

ФЕНОМЕН ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ ЯК ЗАГРОЗИ МІЖНАРОДНІЙ БЕЗПЕЦІ

Смачило Т.В., Кривцун А.Р.

Тернопільський національний економічний університет

Досліджено поняття тероризм як метод впливу шляхом здійснення теракту для досягнення поставлених цілей. Виокремлено кібертероризм як інформаційну атаку на електронну інформацію, обчислювальні системи, банківські системи, технічні засоби передачі даних та інші системи інформаційної інфраструктури. Визначено основні особливості та характеристики кібертероризму. Наголошено, що медіа-тероризм та кібертероризм є видовими, а інформаційний тероризм – родовим поняттями одного негативного явища – тероризму. Визначено основні напрями боротьби з кіберзлочинністю.

Ключові слова: тероризм, інформаційний тероризм, кібертероризм, медіа-тероризм, інформаційна війна, міжнародна безпека, ЗМІ.

Постановка проблеми. У ХХІ столітті інформація набула цінності не тільки з позиції державної таємниці, а й щодо комерційної таємниці, конфіденційної інформації, персональних даних. Дедалі збільшується кількість способів маніпуляції за допомогою інформації. Одночасно бурхливий розвиток інформатизації, разом із усіма перевагами, створив нові проблеми та загрози у сфері національної безпеки.

Особливо значного поширення набув інформаційний тероризм, оскільки в умовах глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби національних інтересів будь-яких держав стає інформаційний простір. Осмислення феномену інформаційного тероризму є передумовою формування більш чітких уявлень про запобігання загроз, здатних зруйнувати державні інститути, основи національної безпеки держави загалом.

На сьогодні можна спостерігати значне підвищення уваги до питання протидії інформаційному тероризму, водночас багато питань залишаються невивченими. Значною мірою це викликано розв'язаною проти України «гібридною війною», однією із ключових складових якої залишається інформаційна сфера [8].

Аналіз останніх досліджень і публікацій. Сутність феномену інформаційного тероризму досліджується в працях вітчизняних та зарубіжних науковців. Серед дослідників, які займалися вивченням тероризму та інформаційного тероризму, потрібно згадати Д. Белла, Ж. Бодрійяра, Е. Гіденса, М. Кастельса, Е. Тоффлера, Ф. Фукуяму, С. Хантінгтона, Б. Хофмана, А. Шміда, О. Зернецьку, О. Гриценку, В. Іванову, С. Макаренку, М. Ожевана, Г. Почепцова, А. Чічановського та інших.

Однак у наукових роботах повною мірою не відображено тенденції швидкого розвитку інформаційного тероризму та недостатньо вивченими є нові феномени цього явища.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значну кількість праць з даної проблематики, вона потребує подальшої наукової розробки, а також розгляду проблеми взаємовпливу сучасного інформаційного тероризму.

Метою статті є дослідження поняття та змісту інформаційного тероризму як загрози міжнародній безпеці на сучасному етапі світового розвитку.

Мета статті обумовлює завдання дослідження:

– проаналізувати поняття та розуміння тероризму та міжнародного тероризму на даному етапі;

– охарактеризувати визначення інформаційного тероризму та його види;

– виокремити заходи протидії інформаційному тероризму.

Виклад основного матеріалу дослідження.

Перш за все, зупинимось на дослідженні такого поняття як «тероризм». Перші історичні згадки про появу цього терміну з'явилися у 1798 році, коли філософ Іммануїл Кант використав його для висвітлення песимістичного погляду на долю людства [5].

У теперішній час серед науковців не існує єдиного трактування поняття «тероризм». У. Лаккер звернув свою увагу на випадковості, ірраціональності та недоступності розуміння тероризму. Він зауважив, що: «Не повинно бути ілюзій стосовно того, що можна дізнатися про походження та характер тероризму. Встановленню піддається лише той факт, що при одних, обставинах терор частіше здійснюється, ніж при інших, і що при деяких обставинах він взагалі не може мати коріння. Перевантажений значенням за своєю природою поняття не піддається всім зусиллям виробити всеохоплююче і об'єктивне визначення тероризму. Такого визначення не існує і не буде знайдено в найближчому майбутньому» [1]. Однак, тероризм, може отримати своє визначення, так як основним питанням в даному випадку стає з'ясування того, наскільки послідовно і точно поняття використовується до певних явища, та що визначається основним критерієм для визначення сутності поняття.

