

УДК 004.738.5:351.862.4:316.472.4
DOI: 10.31733/15-03-2024/2/333-335

Олексій БЕРВЕНО

аспірант кафедри управління
та адміністрування
Дніпропетровського державного
університету внутрішніх справ

СОЦІАЛЬНІ МЕДІА ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Соціальні медіа є неабиякою силою у сучасному світі, вони змінюють спосіб, яким ми спілкуємося, отримуємо інформацію та формуємо свою думку. Ця потужна платформа володіє значним впливом на наше суспільство, включаючи його національну безпеку. Проте, разом із своїми позитивними аспектами, соціальні медіа також можуть становити загрозу для національної безпеки з ряду причин.

По-перше, соціальні медіа можуть стати ідеальною платформою для поширення дезінформації та фейкових новин. Вони дозволяють швидко та ефективно розповсюджувати неперевірену інформацію, що може сприяти паніці, соціальним конфліктам та навіть загрозам безпеці країни.

По-друге, соціальні медіа можуть бути використані для маніпулювання громадською думкою та впливу на політичні процеси. Це може включати в себе спроби залучити громадян до різних форм акцій, в тому числі й антидержавних або терористичних дій.

Крім того, соціальні медіа можуть стати майданчиком для радикалізації та розповсюдження екстремістської пропаганди. За допомогою соціальних мереж можна легко зв'язатися з людьми, які поділяють подібні переконання, що створює сприятливі умови для рекрутування нових членів до різних радикальних груп.

Нарешті, соціальні медіа можуть бути використані для кібератак на національну інфраструктуру та системи комунікацій, що також загрожує національній безпеці.

Знання використовуються для захисту свого нарративу, одночасно спотворюючи, атакуючи та розділяючи суспільство, цінності та культуру інших конкуруючих націй. Війни переходять від періодичного конфлікту до постійної конкуренції. Соціальні мережі становлять серйозну загрозу національній безпеці; Зокрема, ці загрози пов'язані з Social Engineering, атаками на веб-додатки та фішингом. Такі платформи, як Facebook та інші, загрожують національній безпеці. Іноземні ворожі організації використовують соціальні медіа як інструмент для вербування, комунікації та навчання своїх членів, а також поширюють пропаганду та радикалізацію значною мірою. У міру того, як інформаційна та психологічна війна переміщується зі звичайної сфери в кіберпростір, з розвитком технологій, платформи соціальних медіа стали кращою зброєю для суб'єктів національних держав у визначенні масового вираження на певну тему. Що стосується використання соціальних мереж, слід пам'ятати, як швидко може поширюватися інформація і наскільки великим може бути вплив віри в неправдиву інформацію на національну безпеку. Замість того, щоб відкидати соціальні медіа та сприймати національну безпеку як загрозу, уряди повинні визначити, чи можна довіряти інформації, отриманій через соціальні мережі, щоб вони могли скористатися можливостями обміну інформацією соціальних мереж [1].

Правоохоронні органи в усьому світі використовують чудову форму «розвідки з відкритих джерел» для підключення, зіставлення, аналізу, прогнозування та обміну розвідувальними даними, використовуючи дані, зібрані з соціальних мереж, також відомі як «розвідка соціальних мереж» (SOCMINT). Такі практики, як суворе дотримання, перегляд, своєчасний перегляд та знищення записаних даних, індивідуальне спостереження з боку головного спеціаліста з безпеки формування, які дозволяють новинним засобам масової інформації повідомляти про політику агентства щодо соціальних медіа для кращого дотримання та прозорості, необхідність і можуть бути включені залежно від вимог державних органів. Тут потрібне застереження, щоб ще раз наголосити, що інтелект і методи соціальних медіа не є безпомилковими, але їх можна вдосконалити та інституціоналізувати. Розвідувальна інформація, зібрана з соціальних мереж, може лише

підтримувати та надавати контекст достовірній розвідувальній інформації, зібраній правоохоронними органами, і завжди має бути перевірена [2].

