УДК 341.3

Ігор Сергійович Воєводін,
викладач кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

Кібервійна як сучасний метод ведення збройних конфліктів

Розділення дійсності на реальність і віртуальність, пов'язану з появою всесвітньої мережі Інтернет, у найближчі кілька років буде подолано і остаточно сформується єдина дійсність. Фактично це означає, що інформаційні технології будуть присутні повсюдно і будуть постійно використовуватись у всіх сферах побуту, соціальному, політичному, економічному житті, формуючи так званий «кіберпростір». В той же час, це передбачає нові ризики і нові види вразливості. Зокрема, мова йде про кібервійну – цілеспрямований деструктивний вплив інформаційних потоків у вигляді програмних кодів на матеріальні об'єкти та їх системи заради їх знищення, порушення функціонування або перехоплення керування ними [1].

Міжнародний Комітет Червоного Хреста під терміном «кібервійна» розуміє операції, за допомогою потоку даних, спрямовані проти комп'ютера або комп'ютерних систем, коли такі використовуються у якості засобу і методу війни в ситуації збройного конфлікту [2, с. 69].

Кібервійна викликає потенційну стурбованість з огляду на вразливість кібермереж і наслідки гуманітарного характеру, до яких можуть призвести кібератаки. Шкода, яка завдана фізичним особам, організаціям або об'єктам інфраструктури в результаті інцидентів у кіберпросторі, зокрема цілеспрямованих атак, може бути не менш істотною, аніж наслідки традиційних збройних конфліктів і зіткнень [3, с. 101].

Стосовно питання застосовності міжнародного гуманітарного права в кіберпросторі, слід зазначити, що переважно більшість його норм формувалася досить давно, коли людство навіть не уявляло можливість переведення війн у нову «кіберплощину» і автори текстів міжнародних конвенцій не могли описати правила поведінки, які б поширювали свою дію на ще не існуючий простір, новітній театр ведення війни.

Кіберконфлікти за своєю сутністю є унікальним явищем. По-перше, вони не пов'язані із застосуванням звичайної, кінетичної зброї, у зв'язку з чим достатньо складно визначити місце проведення бойових дій. Кібератаки можуть мати місце в різних місцях планети, знаходитися під юрисдикцією різних держав, а тому визначити театр ведення війни і обмежити цю територію на практиці виявляється вкрай складно. Іншою особливістю є складність у визначенні складу учасників, адже від цього залежить не тільки кваліфікація конфлікту, але й обсяг захисту, що надається кожній особі, визначення законних цілей для нападу і можливість притягнення до відповідальності [3, с. 101–102].

В 2013 р. Об'єднаним центром передового досвіду по кібероборонi НАТО було прийнято документ, відомий як «Таллінське керівництво щодо застосування юридичних норм міжнародного права до військових дій у кіберпросторі». Він став першим документом такого роду і закладає основи юридичного забезпечення застосування засобів ведення інформаційно-технічного протиборства у комп'ютерних мережах. Основний висновок полягає в тому, що згідно з існуючими поглядами, основоположні принципи міжнародного права застосовні до дій у кіберпросторі. Той факт, що комп'ютерні атаки в ході збройних конфліктів не мають безпосередньої динамічної, фізичної або насильницької форми не виводить їх за межі дії міжнародного гуманітарного права [4, с. 18]. Тобто кіберпростір нічим не відрізняється від інших сфер протиборства і не вимагає особливих підходів до його юридичного забезпечення.

У своїй доповіді за 2015 р. Група урядових експертів по досягненням в галузі інформатизації і телекомунікацій в контексті міжнародної безпеки ООН зазначила, що в процесі використання інформаційно-комунікаційних технологій держави зобов'язані керуватися принципами міжнародного гуманітарного права – гуманності, необхідності, пропорційності і вибірковості [5].

Таким чином такий феномен як кібервійна виводить міжнародно-правове регулювання збройних конфліктів на новий рівень складності, який може поставити перед міжнародним гуманітарним правом низку принципово нових питань. Доки немає спеціалізованого юридично обов'язкового міжнародного документу, який би регулював правила ведення війни у кіберпросторі, мають застосовуватися принципи та норми міжнародного гуманітарного права щодо пропорційності та

незастосування невибіркової зброї, проведення розмежування між військовими цілями і цивільними особами і недопущення віроломства.

Список бібліографічних посилань

1. Овчинский В., Ларина Е. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Книжный мир, 2014. 352 с.
2. Международное гуманитарное право и вызовы современных вооруженных конфликтов : доклад / подгот. Междунар. Комитетом Красного Креста. XXXII Междунар. конф. Красного Креста и Красного Полумесяца. Женева, Швейцария, 8–10 дек. 2015 г. 108 с.
3. Применение международного права в киберпространстве. *Индекс безопасности*. 2015. № 3 (114), т. 21. С. 101–118.
4. Гриняев С. Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве в оценках западных экспертов. *Обзор НЦПТИ*. 2015. № 3. С. 18–22.
5. Бойко С. М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее. *Международная жизнь*. 2016. № 8. С. 53–71.

Одержано 01.11.2019