УДК 341.4:004

Андрій Васильович Войціховський,
кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ

Кібератаки як елемент гібридної війни

Гібридна війна може розглядатися як більш досконалий або ефективний спосіб ведення війни, оскільки вона прагне досягти політичних цілей без широкого використання збройних сил та насильства. Особливістю гібридної війни є свідоме розмиття меж між війною і миром, вона не оголошується, її ініціювання зазвичай проходить непомітно. Використання цілого ряду інструментів гібридної війни, таких як кібератаки, заходи економічного впливу, інформаційні операції та обмежені фізичні атаки, які породжують невизначеність у широких верств населення, можуть бути достатніми для досягнення політичних цілей.

Одним із ефективних елементів гібридної війни є кібератаки. Вони направлені, насамперед, на дестабілізацію комп'ютерних систем держави. Міждержавні відносини і політичне протистояння інколи знаходять своє продовження в мережі Інтернет у вигляді окремих проявів втручання в комп'ютерні системи. Розглянемо лише декілька видів кібератак, що є елементами гібридної війни:

- вандалізм – атака, яка завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат. До таких кібернетичних атак можна віднести пошкодження вебсайтів державних органів і установ, заміну змісту образливими чи пропагандистськими малюнками тощо;

- пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення;

- збір інформації (кібершпигунство) – злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні;

- відмова сервісу – атаки з великої кількості комп'ютерів, основна мета яких є порушення функціонування сайтів або комп'ютерних систем;

- втручання в роботу обладнання – атаки на комп'ютери або сервери, які, наприклад, забезпечують роботу комунікаційних цивільних або військових систем, що призведе до відключення або виникнення помилок при обміні даними;

- атаки на об'єкти критичної інфраструктури – атаки на комп'ютери та системи, що забезпечують життєдіяльність населених пунктів і держави взагалі, а саме: системи водопостачання, електроенергії, транспорту тощо [1].

З розвитком інформаційно-комунікаційних технологій рівень і чисельність кібератак постійно зростає. Деякі держави почали приділяти значну увагу захисту від кібератак – розробляти необхідні засоби для організації системної оборони і захисту об'єктів критичної інфраструктури, а також формувати спеціальні підрозділи, основним завданням яких є забезпечення національної кібербезпеки.

Крім того, держави почали витрачати більше ресурсів на створення своїх кіберможливостей, і роль використання кібердомену (віртуальної сфери) неспинно зростає саме у військовій сфері. Такий стан речей свідчить про початок гонки цифрових озброєнь, де правила участі міжнародною спільнотою ще не кодифіковані.

Розвинені країни докладають значних зусиль для вироблення власної кібернетичної зброї, яка замінить за ефективністю класичну зброю (кулі, бомби, танки, літаки тощо). Такий сценарій розвитку військової стратегії вже стає реальністю. Так, наприклад, Міністерство оборони США відкрито заявляє, що вони створюють комп'ютерний код, здатний вбивати. Згідно з опублікованим посібником Міністерства оборони США про військові дії, операції із використанням кіберзброї можуть викликати такі загрози як знищення або пошкодження ядерної установки; відкриття дамби над населеним пунктом, що спричинить руйнування; відключення служби управління повітряним рухом, що спричинить аварії літаків тощо [2, с. 522].

У сучасних умовах розвитку інформаційного суспільства ефективна протидія кібератакам як проявам гібридної війни потребує не лише спільних зусиль розвинутих країн світу, але й розробку і здійснення максимально ефективних міжнародних інструментів. Тому всі економічні і політичні ресурси з протидії загрозам кібербезпеки повинні розглядатися на найвищому світовому рівні за участю основних кібердержав.

Забезпечення ефективної протидії кібератакам диктує важливість розробки, здійснення й удосконалення ефективних національних і міжнародних заходів:

- розробка державами ефективних моделей державної політики та національної концепції з кібербезпеки, що відповідають вимогам національної безпеки держав в контексті глобальних викликів та інших тенденцій сучасності;

- розвиток міжнародно-правових механізмів і загальної міжнародної політики по розробці і здійсненню ефективних інструментів з протидії кібератакам;

- налагодження і розвиток тісного співробітництва з НАТО, ОБСЄ, ЄС у галузі протидії різним проявам гібридної війти, у тому числі кібератака тощо.

Список бібліографічних посилань

1. Івахів Б. Кібертероризм як засіб ведення зовнішньої політики РФ // Free Voice Information Analysis Center : сайт. URL: http://iac.org.ua/kiberterorizm-yak-zasib-vedennya-zovnishnoyi-politiki-rf/ (дата звернення: 20.10.2017).
2. Кібербезпека як важлива складова всієї системи захисту держави // Міністерство оборони України : офіц. веб сайт. 07.05.2018. URL: http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (дата звернення: 26.10.2019).
3. Limnell J. The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War. *International Journal of Cyber-Security and Digital Forensics (IJCSDF).* 2015. Vol. 4, No. 4. P. 521–532. DOI: https://doi.org/10.17781/P001973.

Одержано 28.10.2019