

УДК 316.485.26 «19/20»

І.В. РОЗНАТОВСЬКИЙ

КІБЕРТЕРОРИЗМ: ПРОБЛЕМА ВИЗНАЧЕННЯ

Рознатовський Ігор Валерійович – асистент кафедри філософії та соціології Луганського національного університету імені Тараса Шевченка

Розглядається кібертероризм як відносно новий вид терористичної діяльності. Терористичні угруповання використовують Інтернет не тільки для особистого листування і пересилання різного роду інформації, за допомогою Інтернет-технологій терористи на якісно новому рівні організують свою діяльність. У зв'язку з відсутністю єдиного визначення кібертероризму автор пропонує універсальне визначення цього соціального явища, спираючись на ряд уже існуючих у науці визначень.

Ключові слова: кібертероризм, терористична діяльність, Інтернет-технології, комп'ютерні мережі.

Рассматривается кибертерроризм как относительно новый вид террористической деятельности. Террористические группировки используют Интернет не только для личной переписки и пересылки различного рода информации, с помощью Интернет технологий террористы на качественно новом уровне организуют свою деятельность. В связи с отсутствием единого определения кибертерроризма, автор предлагает универсальное определение этого социального явления, опираясь на ряд уже существующих в науке определений.

Ключевые слова: кибертерроризм, террористическая деятельность, Интернет-технологии, компьютерные сети.

The article examined cyberterrorism as a relatively new kind of terrorist activity. The author points out that terrorist groups use Internet not only for personal correspondence and sending different kinds of information, with the help of the Internet technologies terrorists at a qualitatively new level organize their activities, which, by the way, often leaves traces and help secret services to fight terrorists' organizations. Due to lack of a unified definition of cyberterrorism, the author creates a universal definition of this social phenomenon, based on a number of existing scientific definitions.

Keywords: cyberterrorism, terrorist activity, Internet-technologies, computers' networks.

© І.В. Рознатовський, 2012

Наприкінці ХХ століття вокабуляр соціологів і правоохоронців поповнився новим терміном, який визначав протиправні діяння в системі Інтернет як кібертероризм. По мірі того як зростала частка використання комп'ютерів і технологій з ними пов'язаних, зростала і спокуса серед кримінальних елементів та угруповань, у тому числі і терористичних, використовувати в своїх цілях нові блага цивілізації.

Постановка проблеми. Хто такий кібертерорист і якими критеріями слід керуватися, щоб кваліфікувати протиправне діяння, пов'язане з комп'ютерними системами і мережами, як кібертероризм? Джон Девіс, особа відповідальна за кіберзахист у Пентагоні, кажучи про характер кібератак зауважив, що тут представлений весь спектр: «від витівок нудьгуючого підлітка, до погроз національного масштабу» [8].

Аналіз останніх досліджень і публікацій. Так само як у такого соціального явища, як «тероризм» немає чіткого наукового визначення, так немає такого визначення і в його різновиді як «кібертероризм». Розглянемо ряд визначень кібертероризму. У своїх статтях «Кибертерроризм как новая форма терроризма» та «Кибертерроризм – миф или реальность» [«Кибертероризм як нова форма тероризму» і «Кибертероризм – миф чи реальність» (переклад авт.)] Голубев В.А. пише: «Під комп'ютерним тероризмом (кібертероризмом) слід розуміти умисну, політично вмотивовану атаку на інформацію оброблювану комп'ютером, комп'ютерну систему і мережі, яка створює небезпеку для життя і здоров'я

людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту. Під комп'ютерним тероризмом (кібертероризмом) слід розуміти залякування населення та органів влади з метою досягнення злочинних намірів» (переклад авт.) [2].

У словниках Yandex знаходимо таке визначення кібертероризму: «Кібертероризм (кібервійна) – напади на комп'ютери за допомогою несанкціонованого доступу, які здійснюються з метою саботувати роботу відповідних установ» (переклад авт.) [5].

Оксфордський словник пропонує таке визначення: «Cyberterrorism – the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society...» [10]. [Кібертероризм – політично вмотивоване використання комп'ютерів та інформаційних технологій для того, щоб викликати в суспільстві хвилювання і страх (переклад авт.)].

Мета дослідження. Метою запропонованої статті є, на основі ряду визначень, формулювання нового універсального визначення кібертероризму.

