Секція: Національна безпека

Шаршаткін Данило Юрійович
старший викладач кафедри розвідки
Військова академія
м. Одеса, Україна

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Сьогодні все частіше актуалізуються проблеми державної та міжнародної інформаційної безпеки. З огляду на транснаціональну природу сфери інформаційно-комунікаційних технологій (ІКТ) найчастіше проблеми такого характеру не можуть бути вирішені на рівні окремих держав і вимагають міжнародних відповідей.

Сфера ІКТ характеризується анонімністю багатьох рядових учасників і відсутністю монополії держави на застосування «сили» в інформаційному просторі. Також варто зазначити високу потенційну загрозу застосування інформаційної зброї. Незважаючи на те що в багатьох передових країнах військові бюджети після завершення «холодної війни» скоротилися, витрати урядів на інформаційну безпеку активно ростуть. Це свідчить про високу значущість даної теми для держав різних рівнів.

Інформатизація загалом є однією з ключових характеристик сучасності. Через розвиток інформаційного сектору безліч сфер уже стали значно більш масштабними й конкурентними. Водночас політичне лідерство конкретних держав передбачає й інформаційне лідерство: якщо в 1990-х і початку нульових років інформатизація сама по собі бачилася дослідникам джерелом глибинних трансформацій в економіці держави, то сьогодні вона виступає в якості базової інфраструктури,необхідної для розвитку різних галузей бізнесу, суспільства й самої держави. На перше місце за ступенем впливу виходить похідна високого розвитку ІКТ - дані

користувачів, персональні дані та так звані великі дані (bigdata). Значущість даних сьогодні набагато перевищує значущість програмного забезпечення та технічної інфраструктури [1].

Рівень розвитку держави і його положення на міжнародній арені сьогодні значною мірою зумовлені рівнем його інформатизації. Розвинені країни істотно відрізняються за ступенем впровадження та ефективності експлуатації ІКТ. Це явище отримало назву «Цифровий розрив». Проблема цифрового розриву сьогодні перешкоджає реалізації економічного потенціалу ІКТ на міждержавному та глобальному рівнях. Цифровий розрив часто погіршує інші види нерівностей між державами - економічне, соціальне.

В останні роки в дослідницькій літературі все частіше з'являється поняття «балканізація Інтернету» - регіоналізація режимів управління Інтернетом. У свою чергу, це веде до виділення суверенних сегментів глобальної мережі. Межі цих сегментів можуть, як повторювати державні кордони, так і суперечити їм. Як правило, в основі логіки поділу й сегментації Інтернету лежать міркування щодо забезпечення державної інформаційної безпеки. Держави все частіше приходять в Інтернет інамагаються встановити правила гри на «ділянці відповідальності», яку вони вважають своєю.

У багатьох державах спостерігається створення спеціальних відомчих підрозділів, які офіційно декларують не тільки захист державних і комерційних комп'ютерних мереж і систем, але й можливість проведення атак на інформаційні об'єкти недружніх держав. Про наміри найяскравіше говорить той факт, що найчастіше такі підрозділи створюються в рамках військових і цивільних розвідок, а також збройних сил.

На сьогоднішній день на глобальному рівні все ще не з'явилося загальновизнане визначення інформаційної зброї та інформаційної війни. Насамперед це викликано термінологічними розбіжностями, які, зі свого

боку, викликані різницею інтересів держав і різницею в підходах до інформаційної безпеки. Термін «інформаційна війна» в більшості вітчизняних робіт має розширене тлумачення (інформаційна війна, як форма міждержавного протиборства) і використовується в іншому сенсі, ніж в американських військово-політичних і наукових колах. Західні дослідники схильні використовувати термін «кібервійна», яка обмежується впливом на комп'ютерні системи.

З метою уніфікації тут і далі ми будемо використовувати термін «інформаційна конфронтація», як найбільш широкий за змістом і нейтральний за характером. Під інформаційною конфронтацією ми будемо розуміти будь-які форми негативної взаємодії між суб'єктами в інформаційному поле - від дипломатичних нот і негативно забарвлених повідомлень засобів масової інформації до застосування кіберзброї та активних систем радіоелектронної боротьби (РЕБ) під час гібридного конфлікту.

