РОЗДІЛ VII. АКТУАЛЬНІ ПРОБЛЕМИ КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНОЛОГІЇ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

DOI https://doi.org/10.26661/2616-9444-2018-1-15

УДК 343.123.3/.5: 343.436: 323.281

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЕЛЕМЕНТ СУЧАСНОЇ УКРАЇНСЬКОЇ ПОЛІТИКИ

Єна І.В., к.ю.н., доцент

Запорізький національний університет, вул. Жуковського, 66, м. Запоріжжя, Україна
ena-irina@ukr.net

Статтю присвячено аналізу такого складного явища, як інформаційний тероризм, який у сучасних умовах розвитку української політики отримав надзвичайний розвиток і значення, оскільки політичні групи отримали надзвичайно ефективний механізм впливу на поведінку громадян, органів, наділених владними повноваженнями, і суспільства загалом.

Доступ до інформації та широкі можливості її використання стали важливим ресурсом політичної влади. І, на жаль, це явище не повною мірою вивчено, а тому відсутні доречні рекомендації щодо розслідування та протидії такому різновиду злочинної діяльності.

Ключові слова: тероризм, інформаційний тероризм, автоматизовані системи, кіберпростір, пропаганда, політичні групи, транснаціональна злочинність.

INFORMATION TERRORISM AS AN ELEMENT OF MODERN UKRAINIAN POLITICS

Ena I.V.

Zaporizhzhya National University, str. Zhukovski, 66, Zaporizhzhya, Ukraine
ena-irina@ukr.net

The article is devoted to the analysis of such a complex phenomenon as information terrorism, which in modern conditions of development of Ukrainian politics has received extraordinary development and significance, since political groups have received an extremely effective mechanism of influence on the behavior of citizens, authorities endowed with power, society as a whole.

Access to information and wide opportunities for its use have become an important resource of political power. And unfortunately, this phenomenon is not fully studied, therefore, there are no relevant recommendations for investigating and counteracting this kind of criminal activity.

Modern terrorism is significantly different from the use of terrorist tactics by extremist groups in the past. It is a multifaceted phenomenon that goes beyond the traditional intimidation and use of violence or the threat of its use. It should be noted that today in the world crimes and “big politics” are interconnected.

Terrorism is always characterized by a politicized shade, as it manifests itself in the form of political violence, which is carried out in pursuit of a political goal. The presence of a political goal distinguishes terrorism from similar on the objective side of criminal offenses.

One can distinguish the main purpose of information terrorism – it’s information impact on the mass consciousness. And this influence is usually carried out in those spheres where different ideas and views are proclaimed, and there is a certain struggle for them. For example, in the philosophical, legal, religious, political sphere, etc. At the same time, the goal is achieved through the use of information technology.

Taking into account the specifics of modern society and the availability of information technologies, politicians in their work increasingly use methods of information struggle to achieve their political goals. That allows to significantly increase the efficiency of their activities in such areas, such as: search for money; project financing; propaganda of its goals; collection of information; efficiency, scale of influence on consciousness; dissemination of information material, propaganda; coordination of activities of political groups and the exchange of information for solving common problems; increasing opportunities

for the exchange of complex comprehensive information; discrediting political opponents; creating instability in society; programming behavior of people, etc.

The main danger of this type of terrorism is that, unlike the classic terrorist attack, it is possible to use unknown terrorist technologies that directly carry out a frightening effect on the mass consciousness.

In our opinion, solving the problem of information terrorism consists not only in the use of preventive measures aimed at detecting terrorist attacks in the information space, the reasons and conditions for their implementation, but also the thorough work on controlling the activities of the mass media.

It is this complex of actions that should ensure the effectiveness of counteracting law enforcement agencies with information terrorism.

Key words: terrorism, information terrorism, automated systems, cyberspace, propaganda, political groups, transnational crime.

З 1960-х років людство стало свідком глобальних змін у всіх галузях розвитку суспільства – науці, бізнесі, економіці, медицині тощо. Не оминув цей процес і політичну сферу. Рушійною силою таких змін стало проникнення в усі сфери життя інформаційних технологій, їх швидке вдосконалення й модернізація, у результаті чого сьогодні ми спостерігаємо перехід суспільства від індустріального до інформаційного.

