УДК 327.5+351

СТРАТЕГІЯ І ПРАКТИКА КІБЕРБЕЗПЕКИ НАТО

Копійка М.В.
аспірантка кафедри міжнародних медіакомунікацій
і комунікативних технологій Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

Трансформація способів та засобів ведення воєн, поширення гібридних конфліктів та все більша залученість держав до інформаційного протиборства визначають кібербезпеку як одну з важливих складових безпеки міжнародних організацій, держав та національних спільнот. Найбільш впливовою міжнародною організацією, що розробила мережу центрів для протидії кіберзагрозам та дослідження інформаційних впливів, вважається НАТО, яка офіційно визнала кіберпростір операційним середовищем і прирівняла загрози, що там існують, до військових загроз. Організація сформувала передові центри НАТО як національні та багатонаціональні інститути, які допомагають у розробці доктрин кібербезпеки, вивчають попередній досвід, вдосконалюють можливості співпраці, затверджують теоретичні напрацювання та тестують їх за допомогою експериментів, а також навчають лідерів та фахівців країн-членів і країн-партнерів протидіяти кіберзагрозам. Центр кібербезпеки НАТО, який забезпечує боротьбу з кібератаками та кіберзахист інформаційних систем країн Альянсу, а також підготовку фахівців з протидії кібератакам наразі функціонує в Таллінні (Естонія). Створення центру відбулося саме за ініціативою Естонії, коли перші 7 країн-спонсорів уклали меморандум про взаєморозуміння щодо створення Центру, який згодом отримав акредитацію від НАТО. До формування Центру приєдналися й інші країни, також було укладено угоди про співпрацю з Європейською оборонною агенцією та Дослідницьким центром кібербезпеки у Мюнхені. Центр не вважається підрозділом військового командування або структури збройних сил НАТО, персонал та фінансування забезпечуються виключно державами-спонсорами та державами-учасниками [1].

Експертами Центру спільно з Організацією Червоного Хреста та Кібернетичним командуванням США було видано доповідь «Керівні принципи міжнародного права, що можуть бути застосовані під час кібернетичних війн» (Tallinn Manual on the International Law Applicable

to Cyber Warfare), або ж «Талліннські принципи», та «Талліннські керівні принципи 2.0», які вважаються керівними засадами щодо ведення кібервійна і які стосуються положень сучасного міжнародного право про регулювання операцій у кіберпросторі. За форматом «Талліннські принципи» складаються з 95 правил, розподілених на секції, до кожного правила подано юридичний коментар, яким пояснюється прив'язка визначеного принципу до чинних норм міжнародного права. Ключові висновки, зроблені експертами, містять положення про те, що держави несуть відповідальність за кібератаки проти інших держав, які ведуться з їх території; застосування сили в кіберпросторі є забороненим, оскільки здійснення кібератак призводить до руйнування інфраструктури, цифрових ресурсів та систем життєзабезпечення держав чи завдання шкоди окремим особам; застосування контрзаходів у відповідь на кібератаки є законним; за умови чіткої ідентифікації держави-нападника, держава, що зазнала кібератак, що призвели до людських жертв чи до інших серйозних втрат, має право застосувати силу у фізичному чи кіберпросторі; кібервійни дозволяється вважати «збройними конфліктами» і застосовувати норми міжнародного гуманітарного права; кібероперації, що залякують населення, заборонені; кібероперації, які призвели до жертв серед цивільного населення, вважаються військовими злочинами; атаки об'єктів, необхідних для виживання цивільного населення, заборонені. При цьому доповідь експертів є незалежною від документів НАТО та необов'язковою для виконання, оскільки представляє особисту думку авторів [2]

Водночас, констатується у документах організації, кіберзагрози безпеці Альянсу стають все частішими, складнішими, руйнівними та примусовими, тому НАТО та держави-члени і союзні держави покладаються на потугу кіберзахисту для виконання основних завдань Альянсу щодо колективної оборони, управління кризовими ситуаціями та спільної безпеки. Наразі, вважають в Альянсі, кібербезпека є одним з найголовніших пріоритетів для НАТО, оскільки «…гібридні атаки можуть зашкодити військовій і цивільній сфері життєдіяльності країн, зокрема економіці, транспортним системам, мережам комунікацій, а також енергетичній безпеці, тому заходи, схвалені протягом поточних років, сприятимуть ефективній регіональній безпеці у форматі НАТО» [3].

