УДК - 323.284:351.746+007

Макар Роман,
студент магістратури спеціальності «Країнознавство»
факультету міжнародної політики, менеджменту та бізнесу
ДВНЗ «Ужгородський національний університет»
Науковий керівник: канд.політ.наук, доц. Г.І. Мелеганич

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ ЯК ОДНОГО ІЗ СПОСОБІВ ІНФОРМАЦІЙНОЇ ВІЙНИ

Стаття присвячена проблемі кібертероризму як інструменту впливу на національну політику країн. Розглянуто концепції інформаційної боротьби в розвинених країнах та методи ведення інформаційної війни в країнах Європи та США. Висвітлено історію розвитку тероризму та його прояви в сучасному світі. Робиться спроба аналізу розвитку інформаційних технологій та їх впливу на формування нової системи міжнародних відносин в XXI столітті.

***Ключові слова**: тероризм, інформаційний тероризм, інформаційна війна, кібертероризм, ЗМІ, нормативно-правове закріплення, національна безпека.*

Метою статті є спроба аналізу тероризму, як одного з методів ведення інформаційної війни та основних цілей та методів її ведення.

Виклад основного матеріалу. Незважаючи на велику кількість праць з означеної проблематики, це питання потребує подальшої наукової розробки, а також розгляду проблеми взаємовпливу сучасного тероризму як невід'ємної частини інформаційної структури та засобів масової інформації.

Серед дослідників, які займалися вивченням тероризму в умовах глобалізації, розвитку інформаційно-комунікаційних технологій та зростання ролі засобів масової інформації в житті суспільства, потрібно згадати Д. Белла, Ж. Бодрійара, Е. Гіденса, М. Кастельса, Е. Тоффлера, Ф. Фукуяму, С. Хантінгтона, Б. Хофмана, А. Шміда та ін.

У сучасному суспільстві зросло значення інформації. Інформація набула цінності не тільки з точки зору державної таємниці, а й в плані комерційної таємниці, конфіденційної інформації, персональних даних. Завдяки розвитку засобів цифрової цивілізації, значного розширення обсягів застосування у буденному житті різноманітних засобів програмного забезпечення, відбулося широкомасштабне проникнення засобів автоматизації професійної діяльності, мережевих комунікацій, засобів візуалізації та оброблення даних у сферу економіки. У той же час інформація і знання розглядаються як інтелектуальний капітал, як товар, який має свою вартість. У міру формування інформаційного суспільства рівень економічної безпеки країни у все більшій мірі буде визначатися здатністю впровадження інформаційно-комунікаційних технологій в економічні, соціальні, військові, технологічні та культурні сфери суспільства. Тому проблеми забезпечення взаємозв'язку економічної та інформаційної безпеки держави привертають сьогодні все більшу увагу фахівців, які працюють в сфері інформаційних технологій, економіки, політики, права та міжнародних відносин.

Як підкреслюється в Окінавській Хартії глобального інформаційного суспільства, інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття. Їх революційний вплив стосується способу життя людей, їх освіти і роботи, а також взаємодії уряду та громадянського суспільства. Інформаційні технології швидко стають життєво важливим стимулом розвитку світової економіки [1].

У сучасному світі існує багато способів маніпуляцій завдяки інформації. Маніпулятивні технології набувають дедалі ширшого використання, завдяки їм ведуться інформаційні

війни, знищення опонентів (конкурентів), вплив на маси і багато інших дій. Але останнім часом великої популярності набув інформаційний тероризм [2].

На перший погляд, на відміну від тероризму інформаційний тероризм – явище не таке страхітливе. Немає вибухів, закривавлених трупів і стогонів поранених. Але якщо копнути трохи глибше, відкривається не така вже й радісна картина. Інформаційний тероризм – це не тільки кіберзлочини, хоча, звичайно ж, вони частина цього явища, це також некоректні маніпуляції з інформацією або її підтасування, а в деяких випадках і подача свідомо помилкових фактів, внаслідок чого відбувається залякування населення, впровадження параноїдальних думок.

Інформаційні злочини суттєво впливають на інформаційну безпеку держави не тільки через те, що завдяки цим злочинам заподіюється значний економічний збиток, але насамперед через те, що наслідком вчинення зазначених злочинів є порушення нормальної роботи інформаційних і комунікаційних систем, а також поширюється інформація, що має протиправний характер [3, с.173].

Інформаційний тероризм – це злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій [4, с. 98].

Сучасний інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав. Доступність інформаційних технологій значно підвищує ризики інформаційного тероризму. Розвиненість інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму.