На сьогодні, існує багато пояснень, або ж визначень тероризму. Розглядаючи це поняття в загальному значенні, тероризм – це метод впливу шляхом здійснення теракту для досягнення поставлених цілей, через який постраждали від теракту не є об'єктом. Зараз цей феномен став настільки поширеним, що стає всесвітнім явищем і його масштаби перетворюються на багатоаспектне явище, яке останнім часом дуже швидко еволюціонує, і як наслідок набуває міжнародного характеру. Міжнародний тероризм – це здійснення у світовому чи регіональному масштабі дії терористичними організаціями, угрупованнями, а також за підтримки державних органів окремих

держав, з метою досягнення певних цілей, які є суспільно небезпечними насильницькими діяннями, що пов'язані з викраденням, захопленням, вбивством ні в чому не винного населення, чи загрозою їх життю і здоров'ю, руйнуванням чи загрозою знищення важливих народногосподарських об'єктів, систем життєзабезпечення, комунікацій, застосуванням чи загрозою застосування ядерної, хімічної, біологічної та іншої зброї масового ураження [6].

Суть тероризму – насильство з цілю залякування. Суб'єкт терористичного насильства – окремі люди, чи неурядові організації. Об'єкт насилля – влада під маскою окремих урядових виконавців, або окремі представники від суспільства. Крім того, це може бути державна або приватна власність, інфраструктура, системи, які забезпечують нормальне життя населення. Ціль насилля – досягнення бажаного для терористів розвитку подій – революція, дестабілізація суспільства, початок війни з іншою державою, отримання незалежності певної території, падіння престижу влади, політичних змін зі сторони влади та інше.

Терористичну діяльність можуть проводити терористи в одній особі, терористичні угруповання і організації (в тому числі і міжнародні, які підтримуються зарубіжними державами). Тероризм здійснюється як підпільна, насильницька, цілеспрямована, керуюча, ідеологічна боротьба. Жертви тероризму можуть бути випадкові або обрані терористом. Терористичний акт виконує функцію залякування певних категорій людей або ж пропаганда ідей терористів.

Інформаційна епоха розширила сферу діяльності тероризму, що призвело до появи «інформаційного тероризму», основою якого є маніпуляція свідомістю мас, розповсюдження інформаційно-емоційного ефекту на який розраховано більшість терористичних актів, залучення прихильників серед членів суспільства, вплив на владні структури, які приймають політичні рішення [4].

Порівнюючи визначення поняття «тероризм» та «інформаційний тероризм», складається враження, що інформаційний тероризм не є жахливим. Оскільки відсутні загиблі, поранені. Однак, якщо дослідити його сутність, то сучасний інформаційний тероризм можна охарактеризувати як множини інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав. Крім того, доступність інформаційних технологій значно підвищує ризики інформаційного тероризму, а розвиток інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму [9].

Інформаційний тероризм поділяють на:

- інформаційно-психологічний тероризм (контроль над ЗМІ для поширення дезінформації, чуток, демонстрації могутності терористичних організацій);
- інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу загалом: руйнування елементної бази, створення перешкод на лініях зв'язку, штучне перенавантаження вузлів комунікації та інше) [2].

Виокремимо основні складові тероризму: суб'єкт (або декілька суб'єктів); об'єкт (або об'єкти); мета здійснення; причини і мотив; часові та просторові характеристики; інструменти, які використовуються; наслідки.

Звичайно ж можна виділити підгрупи із перерахованих складових.

За критерієм інструментів (засобів), які використовуються, можна виокремити різноманітні типи тероризму. Складність використання цього критерію полягає в тому, що суб'єкти тероризму, як правило, поєднують кілька засобів – це може бути і захоплення стратегічно важливого об'єкту, в якому знаходяться люди, що стають заручниками, і транспортного засобу із одночасною зупинкою нормального функціонування транспортної системи та інше [7].

