Възможности за използване на социалните мрежи във военни операции

подп. Гл. ас. д-р Петко Димов

В доклада се разглеждат различните възможности за използване на социалните мрежи във военните операции. Твърди се, че същите могат да се използват като оръжие за провеждане на психологически операции, кибер информационни операции, добиване на информация, кибер шпионаж и за провеждане на хакерски атаки.

***Ключови думи**: социални мрежи, кибер, информационни операции, хакерски атаки.*

Classification of information products and software to follow the implementation of tasks in the organization.

The report examines the different options for using social networks in military operations. It is alleged that they can be used as a weapon for conducting psychological operations, cyber information operations, cyber espionage and hacking attacks.

***Key words**: social media, cyber, information operations, hacking attacks.*

Социалните мрежи заемат все по-значима роля в политическия и обществения живот на съвременното общество, като водят със себе си съответните предизвикателства и рискове за обществените дебати и промяна в действията или решенията на държавните институции – президент, правителство, парламент[1]. Интернет е оръжие, което има много високо ниво на проникване в съзнанието и комуникациите на хората, защото голяма част от тях са свързани, чрез акаунтите си в различни платформи за споделяне на опит, документи и впечатления. Днес всички хора са в социалните мрежи, но не всички от тях ни мислят доброто. Според едно изследване във всеки профил с повече от 1000 души се крият поне 3-ма злонамерени маниаци, които използват информацията за своите пъклени планове[2]. Всяка по-голяма група е изложена ежедневно на всички познати видове Кибер заплахи и представлява истински рай за хакерите, поради възможността да ударят едновременно голям брой потребители. Обикновено хакерите се опитват да се сдобият с вашето доверие преди да атакуват.

Разпространението на мобилни устройства също допринася за увеличаване потреблението на социалните медии поради възможността лесно да споделяме преживяванията си в крачка и по време на път. Вижте само няколко примера за разпространението на социалните медии[8]:

- Facebook има почти 2 милиарда потребители към април 2017 г., всеки човек има средно 130 приятели, средното престояване в сайта е 23 минути, като 46 % от потребителите са на възраст над 45 г.
- Twitter има 319 милиона потребители, като 33 % над 45 г., цели 54 % го използват от мобилния си телефон и средното посещение на сайта е 14 минути.

Данните потвърждават високото разпространение на платформите и доказват, че тяхната употреба не е само за младежта. Социални са хората от всякаква възраст и всички прекарват много време на тях без да мислят, че някой ги следи за да ги нападне.

В много от случаите твърде повърхностно се споделя чувствителна информация за себе си или за фирмата в която работят, което води до сериозни рискове. Точно поради тази причина социалните медии са интересни за правителствата, военните и разузнавателни служби.

Напоследък се заговори за проучване на възможността да се използват социалните медии във военни операции, кибер шпионаж или атаки на противникови правителства. Събитията от „Арабската пролет“ през 2011 г. която предизвика революция в Северна Африка и Близкия Изток, чрез организиране в социалните медии го доказват.

Благодарение на масовото им разпространение, социалните медии са идеални за много дейности във военния сектор, които представляват интерес за военните операции и разузнавателните агенции – предимно за осъществяване на контрол, мониторинг и анализ на обществото.

Днес те са абсолютно задължителни за употреба и най-активни в тази дейност са държавите САЩ, Китай и Русия, но останалите страни

(включително такива, като Иран и Сирия) също показват значителен интерес, главно от възможността да се използват в следните видове военни операции:

- Психологически операции PSYOPS и овладяване на общественото мнение;
- Информационни операции в Интернет;
- Кибер разузнаване и шпионаж;
- Хакерски атаки над критичната инфраструктура.

Като основен похват се откроява използването на социалните мрежи за пропаганда и разпространение на религиозна идеология. Точно в тази област социалните медии са много ефективни. Вече има разработени програми от кибер специалисти, които анализират в реално време кибер пространството и влиянието му над реалния свят. Работи се върху ново поколение кибер инструменти, които биха могли да се използват за анализ на толкова голямо количество информация, че да осъществят превенция и ранно предупреждение за различни ситуации.

Министерството на отбраната на САЩ например са създали специален интернет портал за предоставяне на всякакъв вид информация, свързана с използването на социалните медии за военни цели[5]. Сайтът е предназначен да помага на военнослужещите в използването на социалните медии и други Интернет-базирани възможности.

Според последния доклад от ENISA за нарастващите заплахи и тенденции в информационните технологии, социалните медии са един от най-търсените сектори за атака[2].

Благодарение на разпространението на социалните технологии, нападателите ще продължат да развиват нови техники за атака на социалните профили на хората в Интернет. Положението става още по-сериозно ако вземем в предвид връзката им с „Интернет на нещата“ IoT в здравеопазването и образованието.

