УДК 316.6:659.9]:004.7 (043.3)

ІНТЕРНЕТ-ТЕХНОЛОГІЇ ТА ОНЛАЙНОВІ СОЦІАЛЬНІ МЕРЕЖІ У СУЧАСНІЙ ГІБРИДНІЙ ВІЙНІ

О. В. Курбан

Військовий інститут
Київського національного університету ім. Т. Шевченка
вул. Михайла Ломоносова, 81, Київ, 03680, Україна

Висвітлено можливості та перспективи використання онлайнових соціальних мереж для забезпечення реалізації завдань сучасної економічної, політичної або інформаційної війни. Розглянуто попередні розробки українських та зарубіжних дослідників, зокрема Г. Почепцова, Д. Халілова, Д. Тимчука, В. Гусарова та ін. Проаналізовано сучасні технології web 2.0–3.0, що є базовими для онлайнових соціальних мереж, а також на прикладі зовнішньої та внутрішньої політики України розглянуто аспекти ведення інформаційних війн в онлайнових соціальних мережах.

Ключові слова: *інформаційна війна, гібридна війна, он-лайнові соціальні мережі.*

Постановка проблеми. Сучасна інформаційна війна є війною сенсів та ідеологій. Отже, одним із головних завдань мережевих онлайн-проектів в умовах гібридної війни є створення якоїсь віртуальної реальності, що формує необхідне для нападника бачення ситуації конкретними цільовими групами, які є об'єктами інформаційно-психологічної агресії. Головною метою такої діяльності є забезпечення сприятливих умов для реалізації атак у режимі офлайн або окремо в економічній, військовій, політичній чи інших сферах, або в усіх сферах одночасно.

Мета статті — висвітлити можливості та перспективи використання онлайнових соціальних мереж, для забезпечення реалізації завдань сучасної економічної, політичної або інформаційної війни.

Виклад основного матеріалу дослідження. Поставлена мета передбачає вирішення таких головних завдань:

- дослідження історіографічного контексту порушеної проблематики;
- огляд сучасного стану розвитку технологій web 2.0–3.0;
- розгляд сучасних прикладних інструментів проведення інформаційної війни в онлайнових соціальних мережах.

Дослідження прикладних аспектів супроводження інформаційних війн, зокрема в онлайнових соціальних мережах, досі не забезпечено належним чином. Деякі загальні аспекти порушено у працях Г. Почепцова, Д. Халілова, Д. Коника та С. Рендел [3; 5–7; 10–11]. Це питання свого часу досліджували у своїх працях вузькопрофільні українські фахівці Д. Тимчук, В. Гусаров, Ю. Карін, К. Машовець [9].

Вирішення зазначених питань можливо лише за умови інтегрованого підходу, тобто поєднання сучасних техніко-комунікаційних і психотехнологій. При цьому тривалість дії та глибина ударного ефекту залежать від часу, впродовж якого здійснюється опрацювання свідомості цільових груп, а також потужності тиску. Роль і значення онлайнових соціальних мереж у цих процесах важко переоцінити.

Технології web 2.0–3.0 можна визначити як високоточну зброю, що може поцілити не просто в окремі цільові групи, а й в конкретних її представників, чітко визначені персоналії. Така адресність, а за потреби і вибірковість, дає змогу досягати максимального ефекту із оптимізацією витрат часу, інтелектуальних та матеріально-технічних ресурсів.

Аналізуючи результати найвідоміших міжнародних військових, політичних та економічних конфліктів кін. XX — поч. XXI ст., стає зрозумілим, що інформаційно-психологічну зброю сьогодні треба прирівняти до зброї масового знищення. Не вбиваючи фізично, психотехнології спричиняють групові, а також масові психічні розлади, вибухаючи згодом у соціальні конфлікти, жертвами яких стають конкретні індивіди.

Використовуючи весь спектр інформаційно-психологічних операцій, онлайнові соціальні мережі можуть забезпечувати:

– координацію протестних та терористичних рухів;
– поширення контенту, що належить до категорії інформаційної зброї;
– збирання важливої для нападника інформації про персони або організації;
– збирання розвідувальної інформації про офлайн-дії противника;
– відстежування суспільних настроїв;
– локалізацію джерел інформації, що стновлять небезпеку.