Можна впевнено стверджувати, що сьогодні не існує жодної сфери людської діяльності, у якій не використовувались би сучасні комп'ютерні можливості, електронні системи, телекомунікаційні засоби, що забезпечує підвищення значущості інформації та інформаційних ресурсів. Сучасні інформаційні технології дають виняткові можливості для більш ефективного розвитку економіки, політики, держави, проте водночас стимулюють виникнення й розвиток негативних процесів.

Крім безумовно позитивних аспектів масштабне формування інформаційного суспільства вивело на передній план проблему забезпечення безпеки інформації, а також охорони державних, суспільних і приватних інтересів. Нові технології зумовлюють нові глобальні проблеми, однією з яких є поява так званої комп'ютерної злочинності. У зв'язку із цим нових змістовних характеристик набувають такі давно відомі злочини, як крадіжка, підробка документів, тероризм тощо.

Сучасний тероризм істотно відрізняється від використання терористичної тактики екстремістськими групами в минулому. Це багатогранне явище, яке вийшло за межі традиційного залякування та використання насилля або загрози його використання.

Терористична діяльність як складне, багатоаспектне негативне соціально-політичне явище давно переросла національні межі та перетворилася на масштабну загрозу для безпеки всього людства.

Саме цей вид злочинної діяльності в сучасних умовах розвитку української державності отримав особливе значення, оскільки для ситуації, яка сьогодні склалася в українському політичному полі, характерне здійснення нав'язування групою людей певної поведінки органам, що наділені владними повноваженнями, і суспільству загалом. І найефективнішим способом такого впливу й управління суспільством є активне використання інформаційного простору. Отже, доступ до інформації та широкі можливості її використання стали важливим ресурсом політичної влади.

На перший погляд здається, що до вказаної ситуації тероризм як вид кримінального правопорушення не має жодного відношення[1], проте це не так, оскільки сьогодні прийнято

[1] У статті 248 Кримінального кодексу України тероризм визначається як застосування зброї, вчинення вибуху, підпалу *чи інших дій*, які створювали небезпеку для життя чи здоров'я людини, або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень, вчинення чи невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або

виділяти такий новий різновид тероризму, як інформаційний тероризм, що є одним з ефективних інструментів політичної діяльності не лише в Україні, а й у світі.

Варто констатувати, що сьогодні у світі злочини та «велика політика» є взаємопов'язаними. Вони мають такі складники:

– результати еволюції суспільства та ті проблеми, які постають на шляху його розвитку, закономірно й об'єктивно впливають на визнання тих чи інших діянь злочинними через встановлені процедури прийняття законів;

– окремі характеристики та проблемні ситуації в суспільстві використовуються політичними силами для криміналізації діянь, суспільна небезпека яких не очевидна, проте суб'єктивно їм необхідна;

– криміналізація діянь використовується як надійний засіб регулювання поведінки людей;

– криміналізовані діяння перетворюються на інструмент вибіркового правозастосування, яке дає змогу використовувати кримінальний закон у політичній боротьбі [1, с. 12].

Тероризму завжди притаманний політизований відтінок, оскільки він проявляється у вигляді політичного насилля, яке здійснюється з метою досягнення політичної мети. Наявність політичної мети відрізняє тероризм від схожих за об'єктивною стороною кримінальних правопорушень.

Саме інформаційний тероризм, на нашу думку, стає новим та ефективним засобом політичного маніпулювання суспільством поряд з інформаційною війною та інформаційною експансією.

Інформаційний тероризм – нове явище, про що свідчить також те, що донедавна в теорії й практиці було прийнято виділяти три основні види терору:

– внутрішній – відповідні дії громадян однієї держави проти співвітчизників на власній території;

– транснаціональний – відповідні дії громадян однієї держави проти співвітчизників на території інших держав;

– міжнародний – відповідні дії груп громадян, єдиних чи змішаних за національним складом, проти будь-яких осіб на території третіх країн [2, с. 163].

Незважаючи на те, що поняття «інформаційний тероризм» відносно нове для українського суспільства, воно перебувало в колі наукових досліджень таких вітчизняних і зарубіжних авторів, як Є.Л. Вартанова, В.В. Ященко, А.А. Сальников, М. Дюмонтьє, Дж. Бірда, В.Д. Недільніченко, В.І. Смельянов, В.А. Кульба, В.Ф. Антипенко та інші.

