Черниш Р.Ф., к.ю.н. (м. Житомир, Україна)

ОКРЕМІ КРОКИ ПРОТИДІЇ СЕПАРАТИЗМУ В ІНФОРМАЦІЙНІЙ СФЕРІ, ЯК ПЕРЕДУМОВА РЕАЛІЗАЦІЇ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

Вже понад два роки прихильники т.зв. «ДНР/ЛНР» активно використовують інформаційний простір з метою впливу на свідомість громадян, що проживають на тимчасово підконтрольній бойовикам території України, як у власному «медійному ресурсі», так і у засобах масової інформації Російської Федерації.

Зокрема, ними систематично поширюються тенденційні матеріали пропагандистського характеру. Основна тематика: негативна економічна ситуації в Україні, відсутність узгодженості в діяльності вищих органів державної влади, заборгованість із виплатою заробітної платні, «переддефолтний» стан економіки, непослідовність реформ, які проводяться в державі тощо. В якості експертів, які аналізують зазначені проблемні питання, запрошуються фахівців-економістів (з РФ і ті, що проживають на підконтрольних бойовиках територіях) та викладачі Донецьких «вищих учбових закладів».

Поряд з тим, вищевказаними суб'єктами, з метою прихованого психологічного, політичного, комерційного та фізичного примусу, викривлення сприйняття реальності в Інтернет-просторі широко застосовуються маніпулятивні технології. Серед способів та технологій, які використовуються з вищевказаною метою, виділяються наступні: пряме підтасовування фактів; замовчування невигідної інформації; упередженість інтерпретації фактів; надання сфальсифікованої інформації; навішування ярликів для компрометації політиків; використання групових інтересів та ін. [4].

З метою доведення вигідної інформації до суспільства, перевага, як правило, надається електронним засобам масової інформації (Інтернет-видання), які використовують новітні інформаційні технології для розповсюдження новин.

Окремою технологією маніпулювання можна виділити т.зв. маніпулювання на форумах.

Даний вид технології полягає в коментуванні, в т.ч. анонімному, тієї чи іншої проблематики та ситуації різними користувачами Інтернет-ресурсу, що є ознакою демократизму і плюралізму Інтернету. Водночас, зацікавлені особи можуть активно втручатися у форуми, коментуючи, начебто й неупереджено, ті чи ті події. Насправді ж «голос народу» виявляється звичайним пропагандистським засобом, іноді провокативним, але завжди дієвим, бо здається об'єктивним. Маніпулювання на Інтернет-форумах соціально шкідливе, оскільки розповсюдження неправдивої інформації дискредитує сам інститут громадської думки, робить його вразливим та недієздатним [3].

На думку фахівців, сепаратистами і в подальшому активно використовуватимуться інформаційні ресурси з метою впливу на свідомість громадян (в першу чергу молоді), які проживають на сході України (насамперед на територіях, підконтрольних «ДНР/ЛНР»), що негативно впливатиме на безпеку нашої держави на фоні відсутності на вищевказаних територіях повноцінної україномовної сітки мовлення.

Зважаючи на викладене, з метою протидії інформаційній агресії, фахівцями пропонується створення єдиного комунікаційного центру, аналогічного за функціями та завданнями структурного підрозділу НАТО.

У 2014р. в Латвії було створено Центр стратегічних комунікацій НАТО (NATO Strategic Communications Centre of Excellence), серед завдань якого – забезпечити адекватну відповідь на спроби інших країн вплинути на інформаційний простір членів НАТО. Центр має опікуватися питаннями «гібридної війни» [1].

Поряд з тим, ефективним засобом посилення власних можливостей щодо координації інформаційних потоків може стати залучення до активної співпраці волонтерів. Волонтерський рух в мережі Інтернет, як інструмент протидії інформаційній агресії або для здійснення аналогічних атак на інформаційне поле супротивника, став одним із засобів протидії російській агресії проти України.

Серед українських волонтерських проектів, які діють як допоміжні віртуальні ресурси в інформаційно-психологічній війні з російськими агресорами та сепаратистськими рухами, можливо виділити Inform Napalm та «Інформаційний спротив», центр «Миротворець». Зазначені мережеві проекти є яскравим прикладом того, як за допомогою належним чином розбудованої інформаційної мережі та системи роботи можна ефективно забезпечувати та результативно супроводжувати офлайн-процеси.