Однією з головних функцій онлайнових соціальних мереж є можливість координації інформаційних потоків, що розгортаються навколо реальних військових дій.

В умовах сучасних гібридних і лінійних військових конфліктів важливе значення має система доступу до інформації, що надходить із зони бойових дій. А головним завданням будь-якої профільної військової структури є обмеження доступу до джерел інформації сторонніх осіб і поширення інформації у вигідному для себе контексті. Для реалізації зазначеного вище завдання роботу із соціальними мережами потрібно вибудовувати на принципах встановлення контролю над трьома інформаційними потоками, які зосереджені навколо будь-якого об’єкта, зокрема зони бойових дій.

Для чіткого розуміння процедури здійснення контролю за рухом інформації потрібно скласти карту інформаційного поля, на якій змоделювати спрямування та складові частини трьох базових інформаційних потоків: ***вхідного***, ***вихідного*** та ***внутрішнього*** [4, с. 42].

Кожен із визначених інформаційних потоків формують окремі джерела інформації або інформаційні носії, які мають контент, механізм його нагромадження, зберігання та поширення, формуючи загальні обриси та структуру профільного інформаційного процесу. Серед тих, що належать до онлайн мережевих соціальних структур, можна виокремити такі:

– мережеві групи та сторінки центральних органів державної влади;
– мережеві групи та сторінки органів місцевої влади;
– мережеві групи та сторінки координаційних центрів громадських структур (волонтери, ГО, БФ та ін.);
– мережеві групи та сторінки окремих силових підрозділів;
– мережеві групи та сторінки координаційних центрів силових структур (штаби, логістичні центри, центри надання допомоги);
– мережеві групи та сторінки місцевих ЗМІ;
– мережеві групи та сторінки територіальних громад.

Для цих інформаційних потоків визначають окремі цільові групи. Зокрема, для вхідного та внутрішнього інформаційного потоку такими цільовими групами є:
– цивільне населення в зоні конфлікту;
– керівництво місцевих органів влади;
– силовики (військові та поліцейські структури);
– волонтерські структури (благодійні або громадські організації);
– представники ЗМІ (власні та іноземні);
– офіційні спостерігачі (військові та цивільні місії).

Для контенту, що рухається за вихідним інформаційним потоком, цільовими групами є:
– цивільне населення, що мешкає поза зоною конфлікту;
– керівництво центральних органів влади;
– національні та іноземні медіа;
– представники національних та міжнародних громадських організацій;
– керівництво та представники іноземних державних установ.

Карта інформаційного поля в кожній конкретній ситуації формується індивідуально, на основі визначених вище елементів із врахуванням місцевих особливостей та специфіки.

Для перетворення такої моделі на справді дієвий механізм також потрібно визначити принципи й правила контролю та фільтрації інформаційних потоків. У роботі із соціальними мережами це завдання є доволі складним, бо потенційним джерелом інформації може бути будь-яка людина, яка має доступ до мережі інтернет і володіє цінним контентом. У такому разі потрібно налагодити систему регулярного моніторингу всього локального мережевого інформаційного простору в ручному форматі (переглядання змісту профільних сторінок та груп) або за допомогою відповідних програмних сервісів.

Крайнім заходом контролю за мережевим складником зони конфлікту може бути блокування доступу до деяких інтернет-ресурсів та мереж. Утім, як свідчить практика, сьогодні це майже не реально. Тому найкращий засіб контролю за інформаційним процесом — це координування інформаційних потоків та формування правильних меседжів із відповідним контентним супроводом.

Ефективним засобом посилення власних можливостей щодо координації інформаційних потоків може стати залучення до активної співпраці волонтерів. Волонтерський рух в онлайновому мережевому середовищі як інструмент протидії

інформаційній агресії або здійснення аналогічних атак на інформаційне поле супротивника став одним із засобів протидії російській агресії проти України. Загалом світова практика інформаційних війн знає багато таких прикладів.