Основні принципи щодо вдосконалення кібербезпеки Північноатлантичного Альянсу були викладені у положеннях 2019 р., в яких підтверджено, що: кібербезпека є частиною основного завдання колективної оборони НАТО; НАТО підтвердило, що

міжнародне право застосовується в кіберпросторі; основна увага НАТО у контексті кібербезпеки стосується захисту власних мереж (включаючи операції та місії) та підвищення потужності Альянсу; 2016 р. союзники підтвердили оборонний мандат НАТО та визнали кіберпростір сферою операцій, в яких НАТО повинна захищати себе так само ефективно, як це відбувається в повітрі, на суші та в морі; союзники взяли на себе зобов'язання з кібербезпеки як пріоритетної сили, щоб покращити власний кіберзахист; НАТО розширюватиме свої можливості в галузі кібернавчання, моніторингу та інструментарію протидії кібератакам; союзники зобов'язані посилити обмін інформацією та взаємодопомогу у запобіганні, пом'якшенні та відновленні від кібератак; команди НАТО з питань швидкого реагування на кіберзагрози готові повсякчас надавати допомогу союзникам; 2018 р. союзники домовилися про створення нового Центру операцій в кіберпросторі в рамках посиленої командної структури НАТО; для захисту членів Альянсу НАТО може використовувати національні підрозділи кібербезпеки для своїх місій та операцій; 2019 р. союзники схвалили рекомендації НАТО, що містять низку інструментів для подальшого зміцнення здатності НАТО реагувати на значні шкідливі кібератаки; НАТО співпрацює з ЄС у форматі Технічній домовленості з кібербезпеки, яка була підписана 2016 р.; НАТО та ЄС, враховуючи спільні виклики для безпеки і оборони членів Альянсу, зміцнюватимуть співпрацю у сфері кібербезпеки, особливо щодо обмінів інформацією, навчання, дослідження та практики; НАТО активізуватиме співпрацю з діловими колами і приватним партнерством в галузі кібервиробництва; НАТО визнає, що його союзники можуть скористатися кіберпростором, заснованим на нормах, передбачуваним та безпечним [3].

Естонія як країна-член НАТО ініціювала заходи щодо співпраці у сфері кібербезпеки з країнами - учасниками Програми Східного партнерства, зокрема Україною та Грузією. До спільних дій віднесено передусім підготовку персоналу, технічні консультації та надання обладнання. Крім того, враховуючи рівень агресивних кібератак РФ проти України під час гібридної війни на Сході і незаконної анексії Криму, міністр оборони Естонії неодноразово закликав партнерів по НАТО надавати більше фінансової допомоги українській державі. Також Естонія виділила 100 тис євро в трастовий фонд НАТО для підтримки кібербезпеки України та здійснювала в рамках фонду навчання українських фахівців з кібероборони[4]. Наразі Україна має значний потенціал співпраці з центром як країна-партнер, оскільки може поділитися власним досвідом протидії російським кіберзагрозам

та деструктивним інформаційним впливам, що становлять загрозу й для демократичних процесів в європейському регіоні і на міжнародному рівні.

Список використаних джерел

1. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub [Електронний ресурс] – Режим доступу: https://ccdcoe.org/

2. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched [Електронний ресурс] // NATO CCDCOE. – 2017. – Режим доступу до ресурсу: https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html.

3. Cyber defence [Електронний ресурс] – Режим доступу: https:// www. nato. int/ cps/ en/natohq/topics_78170.htm

4. NATO launches cyber defence centre in Estonia [Електронний ресурс] – Режим доступу: http://www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html