На даний момент найбільш ефективними і найдешевшими інструментами тероризму, які активно використовуються є глобальне ЗМІ та Інтернет. У поєднанні вони формують інформаційне поле, де реальність подана у дещо викривленому вигляді, яка повертає настрої людей в дещо інше русло, що дає можливість терористичній стороні схилити погляди населення на свою користь. Також терористи використовують засоби масової інформації для інформування суспільства про свою діяльність, залучення активних людей до своїх дії або психологічний вплив на людей. Важливим завданням для терористів є використання міжнародних засобів інформації для того, щоб поширювати власні ідеї або ж ідеологію. І такі випадки в історії прослідковуються не одноразово. Коли відомий британський телеканал «Channel 4» оприлюднив інтерв'ю в якому показав відомого міжнародного терориста Шаміля Басаєва, Російська Федерація відреагувала обуренням.

Медіа-тероризм або «медіа-кілерство» – це зловживання інформаційними системами, мережами та їхніми компонентами для здійснення терористичних дій та акцій [7; 9].

Ще одним видом тероризму, який варто виокремити є кібертероризм. Його розглядають, як інформаційну атаку на електронну інформацію, обчислювальні системи, банківські системи, технічні засоби передачі даних та інші системи інформаційної інфраструктури. Здійснюється окремими особами або терористичними угрупованнями. Кібертероризм спрямований на те, щоб заволодіти контролем інформаційно-телекомунікаційними системами, тобто не проводити свої ідейні виступи, а системне проникнення, що дасть змогу контролювати інформаційні потоки, завдання шкоди мережам інформаційного обміну та інші деструктивні дії. Перевагою для терористичної сторони є те, що дії такого характеру не обмежені кордонами чи відстанню, тобто не існує національних меж. Також складно виявити об'єкт терористичних дій в інформаційному просторі, оскільки хакери проводять ці операції через підставні комп'ютери, чи певну мережу комп'ютерів, що значно ускладнює пошук чи ідентифікацію місцезнаходження злочинця. Особливо сьогодні, коли технологічне вдосконалення розвивається швидкими темпами, стало важко створити надійну систему безпеки, яка захищатиме від кібертерористів.

Тому кожній державі необхідно провести ряд заходів для протидії інформаційному тероризму. Варто зауважити, що значну роль в цьому відіграє правова база, яка слугує основою для запобігання терористичних актів. Ефективною складовою стає наявність у відповідних структурах будь-якої держави, наприклад в Україні – це СБУ та МВС, спільної бази даних про терористів та осіб, які можуть бути причетними до цього. Це буде ефективним засобом для протидії та профілактики терористичних дій. Для попередження кібертерористичних дій слід виокремити основні напрями такої боротьби:

- уніфікація та гармонізація національного законодавства та міжнародних актів;

- проведення наукових розробок в сфері створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

- створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом;

- удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

- удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки [3].

Стає зрозуміло, що запобігання терористичних дій, особливо боротьба з кібертероризмом, повинні здійснюватись комплексним підходом, поєднуючи силові, політико-дипломатичні, економічні та гуманітарні методи протидії.

Висновки. Отже, розглядаючи інформаційний тероризм як сучасне явище, можна сказати, що він становить значну загрозу суспільству, населенню та міжнародній безпеці. Технологічний прогрес надає більше можливостей терористам здійснювати вплив на людей, на їх свідомість, дозволяє їм притягувати до себе увагу, поширюва-

ти свою ідеологію навіть на великі відстані, тобто не обмежуючи себе територіально. Сьогодні вже усі технічні засоби обробки та зберігання інформації стали легко вразливі силам терористів.

Варто розуміти те, що проблема протидії інформаційного тероризму – це комплексна проблема. Закони держав повинні беззаперечно відповідати технологічній революції і бути готовими захищати їхні інтереси в будь-якому інформаційному полі. Тому уряди держав повинні здійснювати заходи необхідні для гармонізації та вдосконалення законодавства заради їхньої інформаційної безпеки.