Практичний приклад

За прикладом використання соціальних мережевих онлайн структур для забезпечення військового протистояння із залученням волонтерів можна звернутися до досвіду інформаційного супроводження військової операції «Литий свинець», яку організовував Ізраїль у Секторі Гази у 2009 р. Ця віртуальна інформаційно-психологічна операція стала однією з перших та найуспішніших.

Внаслідок прикордонного інформаційного протистояння під час Другої Ліванської війни (2006 р.) ізраїльське керівництво вирішило посилити інформаційний сегмент у структурі ЦАХАЛ та його тісну співпрацю із громадськістю. До співпраці, окрім офіційних ЗМІ, залучили також волонтерів, головним завданням яких було відстежувати інформацію, що з'являлася у соціальних мережах, та поширювати контент, який дає об'єктивну інформацію про перебіг подій і показує діяльність ізраїльських військових у вигідному для них контексті. Також волонтерські групи та окремі блогери орієнтувалися на виявлення та нейтралізацію джерел (інтернет-майданчиків) противника.

Реальні бойові дії розпочалися 27 грудня 2008 р., і вже на початку січня 2009 р. провідні блогери-волонтери відкрили у найпопулярнішій тоді соціальній мережі LiveJornal.com групу «gaza2009» (рис. 1). Модераторами цієї групи стали Марк Бибичков (радник міністра оборони Ізраїлю) та Давід Ейдельман (прес-секретар політичної партії «Кадима»).

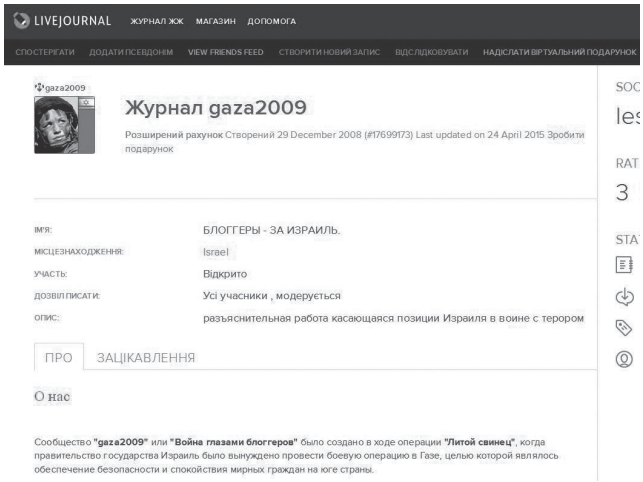

Рис. 1. Група «gaza2009»

Зазначена група стала майданчиком, навколо якої консолідувалась громадськість, а також джерелом інформації для світових медіа. Модераторам вдалося досягнути рівня відвідуваності до 30 тис. на день, що на ті часи та для цієї соціальної мережі було рекордом.

Крім того, зазначена група виконувала функції віртуального штабу. У разі виявлення джерел ворожої пропаганди модератори збирали всіх волонтерів та давали адресу місця, де відбувається ворожа інформаційна атака. Фоловери групи також виявляли та розвінчували фейки, поширюючи викривальну інформацію. За деякий час аналогічні групи з'явилися у мережах Facebook, Odnoklassniki, VKontakte.

Станом на січень 2010 р. ця діяльність перетворилась на глобальний рух, який допоміг ізраїльським військовим у плані комплексного інформаційного супроводу.

Серед аналогічних українських волонтерських проектів, як допоміжних віртуальних ресурсів у інформаційно-психологічній війні з російськими агресорами та сепаратиськими рухами, можна визначити такі, як «Inform Napalm», «Информационное сопротивление», центр «Миротворець» [1; 2; 12].

Практично всі зазначені проекти діють за схемою роботи так званої **OSINT (Open source intelligence) —** ***розвідувальної практики, яка передбачає пошук, вибір та збирання інформації, отриманої із відкритих джерел.*** Важливою частиною такої роботи є системний аналіз наявної інформації із відповідною оцінкою та висновками, що дають змогу зрозуміти логіку та передбачити дії противника.

