Лакота О. В.,
студент,
Національний університет «Одеська юридична академія»

«КІБЕРВІЙНА» В ГЕОПОЛІТИЦІ ТА МІЖНАРОДНОМУ ПРАВІ

Нова інформаційна епоха вплинула на всі сторони суспільного буття. Тепер вже в інформаційному суспільстві домінують не традиційні галузі промисловості, а знання та інформаційні послуги.

Але разом з усіма позитивними моментами, які принесла інформаційна революція, інформаційна епоха зумовлює і нову суспільну відповідальність. Широкого розповсюдження набула так звана «кібервійна», яку можна визнати новою формою класичної війни з відповідними наслідками.

Адже в епоху інформаційної революції для досягнення цілей війни необов'язковим є введення військ, окупація, захоплення територій чи величезні військові витрати. Більш зручною є зброя «мережі», яка є новим четвертим простором після суходолу, моря й повітря.

Важливо також зазначити, що інтернет об'єднує практично весь світ, атака на мережу однієї держави може бути атакою на всіх.

Кібервійна **с**прямована насамперед на дестабілізацію комп'ютерних систем і доступу до інтернету державних установ, фінансових і ділових центрів, і створення безладу і хаосу в житті країн, які покладаються на інтернет в повсякденному житті.

В останнє десятиліття термін «кібервійна» все частіше використовується службовцями США. У більшості випадків під ним розуміються або систематичні напади на інформаційну інфраструктуру, або сукупність кібератак на інформаційні мережі держави.

Як приклад можна навести кібератаки на Америку з боку Ірану. В цьому випадку слід зазначити, що в інтернет-просторі була розпочата справжня війна, про що говорить масштаб дій. Вірус, який стер дані з 30 тисяч комп'ютерів, став найбільш руйнівним за всю історію приватного сектора.

Експерти підтвердили, що загроза виходила саме від Ірану. Метою атак стали не тільки комп'ютери американських відомств, але і корпоративні мережі в Саудівській Аравії. Головною ударною

одиницею вважались «кіберкопи», яких Міністерство оборони Іраку найняло в 2011 році у відповідь на кібератаки американських та ізраїльських спецслужб.

Також одним із яскравих прикладів кібершпигунства є масштабна операція GhostNet. Дана операція охопила 1295 комп'ютерів, третина яких знаходилась в посольствах, міжнародних організаціях, міністерствах. В кібершпигунстві підозрювали уряд Китаю [1].

Поступово світове співтовариство починає усвідомлювати, що кіберпростір перетворюється у поле боротьби, що потребує розробки відповідної стратегії національної та міжнародної безпеки. У зв'язку з розповсюдженням такого явища, як кібератаки постало нагальне питання вирішення даної проблеми, закріпивши певні норми в міжнародних документах.

Щодо нормативного закріплення даного поняття, то слід навести як приклад документ під назвою «Талліннське керівництво з ведення кібервійни», розроблений Об'єднаним центром передового досвіду з кібероборони НАТО. З нього випливає, що кібератаки за силою впливу слід прирівняти до хімічної, біологічної та радіологічної зброї.

Важливим кроком у формування національної системи кібербезпеки стало ухвалення у травні 2011 р. «Міжнародної стратегії розвитку кіберпростору».

У ній викладено не тільки основні підходи до розуміння сучасної глобальної американської політики, але й представлено нові офіційні позиції Сполучених Штатів з питань інформаційної безпеки. У Стратегії також підтверджено лідерські позиції США в інформаційному розвитку, інформаційний потенціал сприймається американським політичним керівництвом як стратегічний ресурс.

В липні 2011 р. було оприлюднено ще одну стратегію кібербезпеки США «Стратегію Міністерства оборони США у сфері кіберпростору». Всесвітня мережа тепер офіційно визнана «полем бою», таким саме як суша, море, повітряний простір або космос.

Стратегія Міністерства оборони передбачає реалізацію п'ятьох стратегічних ініціатив:

1) визначення кіберпростору як самостійної галузі, поля оперативної діяльності;

2) використання тактики «активного захисту»;

3) координація дій з міністерством внутрішньої безпеки щодо стратегічно важливих та інфраструктурних мереж;

4) співробітництво у галузі кібербезпеки з партнерами і союзниками;

5) протидія кібертерористичним атакам через глобальну мережу [2].

Цікавим є те, що напередодні офіційного представлення документу з'явилися повідомлення у ЗМІ про те, що у новій кіберстратегії США буде міститися пункт про те, що кібератака, яка призвела до людських жертв, буде прирівняна до оголошення війни. Але в офіційному тексті Стратегії така норма відсутня, напевно, уряд США не був готовий на такий радикальний крок.

Серед країн, які вже давно розробляють доктрину «інформаційної війни» є Китай. Інформаційну війну китайські офіційні документи визначають як перехід від механізованої війни, яка є характерною для індустріального суспільства, до війни знання й війни інтелекту.

КНР ставить за мету створити до 2020 р. «найбільш інформатизовану» армію у світі, які вони прозвали «мережеві сили», тобто військові підрозділи, укомплектовані висококваліфікованими фахівцями, що володіють комп'ютерними технологіями. Основною інформаційною зброєю китайських хакерів є «шкідники»– заражені комп'ютерні коди [3]. Отже, міждержавні відносини і політичне протистояння часто знаходить продовження в інтернеті у вигляді кібервійни. Країни або окремі громадяни, причетні до інформаційних атак, повинні понести суворе покарання і міжнародний осуд.

ЛІТЕРАТУРА:

1.Проблеми кібервійни та кібербезпеки в міжнародному праві [Електронний ресурс]. – Режим доступу: www.politik.org.ua/vid/publcontent.php3?y=7&p=58&setcss=1&ncss=big

2.Department of Defense Strategy for Operating in Cyberspace [Електронний ресурс]. – Режим доступу: www.defense.gov/news/d20110714cyber.pdf.

3.Леонов О. В. Інтернет як інструмент ведення кібернетичної війни [текст]: / О. В. Леонов // Стратегічна панорама. – 2002. – № 3. – С. 122-127.