Платформа соціальних мереж реструктуризувала соціальну взаємодію між колегами, бізнесом, урядами тощо. Хоча соціальні мережі сприймаються як загроза безпеці, яка в будь-який спосіб є першочерговим обов'язком і місією держав (що, можливо, є раціональним через багато факторів), безсумнівно, що платформи соціальних мереж також використовуються для розвитку соціальної та національної безпеки. Соціальні мережі можна розглядати як найпоширеніший технологічний винахід у 21 столітті. Соціальні медіа зараз є нормою соціальної комунікації в країнах, що розвиваються. Соціальні мережі пропагують позитивні та негативні плани. У глобальному масштабі терористи, сепаратисти, політичні організації, релігійні групи тощо використовують соціальні мережі для поширення своїх знань та ідей. Терористи та інші злочинні угруповання використовують соціальні мережі для оприлюднення своєї інформації, оскільки платформа дешева та легкодоступна. Окрім того, широка громадськість використовує соціальні мережі, щоб розуміти та підтримувати зв'язок з різними соціально-економічними типами.

У рамках політичних і соціальних подій соціальні медіа – це не новий винахід для суспільства, а неодмінний життєвий факт, який сприймається як належне, ніби він існував завжди. Сьогодні ці платформи вже давно стали однією з повсякденних справ у державному, приватному, громадському секторах і лише в індивідуальних та міжособистісних стосунках. Настільки, що коли людина, яка користується соціальними мережами, перестає спілкуватися, для неї це майже так, ніби життя для неї закінчилося. Соціальні медіа, завдяки своїй швидкості, економічності, впливу, поширеності та загальному прийняттю, є найдієвішим інструментом у руках будь-якої організації та групи, яка хоче ініціювати соціальний рух, як це відбувається з державами та всіма іншими інституціями, крім того, це найефективніша зброя.

Наразі роль соціальних мереж або нових медіа у зростанні проблем безпеки, соціальні медіа можна визначити як онлайн-інструменти та сервіси, що об'єднують людей і дозволяють їм взаємодіяти один з одним протягом Інтернет. Нові медіа збільшили соціальну та політичну взаємодію через WhatsApp, Facebook, Twitter, Instagram та інші платформи. Сайти соціальних мереж використовуються терористичними групами, які мають приватні сервери та веб-сайти для поширення своєї пропаганди. Вони використовують засоби масової інформації для вербування, збору коштів, механізмів передачі інформації та інших форм кіберзлочинності. Ця платформа допомагає пропагувати місцеві та міжнародні терористичні групи та пов'язану з ними небезпеку. Міжнародні та місцеві терористичні групи використовують соціальні медіа для організації нападів і шляхів втечі або для організації стратегій [3].

Соціальні медіа використовуються терористичними групами не лише для того, щоб кинути виклик миру та стабільності в країні, але й трапляється, що самі громадяни використовують навколишнє середовище для тероризування один одного за допомогою фейкових новин та фальшивої реклами. Також очевидно, що терористи та інші злочинні угруповання часто використовують соціальні мережі для оприлюднення своїх знань та реалізації своїх стратегій. Незважаючи на те, що інформаційне забруднення спричиняє багато аномічних ситуацій, які можна назвати інформаційними бомбардуваннями та інформаційним розмиттям, тепер усі добре знають; Соціальні мережі – це найпростіший спосіб робити все, що він хоче, особливо в соціальному вимірі. Від торгівлі до політики, від пропаганди до маніпуляцій, від дії до мови – соціальні медіа готові працювати з усім своїм особливим потенціалом і можливостями.

