірані в 2010 р., позаяк його функція справді могла створити загрозу для життя робітників на ядерних об'єктах. Але так як ніхто так і не взяв відповідальність за реалізацію даної акції на себе, а навіть якби це і трапилося, то без добровільного зізнання про політичні мотиви ініціаторів цей акт дуже важко ідентифікувати як кібертероризм, скоріше, як кібердиверсію. Ще менше на кібертеракти подібні неодноразово згадувані події у Грузії та Естонії, а також в Україні, де в період конфліктних ситуацій з Російською Федерацією було фактично зломано більшість урядових сайтів. Окремі фахівці доречно пропонують вважати такі дії або хактивізмом, а в окремих особливо важких випадках, кібервандалізмом, або ж кібершпигунством, якщо акції проводилися з метою отримання та викрадення конфіденційної інформації.

Отож, важливим з термінологічної точки зору є відокремлення кібертерактів від актів хактивізму, як використання власне хакерства цілеспрямовано у політичних цілях, що потенційно може мати великі наслідки для країни. Прикладом може стати діяльність групи «Anonymous» в мережі, що була направлена проти усіх організацій, які захищають авторське право та суміжні права, а також цензуру в інтернеті та відповідальні за замахи зупинки діяльності «WikiLeaks». Врезультаті їх роботи було порушено функції транснаціональних платіжних систем разом з такими відомими інструментами, як «VISA» та «PayPal». Відокремити такі дії від проявів кібертероризму чи навіть кібервійни доволі важко.

Уперше формально про ймовірність подібного розвитку подій було зауважено в дослдженні Групи експертів з розробки «Нової стратегічної концепції НАТО» [2]. У даному документі відзначається, що через збільшення рівня залежності сторін НАТО від ІТ-технологій і зростання кількості атак на інформаційну інфраструктуру, країни НАТО повинні цілком розважливо підійти до проблеми систематизації різновидів кібервійни, та ідентифікації її як дії, яка підпадає під Ст. 5 «Вашингтонського договору». Однак, незрозумілим є питання, чи допустимо розповсюджувати на даний неспецифічний тип воєн традиційне інтернаціональне «право війни», з одного боку, покликане попереджати виникнення війни як останнього засобу розв'язання міжнародних конфліктів із використанням збройної сили, а з іншого - налаштувати «війну за правилами», звести до мінімуму втрати поміж цивільного населення.

З міжнародно-правової точки зору актуально знайти відповідь на питання: чи можливо прояви кібератак у своєму контексті прирівняти до проявів «збройного насильства», котрі попадають під дію Ст. 2(4) «Статуту ООН», та чи можливо кібератаки уважати рівнозначними власне «збройним нападам», які попадають під дію ст. 51 «Статуту ООН». І основне питання: як розпізнати ситуації з міжнародно-правової точки зору, коли держава діє

у кіберпросторі з ціллю свого захисту від ситуацій, коли вона виступає агресором, а відтак, що значить в цьому контексті «міра припустимої самооборони». Незважаючи на той факт, що до останнього публічного варіанту «Нової стратегічної концепції НАТО зазначені питання так і не були внесені, а положення про зв'язок Ст.5 та «кібернападу» удруге було розглянуте на «Мюнхенській конференції з питань безпеки» у 2011 р. [3]. В даному ж спрямуванні відбулася конференція спільного американо-російського дослідження у галузі попередження та протидії кіберзагрозам «EastWest Institute» [4]. У доповіді йдеться про закономірність нормативного формулювання «правил війни» у кіберпросторі. Рекомендовано також внесення відповідних змін до Гаазької та Женевської конвенцій з врахуванням ймовірностей виникнення кібервоєн, позаяк існує брак юридично прийнятного формулювання того, що варто розуміти під кіберзагрозами та кібервійною як такими. Доречно зауважити, що і сама категорія «критична інфраструктура» сформульована далеко не у всіх державах, однак ідентифікована у США, де було прийнято ряд правових документів, що містили визначення «інформації про критичну інфраструктуру».

Отже, доповідь «EastWest Institute» закликає до визначення різного правового статусу у кіберпросторі для цивільних і військових об'єктів, а також забезпечення вищого рівня безпеки для «окремих основних доменів». Йдеться про розповсюдження власне на кібервійни положень «Женевських конвенцій» нового покоління та розвитку міжнародно-правових норм про захист жертв кібервійни.

Зазначимо, що Конвенція нового покоління покликана насамперед:

- надати особливого правового статусу країнам, що знаходяться у стані кібервійни;
- виділити «заборонені прийоми» кібервійни, зіставивши їх з міжнародно-правовими заборонами окремих винятково негуманних видів зброї;
- виділити мирні об'єкти кіберпростору воюючих країн від немирних об'єктів із застосовуванням особливих маркерів на зразок червоного хреста.

Першорядне питання, до котрого звертає увагу вище зазначений документ, - це перспектива законодавчого відокремлення об'єктів захищених в кіберпросторі від незахищених, аналогічно до того, як захистом міжнародних домовленостей користуються під час війни цивільні об'єкти. Автори документа радять встановити особливі кібермаркери на мітки захищених зон кіберпростору.