У свою чергу інформаційний тероризм поділяють на:

1) інформаційно-психологічний тероризм (контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій):

а) медіа-тероризм або «медіа-кілерство» зловживання інформаційними системами, мережами та їхніми компонентами для здійснення терористичних дій та акцій;

2) інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів комунікації тощо):

а) кібер-тероризм – сукупність дій, що включають інформаційну атаку на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупованнями або окремими особами [5, с. 231].

Значною проблемою у дослідженні цього явища є відсутність єдиної загальноприйнятої дефініції «кібертероризму», що може свідчити як про неактивну роботу міжнародних законодавчих інститутів у цьому напрямі, так і про недостатнє осмислення такого явища й його негативних наслідків. Труднощі у визначенні даного поняття також пов'язані з відмежуванням кібертероризму від інших діянь у сфері комп'ютерної інформації (інформаційної війни, кіберзлочинів тощо) та у визначенні специфіки такого прояву тероризму. Найбільш вживаним в наукових колах є термін «кібертероризм», запропонований Д. Деннінгом, професором Джорджтаунського університету, авторитетним експертом у сфері комп'ютерної злочинності та кібербезпеки в роботі «Активність, хактивізм і кібертероризм. Інтернет як засіб впливу на зовнішню політику», який говорить про кібертероризм як про «протиправну атаку або загрозу атаки на комп'ютери, мережі або інформацію, що знаходиться в них, здійсненою з метою примусити органи влади до сприяння в досягненні політичних чи соціальних цілей [6, с.48].

Для кібертероризму як різновиду інформаційного тероризму, залежно від часу і місця його проведення, властива ціла низка характерних особливостей, які надають можливість

відрізняти його з-поміж інших терористичних актів. Зокрема, такі особливості виражаються у суб'єктному складі, об'єктах, засобах та ознаках.

Суб'єктами є держави, юридичні та фізичні особи, які проводять агресивну інформаційну політику, іноземні спецслужби та організації, ЗМІ, релігійні фанатики, організації сектантів та церковників, різного роду місіонерські організації, окремі екстремістські організації, групи. Об'єктами є інформаційні ресурси, бази даних, статистична звітність тощо. Засобами є повідомлення, що поширюються через видання ЗМІ (хибні повідомлення про очікуваний дефолт країни, вибухи, які готуються, вбивства, отруєння), викликаючи паніку серед населення, не зафіксовані на матеріальних носіях погрози та ін. До типових ознак відносять коректне маніпулювання інформацією, високу латентність і конспірацію замовників, джерел фінансування та виконавців, швидку ескалацію, реальну загрозу у суспільстві, рентабельність за вартістю, масштабність за охопленням і відчутність за наслідками, синхронність атак, віддаленість, інтернаціональність й інші [7, с. 224-225].

Сьогодні існують дві великі організації, готові взяти на себе провідну роль у боротьбі з кіберзлочинністю на міжнародному рівні. Це Підрозділ по боротьбі з тероризмом ОБСЄ – організація, що діє під егідою ООН, а також Інтерпол. Крім того, у Європейському Союзі з нового року розпочав роботу Центр з боротьби з кіберзлочинністю (European CyberCrime Centre). Країни-члени ЄС і європейські інституції мають намір підтримувати Центр з боротьби з кіберзлочинністю для створення оперативних і аналітичних можливостей її розслідування і для співпраці з міжнародними партнерами [8, с. 57 – 62].

Небезпека кібертероризму загострюється з приводу того, що він, як й інші види інформаційного тероризму, не має національних меж (терористичні акції можуть здійснюватися з будь-якої точки світу). Крім того, виявити терориста в інформаційному просторі дуже складно, оскільки він діє з допомогою одиного або кількох підставних комп'ютерів, що ускладнює його ідентифікацію та визначення місцязнаходження. Кібертероризм орієнтується на використання різних форм і методів виводу з ладу інформаційної інфраструктури держави або на використання інформаційної інфраструктури для створення обстановки, що приводить до катастрофічних наслідків для суспільства. А стрімке зростання кількості злочинів, що здійснюються в кіберпросторі, пропорційно числу користувачів комп'ютерних мереж (за оцінками Інтерполу, темпи зростання злочинності в глобальній мережі Інтернет є найшвидшими на планеті), що ще раз підкреслює стан небезпеки з боку інформаційного тероризму. За твердженням фахівців ізраїльської контррозвідки, «терористи» за допомогою електронної пошти передають в зашифрованому вигляді інструкції, карти, схеми, паролі та іншу важливу інформацію, розголошення якої може зашкодити національній безпеці держави [9, с. 164-165].