Наразі можна виокремити наступні завдання, які в комплексному застосуванні допоможуть створити суттєвий інформаційний захист для держави:

1. Постійний моніторинг інформаційного середовища на випадок потенційної кібертерористичної загрози.

2. Захист елементів вітчизняної інфраструктури.

3. Створення та оновлення програмного забезпечення, яке зможе захистити інформаційне середовище держави.

4. Усунення прогалів в законодавстві держави.

5. Зауваження населення про кіберзлочини, оскільки 80% атак залишаються невисвітленими для правоохоронних органів.

6. Боротьба з не ліцензованим програмним забезпеченням.

7. Створення системи, яка забезпечить загальнодержавний захист інформації.

Беззаперечно найкращим методом боротьби з інформаційним тероризмом є підтримка новітніх інформаційних технологій та стимули для науково-технічного прогресу всередині держави, що допоможе запобігти кібертероризму. А спонсорювання даних заходів має на себе взяти держава, яка зможе коректно спрямувати усі напрацювання науково-технічного процесу.

Список літератури:

1. Laqueur W. New terrorism / NY., Oxford: Oxford University Press, 1977. – 290 p.
2. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційної безпеці / О.В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009): друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.
3. Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – № 20.
4. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України / О.В. Глазов [Електронний ресурс]. – Режим доступу: <http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf>
5. Діордіца І.В. Поняття та зміст кібертероризму [Електронний ресурс]. – Режим доступу: <http://goal-int.org/ponyattya-ta-zmist-kiberterorizmu>
6. Конвенція про кіберзлочинність: за станом на 7 вересня 2009 р. [Електронний ресурс] // Офіційний веб-портал Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575
7. Медіа-тероризм серед інших видів тероризму: спроба типологічного аналізу / Тетяна Єрохіна [Електронний ресурс]. – Режим доступу: <http://www.social-science.com.ua/article/1002>
8. Пилипчук В.Г. Запобігання інформаційній безпеці України: сучасні тенденції та проблеми / В.Г. Пилипчук // Матеріали наук.-практ. конф. (6 жовтня 2016 р.). – К.: НТУУ «КПІ імені Ігоря Сікорського», Вид-во Політехніка, 2016. – С. 24–28.
9. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни / Т.П. Яцик // Науковий вісник Національного університету державної податкової служби України (економіка, право). – 2014. – № 2. – С. 55–60.

Смачило Т.В., Кривцун А.Р.

Тернопольский национальный экономический университет

ФЕНОМЕН ИНФОРМАЦИОННОГО ТЕРРОРИЗМА КАК УГРОЗЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Аннотация

Исследовано понятие терроризм как метод воздействия путем совершения теракта для достижения поставленных целей. Выделены кибертерроризм как информационную атаку на электронную информацию, вычислительные системы, банковские системы, технические средства передачи данных и другие системы информационной инфраструктуры. Определены основные особенности и характеристика кибертерроризма. Отмечено, что медиатерроризм и кибертерроризм являются видовыми, а информационный терроризм – родовым понятиями одного негативного явления – терроризма. Определены основные направления борьбы с киберпреступностью.

Ключевые слова: терроризм, информационный терроризм, кибертерроризм, медиатерроризм, информационная война, международная безопасность, СМИ.

Smachylo T.V., Kryvtsun A.R.

Ternopil National Economic University

PHENOMENON OF INFORMATION TERRORISM AS A THREAT OF INTERNATIONAL SECURITY

Summary

The concept of terrorism as a method of influence through the commission of a terrorist attack for achievement of the set goals was investigated. Cyberterrorism is isolated as an information attack on electronic information, computing systems, banking systems, technical means of data transmission and other information infrastructure systems. The main features and characteristics of cyber-terrorism are determined. It is emphasized that media terrorism and cyberterrorism are specific, and information terrorism is a generic notion of one negative phenomenon – terrorism. The basic directions of struggle against cybercrime are determined.

Keywords: terrorism, information terrorism, cyberterrorism, media terrorism, information war, international security, mass media.