Практично всі вище згадані проекти діють за схемою роботи так званої OSINT (Open Source Intelligence) – розвідувальної практики, яка передбачає пошук, вибір та збирання інформації, отриманої з відкритих джерел.

Важливою складовою такої роботи є системний аналіз наявної інформації з відповідною оцінкою та висновками, що дозволяють зрозуміти логіку та передбачити дії противника. Одним із базових правил такої практики є те, що близько 90% необхідної для аналізу та прийняття відповідних рішень інформації перебуває у відкритих джерелах.

До таких джерел відносять: традиційні ЗМІ (газети, журнали, радіо, телебачення); інтернет-видання, що відносяться до ЗМІ (новинні сайти та портали, інтернет-ресурси профільних структур); акаунти та віртуальні майданчики у соціальних мережах; офіційні звіти державних структур; публічні заяви політиків та держслужбовців; спостереження — радіомоніторинг, використання загальнодоступних даних, аерофотозйомок (наприклад, Google Earth); професійні та академічні звіти, конференції, доповіді, статті; звіти та виступи в ЗМІ окремих незалежних експертів та експертних груп [2].

Окремим негативними моментом протидії інформаційній експансії є те, що чинні законодавчі акти у сфері інформаційної безпеки здебільшого перебувають на стадії розробки або доопрацювання, внаслідок чого ускладнюється процедура правового реагування та впливу на діяльність суб'єктів інформаційного поля держави.

Так, відсутність низки законодавчо-закріплених понять у вказаній сфері негативно впливає на прийняття рішень слідчими при кваліфікації відповідних протиправних діянь.

Зокрема, диспозиція ст. 111 Кримінального кодексу України (далі КК України) передбачає відповідальність за діяння, умисно вчинене громадянином України, в т.ч. на шкоду інформаційній безпеці, хоча в національному законодавстві відсутнє тлумачення терміну "інформаційна безпека" (в окремих коментарях до ст.111 КК України також вживається поняття "інформаційної експансії"), що створює підґрунтя для правих маніпуляцій з боку зацікавлених сторін кримінального процесу (зазначений термін розуміється ними на власний розсуд через призму суб'єктивності).

Зважаючи на викладене, з метою розбудови в Україні ефективної системи інформаційної безпеки, вважаємо що на рівні відповідних вищих органів державної влади першочергові зусилля повинні бути спрямовані, насамперед, на:

– розробку зміни до чинних нормативно-правових актів, що регулюють правовідносини в інформаційній сфері, з метою усунення наявних у національному законодавстві протиріччя та прогалини. В першу чергу внесення зміни до ст.ст. 111 і 258^3 КК України (розширення поняття підривної діяльності доповненнями, що охоплюють сферу інформаційної діяльності (Інтернет, ЗМІ, соцмережі, галузь інформатизації тощо) та виокремлення інформаційного сприяння терористичній діяльності), що дозволить виробити єдиний підхід до кваліфікації злочинів у вищевказаній сфері, а також ефективно протидіяти намаганням іноспецслуб, організацій, окремих груп та осіб використовувати громадян України для створення важелів інформаційного тиску на нашу державу;

– створення національної інформаційно-телекомунікаційної системи (державного провайдера/оператора телекомунікацій);

– розвиток системи національних інформаційних ресурсів;

– інформатизацію стратегічних напрямів розвитку економіки держави, її безпеки та оборони, соціальної сфери.

Література:

1. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу [Електронний ресурс] / В. Горбулін. – Режим доступу: http://gazeta.dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html

2. Курбан О. Гібридна війна: сили спецоперацій та соціальні мережі [Електронний ресурс] / О. Курбан. Режим доступу: http://ua.racurs.ua/1064-gibrydna-viyna-syly-specoperaciy-ta-socialni-mereji?articlevolist_page=339.

3. Могилко С.В. Техніка і методи маніпуляції в інтернет-виданнях (на прикладі інтернет-газет «Прес-Центр», «Антенна») / С.В. Могилко, Н.І. Зражевська [Електронний ресурс]. – Режим доступу: http://journlib.univ.kiev.ua/index.php?act=article&article=2293.

4. Штоквиш О.А. Історична свідомість як об'єкт маніпулятивних технологій [Електронний ресурс] / О.А. Штоквиш. – Режим доступу: http://www.stattionline.org.ua/histori/107/19992-istorichna-svidomist-yak-ob-yekt-manipulyativnix-texnologij.html.