Якщо говорити про міжнародно-правові акти в цій сфері, головним документом, в якому йде мова про боротьбу з інформаційними загрозами, є Конвенція "Про кіберзлочинність" від 23 листопада 2001 р., ратифікована Верховною Радою України 07 вересня 2005 р. Цей документ націлено на здійснення загальної політики з питань кримінального права, метою якої є захист суспільства від кібертероризму. Однак, у цьому документі нічого не зазначено про поняття «інформаційний тероризм», тільки ретельний аналіз Конвенції дає підстави стверджувати, що кібертероризм є частиною, або, за твердженням деяких науковців, ідентичним поняттям щодо інформаційного тероризму. Важливість означеного міжнародно-правового документа обумовлена процесом правової регламентації та імплементації у чинне законодавство поняття інформаційного тероризму.

Семантика нормативно-правових актів дає підстави стверджувати, що поняття інформаційного тероризму не знайшло свого відображення в чинному законодавстві України, однак на доктринальному рівні означене поняття досліджувалось як юристами, так і фахівцями з державного управління, безпекознавства та політології.

Так, В.О. Коршунов вказує, що інформаційний тероризм – це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою наслідки для життєдіяльності особистості, суспільства і держави [10, с. 6].

Боротба з кібертероризмом – це важливий напрям інформаційної діяльності держави. Закони в цій сфері повинні відповідати вимогам сьогодення. Беручи до уваги низку нормативноправових актів українське законодавство не забезпечує ефективного захисту національних інтересів. Тому уряду нашої держави необхідно проводити цілеспрямовану роботу з гармонізації та вдосконалення законодавства у сфері інформаційної безпеки держави. Україна має розробити ефективну інформаційну політику, спрямовану на інформування громадян та забезпечення їхнього розуміння того, в чому полягають причини тероризму – підвищення медіа-грамотності (вміння протистояти спробам маніпулювання собою за допомогою інформаційних потоків) та довіри до держави та інші складові.

Согодні ми повинні рухатися в напрямі нейтралізації негативного впливу інформаційних воєн на світове співтовариство, адже вони нікому не йдуть на користь, крім PR-менеджерів, журналістів і власників ЗМІ.

Висновок. Одним з найефективніших методів боротьби з інформаційним тероризмом, вважаємо, створення певної спеціальної установи, роль якої полягатиме в розробці нової доктрини інформаційної безпеки у співпраці з експертами у цій сфері та разом зі ЗМІ потрібно реалізувати її в найкоротші терміни. Проте на сьогодні в Україні не існує такого інституту, але заснування єдиного Інформаційного центру протидії інформаційному тероризму на базі Ради Національної безпеки і оборони України є необхідним. Такий центр повинен виконувати певні функції та низку покладених на нього завдань з протидії пропаганді тероризму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 р. [Електронний ресурс]. – Режим доступу: http://zakon4. rada.gov.ua/laws/show/998_163.
2. Бабенко Ю. Інформаційний тероризм / Ю. Бабенко [Електронний ресурс]. – Режим доступу: http://www.aratta-ukraine. com/text_ua.php?id=149.
3. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави [Електронний ресурс]. – Режим доступу: http://pravolib.pp.ua/mejdunarodno-pravovyie-problemyi-obespecheniya.html.
4. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism/ M. Jerrold // NATO Library at:TERRORISM_AND_POLITICAL_VIOLENCE, vol. 12, no. 2, Summer 2000, P. 97-122.
5. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О. В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ІПРТК-2009): Друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.
6. Denning D. Activism, Hacktivism, and Cyberterrorism: the Internetas a Toolfor Influencing Foreign Policy / D. Denning [Електронний ресурс]. – Режим доступу:http://www.rand.org/content/dam/rand/ pubs/monograph_reports/MR1382/MR1382.ch8.pdf.
7. Стрельбицький М. Соціальні передумови (юридичні факти) інформаційного тероризму та кіберзлочинів / М. Стрельбицький, С. Саржан // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2014. – № 2. – С. 21 – 226.
8. Бойченко О.В. Кібертероризм у складі сучасних проблем національної безпеки /О.В. Бойченко, О.О. Ончурова // Форум права. – 2010. – № 2. – С. 57 – 62.

9. Герасименко К. Сучасні ознаки загроз «інформаційного тероризму» / К.Герасименко [Електронний ресурс]. – 2009. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09gkczit.pdf4
10. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 «Політичні інститути та процеси» / В.О. Коршунов. – Дніпропетровськ, 2008. – 18 с.

Makar Roman. FEATURES INFORMATION TERRORISM AS ONE OF THE METHODS OF INFORMATION WAR

The article is devoted to the problem of cyber terrorism as an instrument of influence on national politics of the countries. Pronoun the concept of information warfare (information war) in developed countries. Shows the methods of information warfare in Europe and the United States. Highlights the history of terrorism and its manifestations in the modern world. Examines the role of media and their impact on society. Attempts to analyze the development of information technologies and their influence on the formation of a new system of international relations in the twenty-first century.

Keywords: *terrorism, information terrorism, information warfare, cyber-terrorism, media, legal post, national security.*