Крім того, міжнародним органам потрібно постановити, яку кібернетичну зброю (віруси тощо) необхідно вважати аналогом зброї, що заборонена «Женевським протоколом» (наприклад, ядерної).

Найскладнішим є питання ідентифікації «агресора», яке лишається нерозв'язаним навіть тоді, коли відношення до кібератаки урядових структур певних держав більшості видається безсумнівною (як це було під час атак на Україну у 2013-2014 р.р.). Багато фахівців доходять з даного висновку про кібервійну як «довгочасну холодну війну», котра буде мало схожою до звичайних війн з застосовуванням кінетичної летальної зброї [5]. До того ж, як наголошують фахівці ряду міжнародних організацій, географічною основою кібератаки є, зазвичай, зовсім не та країна, котрій така атака може бути об'єктивно потрібною.

Помітним перехідним періодом такого розгляду стала запропонована у 2011 році Адміністрацією Б. Обами «Міжнародна стратегія для кіберпростору» [6], в котрій безпосередньо йдеться про те, що США за собою лишають право на самооборону відповідно до принципів установчих документів ООН та у відповідь на небезпеку для інформаційної інфраструктурі США готові використовувати «інформаційні, дипломатичні, економічні та військові» прийоми для реагування на такого роду випадки. Керівництво США запропонувало даний документ як глобальну ініціативу і практично закликає прилучатися всім партнерам США до такого уявлення майбутнього кіберпростору. Документ теж зосереджує увагу на практиці США щодо вироблення міжнародних правил поведінки у кіберпросторі, а саме: «Цифровий світ уже не є простором беззаконня, полем для незначної групи еліти…Довгострокові міжнародні правила поведінки держав – в стадії миру та

конфліктів – використовувані й у кіберпросторі…Ми продовжимо працювати на міжнародній сфері з ціллю вироблення консенсусу щодо правил поведінки у кіберпросторі».

Зважаючи на вищезазначене, фігурують повністю справедливі гіпотези, що спроби впровадження в офіційний військовий дискурс категорії «кібервійна» призводитимуть до наступної деформації звичної системи світоустрою, девальвації урядових суверенітетів та стануть сучасною проформою вживання зброї в будь-якому пункті землі без врахування інтересів окремих країн. Швидше за все, уже найближчими роками безпековими організаціями кібервійну буде признано формою традиційної війни і здійснено належне співставлення з нормами ООН критеріїв кібервійни та звичайної війни. Кіберзброя та кібервійни підтверджують прагнення все більшої кількості держав реалізувати приватні проекти національного панування в кіберпросторі, нав'язати решті держав участь у сучасних цифрових змаганнях. Зазначимо, що вже у 1998 р. на такого роду небезпеку змагань інформаційних озброєнь засвідчувала в ООН офіційна російська делегація, котра запропонувала проект міжнародної резолюції, що був відхилений США та їх союзниками.

Найскладнішою на даний час є проблема щодо пояснення положень міждержавних конвенцій в умовах «поствестфальського» світоустрою, коли країни є зовсім не єдиними учасницями кіберконфліктів, а поруч з ними фігурує багато «мережевих громадян» та «насильницьких недержавних акторів», які діють в окреслених теренах кіберпростору. У даному контексті потребує правового переосмислення власне категорія «національної держави» у кіберпросторі.

Уряди провідних країн світу використовують різного роду кібератаки з метою пошкодження чи навіть ліквідації конфіденційної інформації або стратегічних ресурсів конкурентів та супротивників [7]. Якщо фігурує відповідна міжнародна конвенція, яка визначає космічний простір таким, що належить всьому людству, а не окремо взятій країні, і якщо простір повітряний над територією країни проголошується таким, що належить цій країні, то в інтересах світової спільноти є першорядним завданням власне нормативне визначення на міжнародному рівні категорій «кібербезпека», «кібервійна», «кіберзброя», «кібертероризм» та «кіберпростір».

Список використаних джерел:

1. Sommer P. Reducing Systemic Cybersecurity Risk [electronic resource] / P. Sommer , I. Brown // OECD/IFP Project on «Future Global Shocks». - Access: www.oecd.org/dataoecd/57/44/46889922.pdf

2. НАТО в 2020 году: Гарантированная безопасность, динамичное взаимодействие [Електронний ресурс]. – Режим доступу: http://www.nato.int/cps/ru/natolive/official_texts_63654.htm

3. Cyberspace Presents Complex Global Challenges [electronic resource]. - Access: http://www.securityconference.de/Program.425+M58b8d057766.0.html?&L=1

4. Working Towards Rules for Governing Cyber Conflict [electronic resource]. - Access: http://dl.dropbox.com/u/869038/US-Russia.pdf

5. The Ethics of Cyberwarfare.Detail Only Available By: Dipert, Randall R. // Journal of Military Ethics. - Dec2010. - Vol. 9; Issue 4. - P.384-410.

6. International Strategy for Cyberspace [electronic resource]. - Access: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

7. Якубівська Ю. Є. Світові тенденції розвитку кіберзлочинності / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія : Економічні науки. - К. : УДУФМТ, 2014. - № 5-6 (76-77). - С. 125-130.