Одним із базових «золотих правил» такої практики є те, що близько 90 % інформації, потрібної для аналізу та ухвалення відповідних рішень, уміщені у відкритих джерелах. До таких джерел можна зарахувати:

- традиційні ЗМІ (газети, журнали, радіо, телебачення);
- інтернет-видання, що належать до ЗМІ (новинні сайти та портали, інтернет-ресурси профільних структур);
- акаунти та віртуальні майданчики у онлайнових 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.

У провідних країнах світу система OSINT є важливим інструментом захисту національних інтересів та провідною складовою в діяльності профільних силових відомств. Зокрема, в США та країнах НАТО існують окремі мережі центрів, що збирають і опрацьовують відповідну інформацію, формуючи відповідні бази даних та застосовуючи їх для ухвалення відповідних рішень.

Практичний приклад

«***Inform Napalm***» (https://informnapalm.org) — громадський проект з інформаційного висвітлення подій, що стосуються неоголошеної війни Росії проти України, окупації Криму і терористичної діяльності російських спецслужб, а також фанатично налаштованих бойовиків «ДНР», «ЛНР», «Новоросії» (рис. 2). На волонтерських засадах у команду «InformNapalm» увійшли колишні військові, журналісти, аналітики, перекладачі та активісти. У мирному житті кожен із них репрезентує найрізноманітніші професії, але з приходом війни в Україну усі вони стали солдатами інформаційного фронту.

На сьогодні серед волонтерів проекту є ті, що перебувають у зоні АТО як військовослужбовці. Також до співпраці залучають місцевих мешканці в окупованих територіях.

Серед матеріалів, які активісти проекту публікують, є фото- та відеоматеріали, офіційні документи, свідчення очевидців, що підтверджують російську агресію та розкривають військові злочини бойовиків «ДНР-ЛНР».

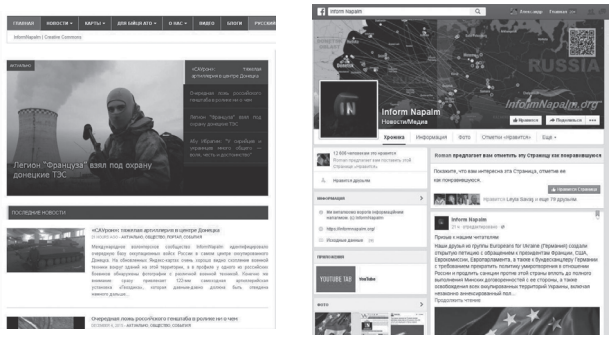

Рис. 2. Портал «ІнформНапалм»

«***Информационное сопротивление***» (http://sprotyv.info) — неурядовий проект, головним завданням якого є протидія в інформаційному полі зовнішнім загрозам, що виникають для України в основних сферах: військовій, економічній, енергетичній, а також у сфері інформаційної безпеки (рис. 3).

Рис. 3. Медіа-група «Інформаційний спротив»

Проект функціонує як ініціатива неурядової організації «Центр військово-політичних досліджень» (м. Київ). Проект розпочався 2 березня 2014 року (день вторгнення Росії до Криму).

Матеріали, що публікують на сайті та мережевих сторінках проекту, — це візуальні (фото та відео матеріали), офіційні документи, свідчення та коментарі очевидців, що надають докази російської агресії та злочинів керівництва «ДНР-ЛНР».

Одним із найважливіших та найпопулярніших ресурсів є портал «***Миротворець***» (https://psb4ukr.org/), який створила група вчених і фахівців з питань дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку, що займаються творчою, науковою та журналістською діяльністю (рис. 4).

Рис. 4. Портал «Миротворець»

Волонтери центру фіксують і зберігають інформацію щодо об’єктів дослідження, в діях яких є ознаки злочинів проти національної безпеки України, життя і здоров’я людини, миру, безпеки людства та міжнародного правопорядку (рис. 5).

