оточення. Буде потрібно час для того, щоб людина знову почала відчувати смак життя.

Література:

1. Давиденко Н.В. Программа психологической коррекции Интернет-зависимого поведения с использованием методов когнитивной психоотерапии / Н.В. Давиденко, М.М. Акопова. // Актуальные проблемы психол. знания. – 2010. - № 3.
2. Психология зависимости : хрестоматия / сост. К.В. Сельченок. - Минск : Харвест, 2007. 3.
3. Ускова Л. Подход к терапии при Интернет-зависимости // Материалы III Всеукраинской науч.-практ. конф. «Феномен зависимости», 17-18 мая 2008 г., г. Днепропетровск, 2008.

Сучасні комунікаційні технології, інформаційни війни і збройні конфлікти

Раад Лейс (Сирія)
Науковий керівник – ст. викладач Кальниченко Н.М.
ХНУМГ

Ми говоримо, що сучасні комунікаційні технології допомагають встановити нові дружні зв'язки між людьми, яких розділяють культурні бар'єри, кордони і відстані. Але в той же час ці технології маскують боротьбу між провідними державами світу за встановлення свого панування в інформаційному просторі.

В даний час Інтернет все активніше використовується в інтересах інформаційного протистояння конфліктуючих сторін і для усунення неугодних режимів. Мережа надає широкі можливості здійснення впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, а також впливу на інформаційні ресурси противника і поширення дезінформації. Активне її використання обумовлене рядом переваг мережі перед звичайними засобами і технологіями: оперативність, економічність, скритність джерела впливу, дистанційний характер впливу, масштабність можливих наслідків, сприйняття інформації та її доступність.

В даний час спецслужби різних країн використовують блоги, соціальні мережі, електронні карти і сайти відеохостингу для публікації інформації - від альтернативного погляду на політику і історію до расистських і

націоналістичних матеріалів, що має вплив на аудиторію в потрібному напрямку. Ефективність подібної діяльності істотно зростає в міру розширення аудиторії та швидко отримує підтримку однодумців з різних країн світу. Наприклад, на порталі «Facebook» можна знайти групи «Бельгії не існує», «Абхазія – це не Грузія», «Ненавиджу Пакистан» та багато інших.

Дослідження в сфері міжнародного інтернет-спілкування свідчать про те, що уряди деяких країн активно використовують інформаційні технології для розпалювання ненависті між людьми різних рас і провокують вибух націоналістичних ініціатив у світі. Так, в 2005 році словацькі націоналісти фоном своєї сторінки в Інтернеті вибрали карту Європи, на якій була відсутня Угорщина. У 2007 році в одному з угорських інтернет-сайтів провели конкурс на кращий антициганській плакат. Інший приклад: молодий китаєць в 2006 році на сайті опублікував матеріали антикитайської спрямованості західних засобів ЗМІ. Американські спецслужби спробували перешкодити цьому сайту, але власник послав сигнал про допомогу, на який відгукнулися понад тисячу користувачів. І потім цей сайт став локомотивом китайського націоналізму в віртуальному просторі, через що почалися вуличні протести і масові кампанії, які бойкотували американські бренди .

За останній час число сайтів, які створені для розпалювання ненависті, збільшилося на 30%, офіційно склавши близько 10 тисяч. У міру еволюції мобільного зв'язку стали з'являтися все нові засоби інформаційно-психологічного впливу. Мобільні інтернет-портали та SMS мають великий потенціал для використання в інтересах спецслужб. Це дає можливість збирати маси людей в потрібному місці в потрібний час. У світі популярне таке явище, як flash-mob (миттєвий натовп). Розсилка закликів до мітингів і демонстрацій сьогодні також відбувається по мобільному зв'язку.

Акці протесту в Єгипті в 2011 році координувалися через Інтернет, а також через оповіщення молоді про місце і час їх проведення. У цій країні користується соціальними мережами кожен третій єгиптянин.

Фахівці пов'язують зростання популярності «Фейсбук» в цьому регіоні з можливостями для вираження незгоди з діями влади і організації антиурядових демонстрацій. У зв'язку з цим деякі західні ЗМІ назвали події в Тунісі і Єгипті «Фейсбук- і Твіттер-революцією».

Повстання в Лівії також почалося з публікацій компромату на сім'ю лівійського лідера М. Каддафі. За словами лідера лівійської опозиції Омара Ш. Махмуда, для виведення людей на вулиці був використаний сайт знайомств «Мавада», який знаходився поза зоною уваги поліції. Цей сайт об'єднав понад 170 тисяч противників М. Каддафі.

В даний час є безліч прикладів, коли задіюють мережі для проведення інформаційних операцій. Один із прикладів – це події навколо Югославії. Серби і косовські албанці активно використовували Інтернет в інтересах того, що потім було названо першою онлайновою війною – коли поширювали інформацію через веб-сайти і електронну пошту, щоб відстоювати власну інтерпретацію національної історії.