Глобальна мережа стає важливим інструментом проекції влади держав на міжнародній арені: «м'якої сили» - з допомогою культурного та лінгвістичного впливу, «жорсткої сили» - завдяки кібератакам, кібершпіонажу і збору розвідувальних даних. Найбільш впливові гравці здійснюють управління через формування порядку денного, створення «правил» і параметрів мережі. Так, наприклад, починаючи з 2015 року у Росії ведеться цілеспрямована політика зі створення державного сегмента Інтернету.

У контексті цифрового парадоксу міць держав та його інформаційна інфраструктура знаходяться у небезпеці застосування інформаційної зброї. Цифровізація ключових сфер життя призвела до того, що вони теж перебувають під загрозою. Небезпека віддаленого злому може поставити під загрозу, як електроживлення окремого регіону (BlackEnergy:

відключення електроенергії в Україні у 2015 році), так і федеральну програму зі збагачення урану (Stuxnet: ядерна програма Ірану, 2010 рік).

На сьогодні критичні інформаційні та традиційні інфраструктури співіснують. Водночас в умовах формування цифрової економіки все більшого поширення набувають інформаційні інфраструктури, оскільки вони більш економічно ефективні, зручні та ергономічні. Отже, з кожним днем усе більше критичних інфраструктур стають інформаційними. Спроби виробити загальноприйняте визначення «критична інформаційна інфраструктура» (КІІ) на глобальному рівні поки що не має успіху.

Дослідники проблем інформаційної безпеки пропонують такий ряд визначень:

- інфраструктура - це набір окремих взаємопов'язаних елементів системи, що підтримують її функціональність і роботу за призначенням;
- критична інфраструктура - це комплекс окремих взаємопов'язаних елементів, що підтримують функціональність національно значущих для країни сфер життєдіяльності;
- критично важлива інформаційна інфраструктура - це сукупність програмно-апаратних, мережевих та інформаційних компонентів, що підтримують функціональність національно значущих для країни сфер життєдіяльності.

Характер міжнародної взаємодії щодо забезпечення інформаційної безпеки відображає більш масштабні процеси, притаманні всій міжнародній системі, зокрема тенденцію до регіоналізації, зростаючу рольнедержавних гравців, поява нових форматів міжнародної взаємодії. На сьогодні можна з упевненістю говорити про зростаючу сек'юритизації (у визначенні Б. Бузана) глобального інформаційного простору, як в Україні, так і в інших країнах, а також про суперечливі тенденції до регіоналізації інформаційного простору за його глобальній природі [2, с. 239].

Асиметричність потенційних заходів у відповідь збільшує ентропію можливої ескалації будь-якого конфлікту, навіть такого, що ґрунтується на чутках, підтасовці фактів або брехні. Зростає актуальність змін у міжнародно-правовій базі, що регулює відносини суб'єктів у інформаційному просторі, а також створення спеціальних правових інститутів, що володіють особливими компетенціями в області ІКТ. У зв'язку з цим вбачається правильним прийняття в Україні окремого закону, що регулює питання критичної інформаційної інфраструктури.

Природа держав, в основі якої лежить поняття про суверенітет і кордони, під час загального розвитку та цифровізації вступає в протиріччя з транскордонною природою ІКТ. На поточний момент складно оцінити ймовірність розвитку глобальної інформаційної кризи або інформаційної війни, але з певністю можна сказати, що по мірі цифровізації число інформаційних конфронтацій між усіма суб'єктами буде збільшуватися.

Література

1. Почепцов Г.Г. Далеке майбутнє, яке бачать військові, уряд і корпорації[Електронний ресурс] / Г.Г. Почепцов. — Режим доступу: http://informat.com.ua/uk/daleke-majbutnye-yake-bachat-vijskovi-uryadi-i-korporatsiyi.
2. Buzan B., Wæver O., De Wilde J [Text] / Security: a New Framework for Analysis // LynneRiennerPublishers,1998. — 239 p.