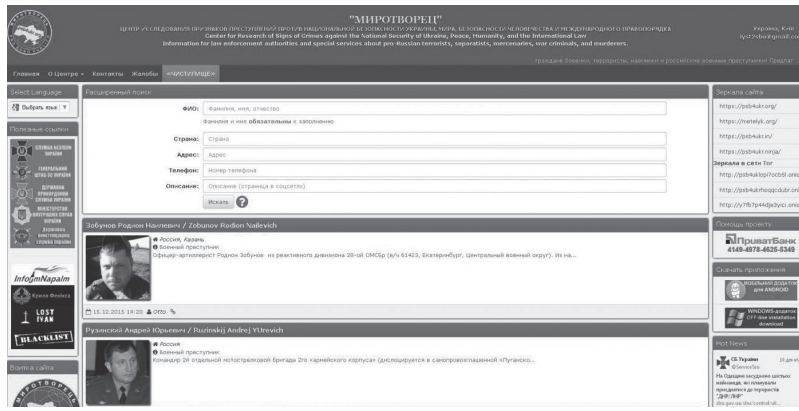

Рис. 5. База персоналій порталу «Миротворець»

Основними джерелами інформації для проведення наукових досліджень центру «Миротворець» є відкриті для загального доступу матеріали, які розміщені в соціальних мережах, у web-виданнях, на приватних web-сторінках, у спеціалізованих форумах і блогах, транслюються на каналах телебачення і радіомовлення.

Зазначені вітчизняні мережеві проекти демонструють, та як за допомогою розбудованої інформаційної мережі та системи роботи можна ефективно забезпечувати та результативно супроводжувати офлайн-процеси.

Отже, ми простежили весь спектр наявних на сьогодні інструментів ведення інформаційної війни, головний принцип яких полягає у гнучкості, оперативності та масштабності процесів системної роботи. І лише від тих, хто ухвалює відповідні управлінські рішення, залежить те, наскільки якісно ці інструменти можуть працювати.

Висновки. Проаналізувавши матеріали досліджуваної тематики, можемо стверджувати, що сьогодні в арсеналі фахівців із ведення інформаційних війн в онлайнових соціальних мережах нагромаджено достатню кількість практичних інструментів виробництва, зберігання, поширення та збирання контенту, що є базовою сутністю та змістом інформаційного протистояння. Ці технології належать до форматів web 2.0 та web 3.0, уособлюючи сучасні тенденції у мережевому онлайн-середовищі. Алгоритм планування та реалізації таких процесів оснований на принципах розбудови карти інформаційного поля та структури комунікаційного процесу, що властиві як офлайн-, так і онлайн-варіантам інформаційної діяльності.

Спираючись на власний досвід ведення інформаційної війни (відсіч російській гібридній агресії), українські фахівці повною мірою володіють можливостями забезпечення ефективних протистоянь (економічних, політичних, військових) та здатні підтримувати необхідний рівень національної інформаційної безпеки в онлайнових соціальних мережах. Підтвердженням цього є такі проекти, як «Інформаційний спротив», «Миротворець», «InformNapalm» [1; 2; 12].

Тим, хто досліджує питання інформаційної війни в онлайнових соціальних мережах, радимо звернути увагу на розробку прикладних алгоритмів роботи та механізмів моніторингу відповідних процесів. Це дасть змогу підвищити ефективність роботи як окремих профільних фахівців, так і якісно поліпшити діяльність відповідних силових структур у системі національної інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «InformNapalm» (Про нас) [Електронний ресурс]. InformNapalm [сайт]. URL: https://psb4ukr.org.
2. «Информационное сопротивление» (О нас) [Электронный ресурс]. Информационное сопротивление [сайт]. URL: http://sprotyv.info.
3. Конык Д., Рендел С. Расставьте сети. Как использовать Интернет в интересах вашего бизнеса. Киев : ЛИК, 2011. 120 с.
4. Курбан О. В. PR у маркетингових комунікаціях : навч. посіб. Київ : Кондор-Видавництво, 2014. 246 с.

