СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ
ЛІГА СТУДЕНТІВ АСОЦІАЦІЇ ПРАВНИКІВ УКРАЇНИ

ПРАВОВІ ЗАСАДИ ФУНКЦІОНУВАННЯ ПУБЛІЧНОЇ ВЛАДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНТЕЛЕКТУАЛЬНОГО РОЗВИТКУ ТА БЕЗПЕКИ СУСПІЛЬСТВА

МАТЕРІАЛИ
Міжнародної науково-практичної конференції
(Суми, 19-20 травня 2016 року)

Суми
Сумський державний університет
2016

Російський режим є головним винуватцем війни. Має бути розглянута інформаційна війна Росії проти України та світу, брехня і агресивна пропаганда Росії, світозлоба Росії, реваншизм проти Заходу, шельмування власної ліберальної інтелігенції, прихована війна (її форми, засоби і потурання інших країн).

Можна припустити, що час для такого масштабного трибуналу ще не настав. Але умова перетворення трибуналу щодо збитого Боїнга рейсу МН17 в трибунал проти військових злочинів Росії на території України має бути передбачена вже зараз.

Але найголовніше – Україна має відстоювати саме викладені вище принципи.

ЛІТЕРАТУРА:

1.Міжнародний трибунал //Політологічний енциклопедичний словник / уклад.: Л. М. Герасіна, В. Л. Погрібна, І.О. Поліщук та ін. За ред. М. П. Требіна. – Х . :Право, 2015.

2. МІЖНАРОДНИЙ КРИМІНАЛЬНИЙ СУД //Юридична енциклопедія: В 6 томах. / Редколегія: Ю. С. Шемшученко (відп. ред.) та інші. — К. : «Українська енциклопедія», 1998. ISBN 9667492001

3. Project on International Courts and Tribunals

Wolfgang Schomburg: Internationale Strafgerichtsbarkeit: Lektionen aus den UN-Tribunalen für das frühere Jugoslawien und Ruanda, Vortrag vom 18. Februar 2008 http://www.foreign-affairs.info/volltext.php?id=124

4.http://www.eurointegration.com.ua/articles/2016/03/29/7046917/

5.http://vidido.ua/index.php/pogliad/article/oficiini_visnovki_slidstva_boing_buv_zbitii_raketoju_buk/

6. http://gpu.com.ua/uk/content/mizhnarodni-tribunali-yak-instrumenti-lyudstva

7. http://zaxid.net/news/showList.do?gaazkiy_sud&tagId=51868

ЗАГАЛЬНА ХАРКТЕРИСТИКА КІБЕРТЕРОРИЗМУ ЯК ЗАГРОЗИ МІЖНАРОДНІЙ БЕЗПЕЦІ

Кіяшко Ю. М.

студент IV курсу юридичного факультету

Сумського державного університету

Наукові керівники: Ілляшенко А. В.

к. держ. упр., ст. викладач кафедри СМП юридичного факультету

Сумського державного університету

Денисенко С. І.

к.ю.н., викладач кафедри СМП юридичного факультету

Сумського державного університету

Невід’ємним елементом глобалізаційної політики у сфері міжнародних відносин є використання ІКТ, що істотно підвищує залежність населення, кожного конкретного індивіда від функціонування інформаційної інфраструктури, яка є дієвим інструментом впливу на постіндустріальне суспільство. Тому гостро постає питання ймовірного використання таких технологій у деструктивних, протиправних й антисоціальних цілях, створюючи загрозу для міжнародної безпеки. Однією із таких, відносно нових, загроз вважається кібертероризм, ключовою метою якого є проникнення у комп’ютерні мережі з ціллю порушення функціонування критично важливих об’єктів інформаційної інфраструктури.

Окремі аспекти явища кібертероризму неодноразово були предметом дослідження у роботах таких зарубіжних та вітчизняних вчених, як А. Фороса,

Д. Деннінга, К. Герасименка, М. Стрельбицького, Т. Яцик та інших дослідників.

На сучасному етапі кібертероризм, є одним із найпоширеніших проявів терористичної діяльності, динаміка розвитку якого безпосередньо пов'язана з активним впровадженням ІКТ у всі сфери життєдіяльності людства. Кібер-атаки можуть завдати значної шкоди не тільки на локальному чи державному, а й міжнародному рівні. Адже зовнішні атаки можуть переслідувати і більш важливі цілі, ніж пасивний збір даних, а об'єктами кібертероризму можуть бути грошова і секретна інформація, апаратура контролю над космічними приладами, ядерними електростанціями, воєнними комплексами, головні комп'ютерні вузли тощо [1, с. 58]. Наведений невичерпний спектр загроз від кібер-атак зумовлює необхідність детального дослідження сучасного кібертероризму як одного з видів тероризму. Адже враховуючи вагомий потенціал такого умисного діяння та відсутність комплексних міжнародно-правових методів його попередження й протидії робить це явище одним із найнебезпечніших, беручи до уваги значення інформації як ресурсу в постіндустріальному суспільстві.

Значною проблемою у дослідженні даного явища є відсутність єдиної загальноприйнятої дефініції «кібертероризму», що може свідчити, про неактивну роботу міжнародних законодавчих інститутів в даному напрямку, 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 визначенні специфіки даного прояву тероризму. Найбільш вживаним в наукових колах термін «кібертероризм», запропонований Д. Деннінгом, професором Джорджтаунського університету, авторитетним експертом в області 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» [2, с. 48]. У роботі за базове визначення взято таке розуміння кібертероизму.