Однак не можна стверджувати, що сутність інформаційного тероризму є дослідженою на достатньому рівні. Більше уваги приділяється все-таки інформаційним технологіям, вивченню кримінально-правової та криміналістичної характеристики тероризму, міжнародному тероризму тощо. На нашу думку, це пов'язано з тим, що суспільство загалом і наукова спільнота зокрема не повною мірою усвідомлюють ті загрози, які несе саме інформаційний тероризм, оскільки він має здебільшого латентний характер, поширюється в специфічному середовищі (сфера його поширення не має кордонів), а отже, має транснаціональний характер.

привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій із тією ж метою.

Відповідно, включення у формулювання кримінального закону словосполучення «інші дії» передбачає досить великий невизначений спектр дій, що ускладнює процес кваліфікації діяння.

Справді, сформулювати ґрунтовне визначення поняття «інформаційний тероризм» досить складно, сьогодні немає загальновизнаної дефініції цього явища. Однак спроби виправити таку ситуацію робилися. Так, О.А. Українська вважає, що інформаційний тероризм можна визначити як форму негативного впливу на особистість, суспільство та державу всіма видами інформації, або, інакше кажучи, маніпулювання суспільною свідомістю за допомогою інформаційних технологій для досягнення певних цілей [3].

М.П. Стрельбицький і С.Л. Саржан пропонують розглядати це поняття в двох аспектах. У широкому розумінні це маніпулювання суспільною свідомістю шляхом масового поширення неправдивої та сфабрикованої інформації з метою створення напруженості в суспільстві, нестабільності, хаосу, спрямованих на реалізацію політичних чи економічних цілей в інтересах терористів. У вузькому розумінні це кібератаки на інформаційні системи, що працюють у контурах управління державними й соціально важливими технологічними об'єктами та системами (атомними чи гідроелектростанціями, банками, хімічним виробництвом, авіацією та іншими видами транспорту тощо), з метою виведення їх із ладу, спричинення економічних, екологічних та інших катастроф [4, с. 220–221].

В.В. Остроухов пропонує розглядати інформаційний тероризм як небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади й управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також спотворення об'єктивної інформації, що спричиняє появу кризових ситуацій у державі, нагнітання страху та напруги в суспільстві [5, с. 136].

Під час аналізу наведених визначень можна виділити основну мету інформаційного тероризму – інформаційний вплив на масову свідомість. І цей вплив, як правило, здійснюється в тих сферах, де проголошуються різні ідеї й погляди, є певна їх боротьба (наприклад, у філософській, правовій, релігійній, політичній тощо). При цьому мета досягається за допомогою інформаційних технологій.

Крім того, варто зазначити, що це найбільш швидкий та ефективний гібридний політико-правовий спосіб управління як окремою людиною, так і групою людей, суспільством, державою в особі державних органів. У цьому контексті необхідно погодитись із тезою К. Клаузевіца про те, що тероризм – це метод ведення війни, політики та пропаганди одночасно.

З огляду на специфіку сучасного суспільства й доступність інформаційних технологій політики у своїй діяльності дедалі частіше використовують для досягнення своїх політичних цілей методи інформаційної боротьби. Це дає їм змогу суттєво збільшити ефективність своєї діяльності за такими напрямами:

- пошук грошей;
- фінансування проектів;
- пропаганда своїх цілей;
- збір інформації;
- оперативність, масштабність впливу на свідомість;
- поширення матеріалів інформаційного, пропагандистського характеру;
- координація діяльності політичних груп та обмін інформацією для вирішення загальних завдань;
- збільшення можливостей обміну складною комплексною інформацією;
- дискредитація політичних опонентів;
- створення нестабільності в суспільстві;

– програмування поведінки людей тощо.

На підставі аналізу спеціальної літератури можна зробити висновок, що інформаційний тероризм прийнято поділяти на види.

Так, наприклад, Т.Л. Тропіна виділяє два види кібертероризму:

а) здійснення за допомогою комп'ютерів і комп'ютерних мереж терористичних дій;

б) використання кіберпростору у своїх цілях терористичними групами, проте не задля здійснення терактів [6].

Ми також пропонуємо виділити два види інформаційного тероризму. Перший – інформаційно-психологічний тероризм, який являє собою вплив на свідомість людини за допомогою можливостей засобів масової інформації (далі – ЗМІ), тобто терористи звертаються до суспільства за допомогою друкованих видань, радіостанцій, телеканалів, інтернет-медіа.

