УДК 327.5

МІЛІТАРИЗАЦІЯ КІБЕРПРОСТОРУ ЯК ЧИННИК АКТУАЛІЗАЦІЇ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИНАХ

Сябро А. В.
аспірантка кафедри міжнародної інформації
Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

Бурхливий розвиток інформаційних технологій та їх широке впровадження у всіх сферах життєдіяльності суспільства призвели до подальшої актуалізації проблеми інформаційної безпеки. Завдяки впровадженню сучасних технологій держави отримали можливості пришвидшити процеси модернізації суспільства шляхом реалізації програм електронного урядування, електронної комерції, дистанційних форм зайнятості тощо. Водночас, як показала практика розбудови інформаційного суспільства, технології, маючи подвійний характер використання, часто використовуються для протиправної діяльності або стають засобами протиборства у міждержавних суперечках і конфліктах. Таким чином, науково-технологічний розвиток призвів до появи нових викликів та загроз для системи підтримання міжнародного миру і безпеки. Показовою в цьому контексті є проблема мілітаризації кіберпростору, яка обговорюється як в експертних колах, так й на міжнародному рівні в рамках діяльності міжнародних міжурядових організацій, зокрема, ООН.

Досліджуючи проблему мілітаризації кіберпростору, науковці намагаються визначити передумови виникнення феномену. У сучасній літературі автори переважно використовують 2010 р. як межу, після якої держави розпочинають активно створювати кіберпотенціал для оборонних чи наступальних цілей (хоча використання кіберпростору у військових цілях розпочалося ще у Косовому). Саме у 2010 р. за допомогою вірусу Stuxnet відбулася масштабна атака на комп’ютерні системи заводу із збагачення урану в Натанзі, а також подальше гальмування строків запуску ядерної АЕС в Бушері. Таким чином, незважаючи на відсутність реальних матеріальних збитків від застосування кіберзасобів, держави відчули небезпеку, що може з’явитися у зв’язку із зростанням вразливості критичних елементів інфраструктури та потенційною можливістю використання кіберпростору для завдання удару по державі-супротивнику. Це призвело до масштабних трансформацій у системі оборони багатьох країн та дало поштовх до мілітаризації кіберпростору, оскільки значна кількість держав прийняли військові доктрини кібербезпеки, національні

стратегії кібербезпеки, створили спеціальні підрозділи, що займаються питаннями кібербезпеки у різних сферах військового протистояння або утворили так звані кібервійська, відповідальні за ведення воєнних дій у кіберпросторі або за кібероборону. Однак, як показують дослідження, з-поміж 114 держав, що мають доктрину і стратегію кібербезпеки, тільки 47 розробляють і реалізують саме військові програми, а решта 67 – виключно цивільні.

Слід також зазначити, що ступінь мілітаризації кіберпростору залежить не тільки від стратегічних цілей, але й від наявних ресурсів та потенціалу. Тому важливим напрямом дискусії є трансформація міжнародної політичної системи в умовах бурхливої інформатизації та віртуалізації міжнародного політичного простору. Так, аналізуючи появу так званої «кібервестфальської системи», науковці переважно розглядають питання нового виміру геополітичного протиборства – інформаційного, який передбачає врахування не тільки традиційних чинників, що визначають потугу держави, а й нетрадиційних – рівень наукового та технологічного розвитку держави в цілому, рівень кіберпотенціалу держави, рівень розвитку інтелектуального капіталу тощо. Отже, змінюються базові поняття традиційної геополітики, що призводить до трансформації уявлень про територію, національний інтерес, державний суверенітет та недоторканість державних кордонів, баланс сил тощо. Тому у новому геополітичному протистояння перемагає та держава, яка має високий кібепотенціал та активно використовує цю перевагу для просування власних національних інтересів на світовій арені. Таким чином, протистояння між державами доповнилося кіберпростором, що обумовило виникнення потреби розробки таких понять, як віртуальне поле бою, інформаційні озброєння, інтелектуальні бійці, а також розробку нових підходів до ведення бойових дій. Слід зауважити, що найбільш активними у пошуку нових методів протиборства виступають держави, між якими вже тривалий час існує конфлікт, і які використовують кіберпростір як засіб повідомлення про період ескалації напругі у протистоянні.

Важливим напрямом дослідження проблеми мілітаризації кіберпростору є вивчення взаємозв’язку між військовим суперництвом та стратегічними цілями держав-учасників протистояння. Це проявляється у впровадженні так званої «перегорнутої мілітаризованої дипломатії», що передбачає використання мілітаризованих активів (тобто кіберзброї) задля доступу до необхідних ресурсів, покладаючись при цьому на діяльність дипломатів, які повинні обмежити потенційну ескалацію протистояння. Таким чином, якщо об’єкт такої діяльності є вкрай важливим для захисту національних інтересів або для досягненні переваги у міждержавному протистоянні, то використання кіберзброї має передбачати усвідомлення

небезпеки викриття як держави-ініціатора використання інформаційних засобів протиборства, неможливості подальшого використання аналогічних засобів та потенційну можливість подальшої ескалації конфлікту у разі ідентифікації кібератаки.

Таким чином, незважаючи на наявність розбіжностей в оцінці феномену мілітаризації кіберпростору, більшість експертів вважає, що рівень та темпи мілітаризації кіберпростору держави залежать від кількості кібернападів або наступальних операцій у кіберпросторі проти неї. Важливим фактором також є ефективність реалізації національних стратегій інформатизації, оскільки масштаби використання кіберпростору формують залежність від гарантій його безпеки. Отже, чим вищим є рівень інформатизації держави, тим більше вона схильна до мілітаризації кіберпростору задля забезпечення національної інформаційної безпеки.