Для кібертероризму, як різновиду інформаційного тероризму, залежно від часу і місця їх проведення властиві цілий ряд 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 [3, с. 224-225].

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 через один або декілька підставних комп'ютерів, що ускладнює його ідентифікацію та визначення місцезнаходження. 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) 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 [4, с. 164-165]. За останні роки кібертероризм перетнув майже всі межі, що зумовило виникнення активних дискусій навколо даного питання. Загроза тероризму в мережі виявилася більш суттєвою ніж очікувалося, а динаміка розвитку такого явища схильна до подальшого зростання.

Значним кроком для розвитку кібертероризму стало тотальне поширення Інтернету за допомогою можливостей якого можна здійснювати нелегальне втручання в інформаційні системи, в тому числі й системи державного (міждержавного) значення (аеропортів, залізниць, електростанцій та ін.) Кібертероризм став серйозною соціально-небезпечною загрозою для людства, порівняно, навіть, з ядерною, бактеріологічною і хімічною зброєю, причому ступінь цієї загрози через свою новизну, не до кінця ще усвідомлений і вивчений. Досвід, що є у світової спільноти у цій сфері, зі всією очевидністю свідчить про безперечну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів; кібертерорист здатний в рівній мірі загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі [5].

Таким чином кібертероризм, залишаючись малодослідженим явищем є однією з найбільших загроз сучасності. Основна небезпека такого прояву терористичної діяльності пов'язана зі стрімким розвитком ІКТ та відсутністю необхідної нормативної бази, що створює складність при відмежуванні такого явища від інших до нього подібних та, відповідно, наявність труднощів у питанні вироблення методів протидії. Тому, на сучасному етапі, гостро постає необхідність у формуванні міжнародно-правового режиму базовими поняттями якого мають бути інформація, інформаційно-комунікативні технології та методи їх використання з ціллю вироблення нових й удосконалення існуючих механізмів протидії кібертероризму з метою підтримання міжнародного миру та забезпечення безпеки людства.

ЛІТЕРАТУРА:

1. Яцик Т. Особливості інформаційного тероризму як одного із способів інформаційної війни / Т. Яцик. Науковий вісник Національного університету ДПС України (економіка, право). – 2 (65). – 2014. – С. 55–60.

2. 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

3. 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.

4. 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

5. Chambet P. Le cyber-terrorisme / P. Chambet [Електронний ресурс]. – Режим доступу: http://www.chambet.com/publications/Cyberterrorisme.pdf

ВІДНОСИНИ УКРАЇНИ І НАТО : ПЕРСПЕКТИВИ РОЗВИТКУ ТАКИХ ВІДНОСИН ТА МОЖЛИВІСТЬ ВСТУПУ УКРАЇНИ ДО ОРГАНІЗАЦІЇ ПІВНІЧНОАТЛАНТИЧНОГО ДОГОВОРУ

Пронський Е. А.
студент ІІ курсу юридичного факультету
Сумського державного університету
Науковий керівник: Денисенко С. І.
к.ю.н., доцент, викладач кафедри СМП юридичного факультету
Сумського державного університету

Непряма агресія РФ проти України, яка наприкінці серпня 2014 року почала переростати в обмежене вторгнення регулярних російських військ, знову повернула на порядок денний питання отримання ефективних механізмів збереження незалежності і суверенітету нашої держави. Тому логічними наслідком стало поновлення інтересу до НАТО, який в України офіційно зник в 2010 році, коли було оголошено про позаблоковість. Питання приєднання України до НАТО з кожним днем в умовах сьогодення стає більш актуальним як серед звичайних громадян України, так і серед представників вищих ешелонів влади нашої держави. Україні, її громадянам, в першу чергу потрібне мирне співіснування, відсутність міждержавних агресій та збройних конфліктів, тому актуальність інтеграції України до НАТО тільки зростає, адже відомо, що на європейському континенті саме НАТО залишається таким регіональним військово-політичним об'єднанням, який не лише дозволяє гарантувати безпеку своїм членам, а й шляхом залучення до співпраці третіх країн, створює передумови до вироблення підходів конструктивного вирішення міждержавних питань.

Спочатку розглянемо, що таке НАТО. НАТО (англійською мовою — North Atlantic Treaty Organisation, або Організація Північноатлантичного договору) — це військово-політичний союз, створений для захисту країн євроатлантичного регіону (тобто Європи і Північної Америки), насамперед від зовнішніх загроз. Метою НАТО є колективний захист його країн-членів. Головна роль НАТО полягає у забезпеченні свободи і безпеки країн-членів за допомогою політичних і військових засобів. Альянс стоїть на захисті своїх країн-членів від загрози агресії, будь-який напад на членів НАТО у Європі чи Північній Америці розглядається як «напад на всіх», і кожна з держав-членів зобов'язалася надавати допомогу союзникам.

Відносини між НАТО і Україною постійно розвиваються з самого моменту отримання Україною незалежності в 1991 році. Зважаючи на стратегічну позицію України як моста між Східною та Західною Європою, відносини між НАТО і Україною мають провідне значення для розбудови миру і стабільності в євроатлантичному регіоні. В 1994 році Україна стала першою країною — членом СНД, яка приєдналася до Партнерства заради миру, 1997 року було підписано Хартію