При цьому ЗМІ можна вважати найбільш зручним, швидким і найбільш поширеним засобом поширення інформації терористичного змісту. Крім того, варто мати на увазі, що інформація, яка поширюється сучасними ЗМІ, не підлягає цензурі, вони у своїй діяльності користуються одним із досягнень демократичного устрою – свободою слова, що гарантована Конституцією України. Цей фактор також може використовуватись терористами з огляду на комерційний характер їх діяльності та знаходження у власності політиків, бізнесменів тощо.

Тому вважаємо за доцільне внести пропозицію щодо законодавчого обмеження поширення інформації, виготовленої у вигляді письмового тексту, відео- й аудіоряду, якщо вона провокує насилля та порушення прав і свобод людини. Звісно, таке обмеження може мати місце тільки після проведення відповідного експертного дослідження із застосуванням лінгвістичних і психологічних знань.

Однак при цьому можуть виникнути труднощі у вигляді певної політичної, релігійної заангажованості спеціалістів, яким може бути доручено проведення дослідження. Тому, на нашу думку, варто уникати залучення до подібних досліджень представників громадських організацій певної спрямованості, релігійних, політичних організацій тощо. Крім того, для забезпечення повноти й об'єктивності дослідження необхідно призначати комплексну експертизу, включити до складу експертів не залежних одне від одного осіб та формувати висновки на підставі зіставлення їхніх думок.

ЗМІ є не просто суб'єктами впливу на масову свідомість, а ключовим інструментом, за допомогою якого проходить безпосереднє її формування. ЗМІ повинні виконувати функції посередника між джерелами інформації (органами державної влади, громадськими організаціями, політичними партіями) та її споживачами (громадянами) [7].

Другий вид інформаційного тероризму – це інформаційно-технічний тероризм, який здійснюється, як правило, за допомогою використання спеціальної комп'ютерної техніки та може знаходити прояв у таких діях, як пошкодження ліній зв'язку, телекомунікаційних мереж і систем, викрадення, перекручення інформації, знищення баз даних тощо. Обов'язковим наслідком таких дій має бути створення небезпеки загибелі людей, заподіяння шкоди здоров'ю, майну, тобто вони мають бути спрямовані на порушення відчуття безпеки, залякування населення тощо.

Наведене дає можливість зробити висновок про те, що інформаційні, комп'ютерні технології під час здійснення інформаційного тероризму мають подвійний характер. З одного боку, вони є об'єктом посягання (наприклад, під час вчинення кримінального правопорушення, передбаченого ст. 361 Кримінального кодексу України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»), а з іншого – як знаряддя злочину, що використовується терористами (наприклад,

під час вчинення кримінального правопорушення, передбаченого ч. 1ст. 361[1] Кримінального кодексу України «Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»).

І допомогти відмежувати інформаційний тероризм від інших його видів та інших кримінальних правопорушень знову допомагає мета його здійснення.

Бурхливий розвиток інформаційних технологій сприяв тому, що політики отримали новий інструмент впливу на свідомість людей – віртуальну реальність, яка розширює можливості маніпулювання шляхом нав'язування нових цінностей та ідеалів і формування віри в те, що особа сама сформувала такі погляди у своїй свідомості.

Особливу роль під час використання вказаного методу відіграє мережа Інтернет, оскільки вона має досить широку аудиторію (більшу порівняно зі ЗМІ) та практично необмежені можливості поширення інформації. Саме це привернуло увагу також політичних груп, які за допомогою глобальної мережі вирішують основне завдання – забезпечення найбільшого охоплення аудиторії та доведення до неї інформації без цензури й швидко.

Ще однією особливістю інформаційного тероризму є те, що його прояви перебувають за межами кримінальної відповідальності, на відміну від кримінально караних діянь, які прийнято називати комп'ютерними злочинами, оскільки ці дії за своєю суттю можуть і не бути порушенням закону, проте завдавати шкоди як окремим членам суспільства, політичним об'єднанням, так і державі загалом.

Відповідно, такий вид тероризму здається менш небезпечним явищем, проте це лише на перший погляд. Насправді дезінформація суспільства, дискредитація органів влади мають більш тяжкі наслідки. Наприклад, поширення через ЗМІ неправдивої інформації може налаштувати громадян проти діяльності органів державної влади та спонукати їх до прийняття поглядів терористичних організацій, що може призвести до більш радикальних проявів.