Сьогодні потоки соціальних мереж, такі як Twitter, являють собою велику кількість щоденних даних про потоки в режимі реального часу. Теми в цих потоках охоплюють всі види людського спілкування, від обміну інформацією про будь-який продукт, предмет або актив, який тільки можна собі уявити. Для публічних заходів стало нормою спочатку повідомляти новини про потоки в соціальних мережах, але потім мейнстрімні ЗМІ, які отримали цю новину, наслідували цей приклад. У літературі було висловлено припущення, що соціальні медіа є дійсним, цінним та ефективним інструментом у режимі реального часу для вимірювання суб'єктивних реакцій людей на події та активи. У зв'язку з «великими даними», що генеруються в щоденних потоках соціальних мереж, монетизація та вимірювання реакції громадськості мають бути автоматизованими та найбільш доцільними. Спільнота кризового реагування використовує Twitter та подібні соціальні мережі без особливого успіху для управління кризами під час конфліктів, природних або техногенних катастроф. Уряди та правоохоронні органи також шукають шляхи моніторингу та

передбачення насильства, а також аналізу реакції громадськості на різні події з точки зору національної безпеки. Моніторинг соціальних мереж був представлений як новий корисний ресурс для ситуаційної обізнаності під час терористичних інцидентів. Однак, як показують автори, автори дбають про те, щоб приділити увагу етичним питанням, пов'язаним із поширенням надмірних публікацій у Twitter під час тероризму, оскільки це може допомогти з порядком денним нападників [4].

Отже, соціальні медіа, хоча і є надзвичайно важливим інструментом для комунікації та обміну інформацією, можуть також становити серйозну загрозу національній безпеці через поширення дезінформації, маніпуляцію громадською думкою, радикалізацію та кібератаки. З цього приводу важливо вживати заходів для виявлення та боротьби з такими загрозами, зберігаючи при цьому принцип свободи слова та відкритого доступу до інформації.

1. Salik, H., ve Iqbal, Z. (9 Eylül 2019). The Geopolitics. URL : <https://thegeopolitics.com/social-media-and-national-security/>
2. Shruti, P. (2016). The Social Media Challenge to National Security: Impact and Opportunities. New Delhi: Institute for Defence Studies and Analyses.
3. Chukwuere, J. E., ve Onyebukuva, C. F. (2018). The Impacts of Social Media on National Security: A View from the Northern and South-Eastern Region of Nigeria. International Review of Management and Marketing, 8(5), 50-59.
4. Sykora, M. D. (2013). National Security and Social Media Monitoring: A Presentation of the EMOTIVE and Related Systems. European Intelligence and Security Informatics Conference.

УДК 355.40

DOI: 10.31733/15-03-2024/2/335-336

Богдан ВІННІЧУК

здобувач кафедри
національної безпеки

Владислав СТРЕЛКОВ

старший викладач кафедри
національної безпеки
Волинського національного
університету імені Лесі Українки,
доктор філософії

РОЛЬ OSINT-РОЗВІДКИ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Національна безпека в сучасному світі є міждисциплінарною діяльністю у сфері державотворення та націєтворення. Цей аспект діяльності охоплює всі без винятку аспекти державності та інших суспільних практик та інститутів, оскільки становить собою умову якісного функціонування політичної системи держави й суспільства, а також супроводжує управлінський цикл на всіх етапах, окрім того, національна безпека стосується й соціальної та політичної прогностики, що дозволяє в подальшому передбачувати наслідки реалізації тих чи інших інтересів, потреб та ідей [1].

Розвідка як невіддільний від національної безпеки елемент структури гарантування забезпеченості й захищеності нації провадить власне буття в різних формах, одна з них – розвідка з відкритих джерел, тобто OSINT. Отже, дослідження взаємопов'язаності цих двох феноменів, системи та підсистеми становить істотний інтерес для сучасного та подальшого покоління наукових досліджень у межах окресленої тематики.

Розвідка та національна безпека тісно пов'язані між собою, оскільки розвідка забезпечує своєчасну та достовірну інформацію про потенційні або реальні загрози національним інтересам, а також про можливості та наміри супротивників. Розвідка допомагає приймати обґрунтовані рішення щодо захисту національної безпеки, планувати та виконувати заходи протидії, а також визначати пріоритети та ресурси для забезпечення національної безпеки. Розвідка також сприяє розвитку та підтримці міжнародного співробітництва у сфері безпеки, обміну інформацією та досвідом, а також підвищенню