5. Почепцов Г. Від Facebook'у і гламуру до Wikileaks: медіа комунікації. Київ : Спадщина, 2012. 464 с.
6. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс]. Media sapiens [сайт]. URL: http://osvita.mediasapiens.ua/trends/1411978127/ novye_podkhody_v_ sfere_zhestkikh_infovoyn/.
7. Почепцов Г. Г. Информационные войны. Новый иснтрумент политики. Москва : Алгоритм, 2015. 256 с.
8. Самохвалова Л. Московський слід колорадського Жука, або Хто і як готує «Майдан-3» [Електронний ресурс]. Укрінформ [сайт]. URL: http://www.ukrinform.ua/ rubric-politycs/ 1948496-moskovskij-slid-koloradskogo-zuka-abo-hto-i-ak-gotue-majdan 3 .html.
9. Вторжение в Украину: хроника российской агрессии. Тымчук Д., Карин Ю., Машовец К., Гусаров В. Киев : Брайт Стар Паблишинг, 2016. 240 с.
10. Халилов Д. Маркетинг в социальных сетях. Москва : Ман, Иванов и Фербер, 2013. 240 с.
11. Халилов Д. Мониторинг социальных сетей и блогов [Электронный ресурс]. Энциклопедия маркетинга. URL: http://www.marketing.spb.ru/lib-comm/internet/ smm_monitoring. htm?printversion.
12. Центр «Миротворец» [Электронный ресурс]. Миротворец. URL: https://informnapalm.org.

REFERENCES

1. «InformNapalm» (Pro nas). InformNapalm. Retrieved from https://psb4ukr.org (in Ukrainian).
2. «Informatcionnoe soprotivlenie» (O nas). Informatcionnoe soprotivlenie. Retrieved from http://sprotyv.info (in Russian).
3. Konyk, D. & Rendel, S. (2011). Rasstavte seti. Kak ispolzovat Internet v interesakh vashego biznesa. Kiev : LIK (in Russian).
4. Kurban, O. V. (2014). PR u marketynhovykh komunikatsiiakh. Kyiv: Kondor-Vydavnytstvo (in Ukrainian).
5. Pocheptsov, H. (2012). Vid Facebook'u i hlamuru do Wikileaks: media komunikatsii. Kyiv: Spadshchyna (in Ukrainian).
6. Pocheptcov, G. Novye podkhody v sfere «zhestkikh» infovoin. Media sapiens. Retrieved from http://osvita.mediasapiens.ua/trends/1411978127/ novye_podkhody_v_ sfere_zhestkikh_ infovoyn/ (in Russian).
7. Pocheptcov G. G. (2015). Informatcionnye voiny. Novyi isntrument politiki. Moskva : Algoritm (in Russian).
8. Samokhvalova, L. Moskovskyi slid koloradskoho Zhuka, abo khto i yak hotuie «Maidan-3». Ukrinform. Retrieved from: http://www.ukrinform.ua/ rubric-politycs (in Ukrainian).
9. Tymchuk, D., Karin, Iu., Mashovetc, K. & Gusarov, V. (2016). Vtorzhenie v Ukrainu: khronika rossiiskoi agressii. Kiev : Brait Star Pablishing (in Russian).
10. Khalilov, D. (2013). Marketing v sotcialnykh setiakh. Moskva : Man, Ivanov i Ferber (in Russian).
11. Khalilov, D. Monitoring sotcialnykh setei i blogov. Entciklopediia marketinga. Retrieved from http://www.marketing.spb.ru/lib-comm/internet/ smm_monitoring.htm? printversion (in Russian).
12. Tcentr «Mirotvoretc». Mirotvoretc. Retrieved from https://informnapalm.org (in Russian).

INTERNET TECHNOLOGY AND ONLINE SOCIAL NETWORKS IN MODERN HYBRID WAR

O. V. Kurban

Military Institute
of Taras Shevchenko National University of Kiev,
81, Mihaylo Lomonosov St., Kyiv, 03680, Ukraine
kurbanbairam0791@gmail.com

The article deals with opportunities and prospects for the attraction of online social networks to provide the implementation of objectives of the current economic, political or information war. It considers the preliminary development of domestic and foreign researchers, including H. Pocheptsov, D. Khalilov, D. Tymchuk, V. Husarov and others. Also the article presents the analysis of the modern technologies of web 2.0–3.0, which are the basis for social online networks. In practical examples of internal and external policy of Ukraine, it gives the discussion of aspects of the information war in online social networks.

Keywords: *information war, hybrid war, online social networks.*

Стаття надійшла до редакції 20.12.2016.
Received 20.12.2016.