Виклад основного матеріалу дослідження. Наведені вище визначення багато в чому різняться один від одного і за змістом, і за обсягом, навіть перше визначення Голубева В.А., яке виведене на основі статті 258 Кримінального Кодексу України, не є вичерпним і «завдяки» витіюватим юридичним виразам заводить у глухий кут процес кваліфікації діяння як акту кібертероризму.

Наприклад, широковідомі в даний час хакери під загальною назвою Anonymous – хто вони: кібертерористи або так звані «моральні хакери» («У деяких випадках хакери можуть з власної ініціативи підтримувати правоохоронні органи в боротьбі проти особливо підлих злочинців. Наприклад, групу під назвою «Моральні хакери проти педофілії» було створено для виявлення і сприяння притягненню до відповідальності осіб, які публікували в Інтернеті дитячу порнографію» [6, с. 50-63]), або це хакери, об'єднані антиглобалістськими чи анархістськими поглядами?

Anonymous – група Інтернет-користувачів без постійного членства і складу. Група часто здійснює всілякі акції протесту в Інтернеті. Всесвітню популярність група отримала завдяки проекту «Чанологія», який був спрямований проти церкви саєнтології та активних дій в підтримку торрент-трекера Pirate Bay. Починаючи з 2008 року, групу Anonymous все частіше пов'язують з міжнародним хакерством, завдяки проведенню акцій протесту в Інтернеті, з метою підтримки свободи слова в глобальній мережі. Дії, відповідальність за які беруть на себе Anonymous, здійснюються не ідентифікованими особами, які використовують термін Anonymous в якості атрибуту [9].

Щоб найбільш коректно визначити – яке протиправне діяння в комп'ютерній сфері є проявом кібертероризму, треба визначити для здійснення яких цілей можуть бути використані Інтернет-технології терористами. «По-перше, вони можуть допомагати їм у впливі на громадську думку та у пропагандистській діяльності. По-друге, такі технології можуть використовуватися для нападів на віртуальні цілі з метою їх зруйнувати. І останнє: ІТ можуть використовуватися для нанесення фізичної шкоди» [5, с. 50-63].

Терористичні угруповання використовують Інтернет не тільки для особистого листування і пересилання різного роду інформації, за допомогою Інтернет-технологій терористи на якісно новому рівні організують свою діяльність. Що, втім, часто грає не на їхню користь, бо така активність у мережі залишає «сліди», що, в свою чергу, допомагає спецслужбам боротися з терористами. Що ж стосується ведення серйозної підривної та розвідувальної діяльності терористами, наприклад атака на сервери Пентагону чи іншої великої державної структури, то тут терористів необхідно мати достатній рівень знань і досвід у даній сфері, чого часто немає.

Вихід із ситуації, що склалася, – залучення комп'ютерних фахівців зі сторони – найманців. У такому випадку фахівець, якого тимчасово залучено (з меркантильних або ідейних причин) до роботи у терористичній організації може бути визначений як кібертерорист. Інакша справа в тому випадку, якщо програміст виконує вказівки терористів під загрозою розправи над ним самим або його рідними й близькими, тут він, програміст, сам є жертвою.

Висновки. Повертаючись до проблеми визначення кібертероризму, зробимо наступний висновок: кібертероризм – проведення або погроза проведення хакерських атак на комп'ютери, сервери або

комп'ютерні мережі держустанов і підприємств, які супроводжуються висуненням вимог з боку сторони, яка бере на себе відповідальність за скоєння кібератаки. Ступінь та характер втрат та пошкоджень від проведення кібератаки або погрози її проведення має впливати на визначення міри відповідальності кібертерориста за скоєне протиправне діяння.

До наведеного визначення ми не включили такі діяння, як наприклад створення сайтів в Інтернет для терористичних організацій (як свідчать статистичні дані приблизно 80 % терористичних організацій мають свої інтернет-сайти) [4, с. 27], написання шкідливих програм (вірусів), або будь-яка пряма чи опосередкована допомога терористичному угрупованню (за винятком безпосереднього скоєння кібератаки). На нашу думку, це можна кваліфікувати як сприяння терористичній діяльності.

