Осадчук Михайло, студент групи КІ-11

КІБЕРВІЙНИ – РЕАЛЬНІСТЬ НАШОГО ЧАСУ.

За вікном XXI століття і людство не може уявити собі життя без технічних засобів комунікації. Тому не дивно, що інформація та інформаційні потоки можуть використовуватися в деструктивних цілях. Інформаційні технології докорінно змінили спосіб ведення військових операцій. У цей час війни ведуться здебільшого за моніторами комп'ютерів. З кожним днем загроза «кібервійни» зростає, а «кібертероризм» не є рідкістю. Тому цю проблему потрібно розглянути з політологічної концептуалізації.

Проблема кіберзагрози набирає обертів серед обговорень політиків, міжнародних військових, медичних та навіть аерокосмічних організаціях [6]. Взагалі термін «кібервійна» міцно увійшов у лексикон військових, фахівців з інформаційної безпеки, політиків.

Кібервійна́ (англ. Cyber-warfare) — комп'ютерне протистояння у просторі Інтернету. Тобто можна зробити висновок, що «кібервійна» є в першу чергу різновидом військових дій, яка несе загрозу автоматизованим системам, радіостанціям, електростанціям, оборонним установам. Іншими словами кілька успішних «кібератак» можуть знищити економіку та боєздатність країни. Прикладом «кібератаки», яка увійшла в історію, є виведення з ладу системи управління ППО Іраку під час операції «Буря в пустелі». Спецслужбам США вдалося заразити спеціальними вірусами комп'ютерну систему з пам'яті принтерів, придбаних для цієї системи у однієї комерційної фірми [6]. На цьому прикладі ми бачимо і мусимо усвідомити, що «кібервійна» - це гірка реальність. Або «кібератака» «Petya.A» 2017 року, яка вивела зі строю близько 18 млн. Інтернет – користувачів та тисячі організацій у тому числі і сервера оборони в Україні, Литві, Білорусі [1] . А з 2014 року по сьогодні ведеться досить серйозна сутичка у «кіберпросторі» між РФ та Україною. [1]

Експерти оборони США, Німеччини, Франції, Британії та КНР розуміють, що мілітаризація глобальної мережі є найбільш небезпечним розвитком «кіберпростору». Так, помічник генерального секретаря НАТО зпитань безпеки Сорін Дукару вважає, що успішне протистояння «кібератакам» – це один з найголовніших викликів, які кидає Альянсу сучасний світ, який наповнений різними інформаційними та комп'ютерними технологіями. Дукару стверджує, що країни НАТО повинні відповідати недружнім країнам «кібератаками» [5] . Країни, які усвідомили, що війна через монітор може нанести не менш сильний удар ніж збройне протистояння створили структури у збройних силах, які відповідають за «кібербезпеку» та «кібервійну». Найкращі «кібервійська» знаходяться у КНР. За даними американської компанії, яка стоїть за інформаційною цифровою безпекою, Mandiant, на 2013 рік збройні сили КНР провели понад 100 «кібератак» на американські компанії та організації. А за ствердженням німецького експерта Сандро Гейко в Китаї знаходяться 15 тис. штатних хакерів [3] . У 2010 році у США та слідом у інших країнах було створено «кіберкомандування». З 2011 року діє «Стратегія операцій в кіберпросторі міністерства оборони США», даний документ містить набір «стратегічних переваг в кіберпросторі», до яких відносяться оперативний зв'язок і можливості обміну інформацією, здійснення експертиз у сфері кібербезпеки. Попри створення структур інформаційної безпеки атаки так і не зменшились і поесли за собою наслідки [9].

Компанії «Center for Strategic» та «International Studies» оцінили завдану шкоду кіберзлочинності за 2014 рік у розмірі 445 млрд. доларів. Найбільше від «кіберзлочинців» страждають США, Німечина, Японія, Британія, КНР [2]. Економіки цих країн щороку втрачають близько 200 млрд доларів. Єврокомісія повідомила, що за даними на 2014 рік, мінімум 1 млн користувачів Інтернету щодня піддається «кібератакам». А сукупний збиток для бізнесу від діяльності «кіберзлочинців», за різними оцінками, становить від 89 до 250 млрд євро на рік [2].

Таким чином, У 2017 загроза у «кіберпросторі» має бути взята до уваги та розглянута з точки зору загрози безпеки не тільки для країн, а й людства загалом. Тому ця проблема потребує якнайшвидшого вирішення та регулювання на міжнародному рівні, адже за

«кіберзброєю» не можна прослідкувати. Одним із вирішень цієї проблеми може бути створення плану реагування на «кіберзагрозу».

Література

1. *Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=3233.*
2. *Госучреждения Германии страдают от хакерских атак [Електронний ресурс]. - Режим доступу: http://www.dw.de/госучреждения-германии-страдают-от-хакерских-атак/a-16691699.*
3. *Ковалёв Н. «Началась новая техногенная эпоха – с кибервойнами, кибертерроризмом, киберпреступностью» [Електронний ресурс] / Н. Ковалёв // Интервью для интернет-газеты «Столетия». – Режим доступу: http://qps.ru/odR7k.*
4. *Мировая экономика теряет 445 млрд долларов из-за «киберпреступков» [Електронний ресурс]. - Режим доступу: http://www.dailycomm.ru/m/27316/.*
5. *Пора вырабатывать правила ведения кибервойн [Електронний ресурс]. - Режим доступу: http://www.psj.ru/press/detail.php?ID=73634.*
6. *Савин Л. Холодная кибервойна [Електронний ресурс] / Л. Савин // Информационно-аналитический портал Геополитика. – Режим доступу:http://www.geopolitica.ru/article/holodnayakibervoyna#.VUAFU9Ltmkp.*
7. *Томахів В.Я. Політологія. Навчальний посібник, 2-ге вид., доп / В.Я. Томахів. — Тернопіль: ТНЕУ, 2017. — 183 с. [Електронний ресурс] - Режим доступу: https://www.twirpx.com/file/2364502/*
8. *Чигур, Р. Ю. Феномен глобалізації: соціально-філософський аналіз / Р. Ю. Чигур // Наукові записки Національного університету «Острозька академія»: Серія «Філософія», Острог, 2015.– Випуск 18.– С. 96-102*
9. *Эдуардо Феббро Кибервойна между Россией и Западом («Pagina 12», Аргентина) [Електронний ресурс] / Э. Феббро. – Режим доступу: http://inosmi.ru/world/20140930/223333408.html.*
10. *Гончарук, Т. В. Філософія сучасного українця у форматі інноваційного суспільства / Т. В. Гончарук // Наукові записки. Сер. Філософія. – Острог : Національний університет «Острозька академія», 2011. – Вип. 9.*