Головною небезпекою цього виду тероризму є те, що в ньому, на відміну від класичного теракту, стають можливими для застосування донині не відомі терористичні технології, які безпосередньо здійснюють залякуючий вплив на масову свідомість. Зброя в цьому випадку також не є традиційною – інформаційні, соціальні технології. Наприклад, широкого поширення набули сайти терористичного спрямування. Саме на них викладаються новини та інші відомості (матеріали) дезінформуючого характеру, які мають сформувати в споживачів такої інформації (населення) відчуття небезпеки, беззахисності, безпорадності, безвихідності, паніки.

Таким чином, ми можемо стверджувати, що тероризм набув глобального поширення, охопивши й кіберпростір.

На жаль, це явище не повною мірою вивчене. Відповідно, відсутні доречні рекомендації щодо розслідування та протидії цьому різновиду злочинної діяльності. Однак динаміка й багатогранність інформаційного тероризму унеможливлює формальний підхід до формування надійних заходів боротьби та запобігання цьому наднебезпечному явищу.

Вирішення проблеми інформаційного тероризму, на нашу думку, полягає не лише в застосуванні превентивних заходів, спрямованих на виявлення терористичних атак в інформаційному просторі, причин та умов їх здійснення, а й у ретельній роботі щодо

контролю діяльності ЗМІ[2]. Саме такий комплекс дій має забезпечити ефективність протистояння правоохоронних органів інформаційному тероризму.

ЛІТЕРАТУРА

1. Пудовочкин Ю.Е. Проблемы политического в преступлении и преступного в политике. *Библиотека криминалиста*. 2013. № 2(7). С. 5–16.
2. Телешун С.А. Сучасний тероризм – українські реалії. Окремі політико-правові зауваження. *Політичний менеджмент*. 2005. № 1. С. 163–169.
3. Украинская О.А. Феномен информационного терроризма в современном обществе. URL: http://www.crime-research.org.
4. Стрельбицький М.П., Саржан С.Л. Соціальні передумови (юридичні факти) інформаційного тероризму та кіберзлочинів. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2014. № 2. С. 217–226.
5. Остроухов В.В., Петрик В.М. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 2008. № 4. С. 135–141.
6. Тропина Т.Л. Киберпреступность и кибертерроризм. URL: http://www.crime-research.org.
7. Остроухов В.В. Засоби масової інформації та неурядові організації як засіб впливу на інформаційний простір. URL: http://westudents.com.ua/glavy/51952-rozdl-1-zasobi.

REFERENSES

1. Pudovozkin, Yu.E. (2013), “Problems of political crime and crime in politics”, *Biblioteka kryminalista*, vol. 2(7), pp. 5–16.
2. Telechun, S.A. (2005), “Contemporary terrorism is Ukrainian reality. Some political and legal remarks”, *Politychyi menedgment*, vol. 1, pp.163–169.
3. Ukrainskaya, O.A. (2015), “The phenomenon of information terrorism in modern society”, available at: http://www.crime-research.org.
4. Strelbizkii, M.P. and Sarzhan, S.L. (2014), “Social preconditions (legal facts) of information terrorism and cybercrime”, *Visnik Luhanskoho detzavnoho universitetu vnutrichnikh sprav im. E.O. Didorenka*, vol. 2, pp. 217–226.
5. Ostrouhov, V.V. and Petryk, V.M. (2008), “The problem of ensuring information security of Ukraine “, *Politychyi menedgment*, vol. 4, pp.135–141.
6. Tropina, T.L. (2012), “Cybercrime and cyberterrorism”, available at: http://www.crime-research.org.
7. Ostrouhov, V.V. “Mass media and non-governmental organizations as means of influence on the information space”, available at: http://westudents.com.ua/glavy/51952-rozdl-1-zasobi.

[2] Це потребує прийняття вдосконалених нормативних актів, які врегулюють питання свободи слова в засобах масової інформації в контексті боротьби з проявами інформаційного тероризму. Крім того, є потреба в організації міжнародного співробітництва в галузі забезпечення інформаційної безпеки, оскільки інформаційний тероризм є явищем, яке не має кордонів.