Використання Інтернету при проведенні психологічних операцій дає ще одну можливість - це контакт з противником без урядових структур або пропаганди. Під час авіанальотів і ракетних ударів блоку по Югославії деякі ЗМІ і користувачі глобальної мережі спілкувалися за допомогою електронної пошти та чатів.

Аналітичні служби рекомендують дослідити можливості Інтернету в плані посилення психологічного впливу в ході спецоперацій, що проводяться за межами країни.

Таким чином, в даний час фахівці не тільки розглядають Інтернет як одне з найважливіших і дієвих засобів впливу в ході психологічних операцій під час збройних конфліктів, а й активно його використовують.

Можливості Інтернету активно використовують також екстремістські і терористичні організації для пропаганди расової, релігійної та інших форм нетерпимості. Розвиток нових інформаційних технологій відкрило тероризму

нові кордони і зумовило появу нового, не менш небезпечного його різновиду - кібертероризму. Такі сайти можна розділити на чотири основні групи:

- Сайти, які поширюють ідеї екстремізму, сепаратизму і тероризму, здійснюють пропаганду радикальних течій ісламу, ідеї джихаду і боротьби з «невірними».

-Інформаційні ресурси. Ці сайти закликають до здійснення терактів, пропагують сепаратизм, релігійну нетерпимість та міжнаціональну ворожнечу.

- Сайти, що розпалюють ксенофобію на основі расової або національної приналежності. Сюди входять інтернет-ресурси антисемітського характеру.

- Інтернет-ресурси довідкового характеру.

На таких сайтах можна знайти інформацію про те, як виготовити зброю, отримати отруйні речовини, зібрати саморобний вибуховий пристрій. Такі сайти можуть бути в будь-якій точці мережі, так як їх інформація надається як довідкова, вони недовговічні і часто змінюють доменні імена.

Цілі використання терористами мережі Інтернет різноманітні:

- доступ до ЗМІ і пропаганда терористичної діяльності;

- створення сайтів з докладною інформацією про терористичні рухи, їх цілі і завдання, публікація даних про час і зустрічі людей;

- використання Інтернету для звернення до масової аудиторії про майбутні дії, розсилка повідомлень по електронній пошті, а також повідомлення терористів про свою відповідальність за вчинення терактів;

- «всесвітня павутина» здатна посіяти паніку, ввести в оману, привести до руйнування емоційних і поведінкових установок людини.

Це тільки здається, що Інтернет надійний і має високу репутацію. Але він ще став благодатним грунтом для поширення різних чуток (в тому числі тривожних) і агітаційних матеріалів. Терористи з угруповання ХАМАС, наприклад, створили кілька сайтів, які орієнтовані на дітей. Тут діти можуть завантажити відеогру, сюжет якої війна з ізраїльтянами в Лівані.

Завдяки мережі члени «Аль-Каїди» можуть зв'язуватися один з одним не тільки для того, щоб запланувати атаки, але і для вирішення тактичних завдань під час їх проведення.

Шифрування повідомлень і передача їх через Інтернет стало повсякденною практикою мусульманських екстремістів в Афганістані, Албанії, Великобританії, Кашмірі, Косово та інших місцях. У своїй доповіді конгресу колишній директор ФБР У. Фрі наголошував на тому, що застосовувалося головним чином шифрування, а не стеганографія.

Інтернет став для багатьох терористичних угруповань свого роду «відкритим університетом» для підготовки нових активістів і виконавців терактів, де пропонуються інструкції по викраденню людей або використання стільникових телефонів для проведення вибухів.

Ще один вид подібної діяльності через Інтернет, – електронний джихад. Західні експерти не виключають, що ісламісти можуть атакувати життєво важливі інфраструктури. Якщо звичайний терорист застосовує вибухівку або зброю, то кібертерорист використовує сучасні інформаційні технології і системи. Торгові центри, банки, біржові ринки - це найбільш можливі мішені майбутніх атак ісламських терористів. Інша стратегія бойовиків - злом комп'ютерних систем оборони або систем водопостачання. Атаки кібертерористів можуть зупинити електропостачання, викликати збої в управлінні повітряним транспортом, мережі кредитних карт, системі управління медичною допомогою. Адже це не вимагає матеріальних витрат. Наприклад, для того щоб підірвати греблю, потрібна тонна вибухівки, її доставка, закладка в уразливі місця і т. Д. Набагато легше відкрити греблю через Інтернет і впливати на її електронні системи управління.

Чому так складно знайти і ліквідувати сайт терористів? Тому що екстремісти широко використовують глобальну мережу, яка дозволяє реєструвати доменні імена сайту в одній країні, а розміщувати інформацію в іншій. І доступ до сайтів може бути доступний з будь-якої точки світу. Паралельно розширюються хакерські війни. Напади хакерів часто носять

психологічний характер. У 2008 році США не змогли нічого протиставити нападу китайських хакерів на сайти американських організацій, які виступали на захист Тибету.

Таким чином, коли з'являються нові способи збору, аналізу та поширення інформації, то це виступає головною умовою розширення інформаційних воєн і сприяє розвитку старих її видів і зародженню нових збройних конфліктів.