СЕКЦІЯ 3. ОСНОВНІ НАПРЯМИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНОГО, ФІНАНСОВОГО, МОРСЬКОГО ТА ІНФОРМАЦІЙНОГО ПРАВА

Басалюк Наталія Василівна
студентка V курсу
судово-адміністративного факультету
Національного університету «Одеська юридична академія»

ІНФОРМАЦІЙНО-ТЕХНІЧНА ВІЙНА Й КІБЕРТЕРОРИЗМ: ПОНЯТТЯ, ОСОБЛИВОСТІ

Глобальна інформатизація зробила світове співтовариство, цілісність якого багато в чому забезпечується, в тому числі, за рахунок інтенсивного інформаційного обміну, більш вразливим – зупинка інформаційних контактів навіть на короткий час здатна призвести до кризи державного або навіть міжнародного рівнів. Інформаційна цивілізація здійснила трансформацію поняття «агресія», яке набуло форм і особливостей «агресії інформаційної».

Під інформаційно-технічною війною М.А. Радіонов та В.С.Пірумов вбачають форму боротьби сторін, що ведеться з використанням спеціальних засобів і методів впливу на чужі інформаційні ресурси при захисті свого інформаційного капіталу [3]. Надаючи власне визначення цьому поняття, зазначмо: інформаційно-технічна війна – будь-який тип інформаційного впливу із застосуванням інформаційної зброї, покликаний порушувати нормальне функціонування інформаційної інфраструктури (дезорганізація роботи технічних засобів, долання системи захисту, обмеження доступу законних користувачів) з можливістю подальшого несанкціонованого збору, копіювання, блокування, видалення інформації. Легального визначення дефініції немає, натомість, у Законі України «Про основні засади забезпечення кібербезпеки України» дано визначення поняттю «кібер-атака». Якщо вважати, що інформаційно-технічну війну характеризує застосування декількох кібератак, то можна сказати, що законодавець все ж підібрався до визначення цього широкого поняття. Серед форм інформаційних атак виділяють: 1) активну атаку, в результаті якої фактично змінюються чи знищуються збережені чи оброблені дані чи інші елементи ресурсу; 2) асинхронну атаку, при якій використовуються переваги динамічної дії системи, що дає змогу керувати вибором часу виконання тих чи інших дій; 3) контрольовану атаку, що направлена на основний потік повідомлень у мережі Ethernet (протокол кабельних комп'ютерних мереж) і

подальшу зміну рухів для повідомлень певного виду з певними ознаками (наприклад такими, що містять конкретні паролі); 4) пасивну атаку, при якій знімається обмеження на доступ до даних чи змінюється форма контролю за доступом до них [2].

Особливостями інформаційно-технічної війни є складність ідентифікації джерела агресії, контрольоване, дозоване нанесення шкоди, припинення дії після повного досягнення цілей, непередбачуваність наслідків – потенційно кібератака проти якої-небудь держави може спровокувати масштабний уже міжнародний конфлікт, оскільки відповідь сторони, що постраждала може бути непропорційною.

В арсеналі інформаційної зброї театру військових дій комп'ютерні віруси, логічні бомби (команди, заздалегідь вбудовані у програму, що спрацьовують у потрібний момент), фальсифікація інформації, засоби нейтралізації тестових програм й різного роду помилки, що свідомо вводяться у програмне забезпечення [4].

Інформаційно-технічну війну не слід ототожнювати із інформаційним терористичним актом. Легальне визначення поняття «кібертероризму» міститься у Законі України «Про основні засади забезпечення кібербезпеки України», де під ним розуміється терористична діяльність, що здійснюється у кіберпросторі або з його використанням. Свої підходи до виокремлення сутнісних ознак даного явища виробила й юридична доктрина. Так, В.А. Голубєв під кібертероризмом розуміє умисну атаку на інформацію, комп'ютерну систему чи мережу, яка створює небезпеку для життя і здоров'я людей чи може призвести до настання інших тяжких наслідків, якщо такі дії були скоєнні з метою порушення суспільної безпеки, залякування населення чи провокації воєнного конфлікту [1]. Аналіз джерел дозволяє дійти висновку, що при трактуванні даної дефініції науковці так чи інакше наближаються до законодавчого визначення терористичного акту, викладеного у ст. 258 Кримінального кодексу України. Усі вони зосереджують увагу саме на меті цього виду кіберзлочину, яка залишається тотожна звичайному терористичному акту.

Засоби здійснення інформаційно-терористичних дій можуть варіюватися у широких межах і включати усі вищеперелічені види інформаційної зброї. У той же час тактика й прийоми інформаційного терору суттєво відрізняються від тактики інформаційно-технічної війни й прийомів інформаційного криміналу. Для кібертерориста головне, щоб дії мали небезпечні наслідки, стали широко відомими населенню й отримали суспільний резонанс.

Як й інформаційно-технічна війна, кібертеракт не має державних меж, кібертерорист може рівною мірою створити загрозу інформаційним системам, розташованим у будь-якій точці земної кулі. Виявити й нейтралізувати віртуального терориста практично неможливо через малу

кількість залишених ним слідів. На відміну від звичайного терориста, який для досягнення своєї мети використовує вибухівку, у руках кібертерориста – сучасні інформаційні технології та необхідний рівень технічної підготовки для запуску кібербомби.

Як бачимо, сучасна науково-технічна революція породила нові форми конфліктів: інтенсивні, небезпечні, масштабні. Сьогодні у боротьбі за сфери економічного й політичного впливу акцент із застосування фізичної сили усе більше зміщується на бік прихованих і гнучких форм агресії, у числі яких – інформаційні війни й кібертероризм.

Список використаних джерел:

1. Голубев В.А. Кибертерроризм – узроза национальной безопасности [Электронный ресурс]. – Режим доступа: http://www.crimeresearch.ru/articles/Golubev_Cyber_Terrorism/2. – Назва з екрану.

2. Информационная война и защита информации. Словарь основных терминов и опередедений. – Москва. – 2011. – 68 с.

3. Пирумов В. С., Родионов М. А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. 1997. № 5. С. 44-47.

4. Расторгуев С.П. Информационная война /С.П.Расторгуев// М.: Радио и связь – 1999. – 222 с.

Науковий керівник: к.ю.н., доцент Міщенко І.В.

Брачук Анастасія Олегівна
аспірант кафедри морського та митного права
Національного університету «Одеська юридична академія»

КОНЦЕПЦІЯ СПРИЯННЯ ТОРГІВЛІ: ВИЗНАЧЕННЯ ПОНЯТТЯ

У найбільш загальному вигляді поняття «сприяння торгівлі» прийнято розглядати, як «зниження торговельних витрат», які представляють собою «різницю між витратами на внутрішню та зовнішню торгівлю, іншими, ніж витрати, що відносяться до традиційних засобів зовнішньоторговельної політики, таких як імпортні мита» [1, 3].

Таким чином, термін «сприяння торгівлі» чітко прив’язується до міжнародної торгівлі, і повинен описувати заходи, спрямовані на зменшення витрат, обумовлених саме міжнародним характером такої торгівлі. При цьому, він чітко розмежовується із питаннями лібералізації торгівлі, які охоплюють застосування тарифних та нетарифних бар’єрів. Власне кажучи, увага до питання сприяння міжнародній торгівлі багато у