Безумовно, існує скептичне ставлення до проблеми кібертероризму, яке базується на ряді причин, а саме:

- Незважаючи на постійно зростаючу частку Інтернет-технологій у різних сферах життєдіяльності суспільства, їх частка все ще залишається незначною. Відносно українських реалій, то тут впровадженню Інтернет-технологій у систему народного господарства і державного адміністрування перешкоджає сама влада, а точніше – корумпована бюрократія, що стоїть при владі, тому що Інтернет-технології значно обмежать можливість застосування корупційних схем. Наприклад, у системі електронних платежів України скотилася з 42-го на 60-е місце за останні 5 років. «Низькі темпи розвитку електронних платіжних систем в Україні, на думку експерта з питань України The Economist Intelligence Unit Тобі Ілза, обумовлені недостатньо розвинутою для цього інфраструктурою і загальною технологічною відсталістю, а також невисоким рівнем ВВП» (переклад авт.) [1].

Але треба зазначити, що професійний рівень українських фахівців у сфері ІТ-технологій високий, що гіпотетично може викликати зацікавленість у представників терористичних угруповань щодо залучення цих фахівців до роботи на свою користь.

- Підривна діяльність у системі Інтернет і в комп'ютерних мережах все ж залишається досить складною з технологічної точки зору. «У 2010 році представники Пентагону заявляли, що США витратили на захист оборонного відомства від хакерів близько 100 мільйонів доларів» (переклад авт.) [7].

- Важливим фактором є те, що кібератаки, як правило, не викликають бурхливої реакції з боку ЗМІ, на відміну від терактів, пов'язаних з підривами, взяттям заручників і т.д., а публічність терористичних атак для самих терористів часто є самоціллю.

- І нарешті, стосовно терористичної активності в Україні в цілому, то, згідно з GTI (Global Terrorism Index), який було розроблено британською дослідницькою організацією World Markets Research Centre, Україна входить до групи країн з найменшим рівнем терористичних загроз [3, с. 7].

Висновки. На думку скептиків, проблема кібер-

тероризму занадто роздута, і необхідна лише для того, щоб тримати суспільство в страху і відповідно його контролювати і для отримання додаткових бюджетних асигнувань. З цією позицією не можна не погодитися, частково звичайно. На нашу думку

кібератаки вже є фактом доведеним і є постійною терористичною практикою і, безумовно, їх кількість і якість будуть постійно зростати, до чого потрібно бути готовим як у технологічному, так і в правовому аспектах.

ЛІТЕРАТУРА:

1. В рейтинге стран по уровню внедрения электронных платежей Украина за последние пять лет скатилась с 42-го на 60-е место [Электронный ресурс]. – Режим доступа: <http://finance.eizvestia.com>.
2. Голубев В. Кибертерроризм как новая форма терроризма [Электронный ресурс] / Владимир Голубев. – Режим доступа: http://www.crime-research.org/library/Gol_tem3.htm.
3. Гребенчук Ю.Л. Терроризм и экстримизм / Ю.Л. Гребенчук // Медиа, терроризм и европейская интеграция / под ред. Ю.Л. Гребенчука. – К.: ЦСЭИ «Диаматик», 2007. – С. 7.
4. Дерех І.А. Медіа і тероризм / І.А. Дерех // Медиа, терроризм и европейская интеграция / под ред. Ю.Л. Гребенчука. – К.: ЦСЭИ «Диаматик», 2007. – С. 27.
5. Кибертерроризм [Электронный ресурс]. – Режим доступа: <http://slovari.yandex.ru>.
6. Мережі і мережні війни: Майбутнє терору, злочинність та бойові дії / Джон Ар-квілла, Девід Ронфельдт; пер. з англ. А. Іщенко. – К.: Вид. дім «Києво-Могилянська акад.», 2005. – С. 50-63.
7. НАТО потратит 67 миллионов долларов на кибербезопасность [Электронный ресурс]. – Режим доступа: <http://lenta.ru/news/2012/03/05/cyber>.
8. Пентагон не исключил вооруженного ответа на кибератаки [Электронный ресурс]. – Режим доступа: <http://lenta.ru/news/2010/05/13/militaerschlag>.
9. Anonymous [Electronic resource]. – Regime to access: <http://www.securitylab.ru>.
10. Cyberterrorism [Electronic resource]. – Regime to access: <http://oxforddictionaries.com/definition/cyberterrorism?region=us>.