Освен това социалните мрежи могат да се използват за постигане на дезинформация и контрол на политическата реторика. Един от методите за това е чрез инфилтриране на поставени лица в отделни социални отворени или затворени групи.

Психологически операции PSYOP.

Социалните мрежи са привилегирован канал за провеждане на психологически операции, използван предимно за излъчване на информация влияеща на настроението (напр. емоции, мотиви, обективна оценка на обосновката и др.) на големи маси от населението и политиката на правителствата. Психологическите операции като цяло са важна част от установяването на дипломатически, военни и икономически дейности. Според американската военна наука психологическите операции са: „планирани операции за предоставяне на достоверна информация на противниковата аудитория с цел повлияване на техните емоции, мотиви, обективна логика и в крайна сметка промяна на поведението на техните правителства, организации, групи и определени индивиди[3].“

В кибер пространството могат да се използват различни технологии за промяна на настроенията по конкретни теми, като например уеб сайтове, виртуална реалност, блогове, новинарски портали, видео игри, чат ботове и разбира се социалните мрежи. Мисията на специалистите по кибер операции е да се възползват от всички кибер технологии и да повлияят на хората да подкрепят каузата им или да създадат атмосфера на страх.

Например, кибер терористите от Ислямска държава провеждат психологическа операция, чрез използване на социалните медии за разпространяване на самоубийствени атентати и привличане на техни последователи[8].

За да повлияят на общите нагласи по дадени теми, военните специалисти биха могли да организират политически и геополитически кампании за разпространяване на желана информация (фалшива или не) за

създаване на дискусия по дадена тема. Дискусиите се използват за повишаване на чувствителността на обществото и влияят върху възприемането на определени събития от потребителя. Естествено те предварително се манипулират с качването на определени коментари и мнения, които да създадат това чувство у посетителите.

Използването на социалните мрежи позволява на атакуващия да създаде анонимни или целеви профили на реални лица и да публикува материали, без никакво забавяне в целенасочени географски региони или политически партии. Това се използва в комбинация с други психологически тактики от всякакво естество. Още повече, че съвременните технологии предоставят ефективни инструменти за анонимна връзка, което прави невъзможно да се разграничат правителствени операции от личното публикуване.

В обобщение, основните предимства на използването на социалните медии за психологически операции са както следва:

- Социалните медии могат лесно да достигнат различни индивиди, които трудно бихме мигли да докоснем по друг начин.
- Използването на социалните мрежи е гъвкаво, убедително, интерактивно и дава възможност за реагиране в динамични ситуации.
- Кибер средата предоставя анонимност.
- Психологическите операции, чрез социалните мрежи са много по-ефективни и предоставят добра почва за желано въздействие от потребителя.
- Информацията лесно може да бъде променяна при нужда.

Операции за събиране на информация OSINT

Социалните медии предоставят една отлична възможност на разузнавателните служби да анализират и провеждат операции за събират информация от открити източници OSINT (Open Source Intelligence). На стратегическо ниво е съвсем възможно да се събира информация от

публично достъпни източници. Миналата година, представител на DARPA (Defense Advanced Research Projects Agency) заяви: „Разбирането на онлайн поведението е необходимо за прогнозиране на тенденциите[7].“

Основни пречки за подобен тип военни операции са платформените ограничения прилагани за запазване на неприкосновеността на личния живот на физическите лица. Поради което в повечето случай се анализира публично достъпна информация. Наблюдават се блогове, социални мрежи, уикита и всякакви други сайтове за събиране на информация.

ЦРУ и много други агенции използват термина „слушане“ за тази дейност[6]. За целта се използва софтуер, който позволява наблюдението на милиарди разговори и генериране на текстови анализи въз основа на предварително определени критерии. Повечето модерни приложения за слушане може дори да определят настроението на участниците в дискусии по отношение на някои теми.

През 2010 г. Министерството на вътрешната сигурност на САЩ откри, че муджахидински терористични групи все повече използват Facebook за пропагандни цели и като платформа за обмен на тактическа информация по насочване на разузнавачи[5]. Терористичните групи също използват Facebook, за да си осигурят връзки към външни радикални форуми, които дават инструкции относно използването на анонимизиращи услуги като Tor, за да маскират истинските си самоличности[8].

Китайското, руското и американското правителство масово инвестират в технологии за слушане и наблюдение. Агенцията за национална сигурност е изградила най-големия информационен шпионски център в Юта за да прихваща, дешифрира и анализира комуникациите в света от всякакъв вид предаване[5].

Пентагонът живо се интересува от софтуер, който автоматично да претърсва социалните медии и да предлага механизми за ранно предупреждение. Това не е толкова проста работа, защото всеки си прави

различни профили и света в мрежите е доста динамичен, необходим е много добър кръстосан анализ.

Тенденция е да се създават специални формирования, които разработват кибер софтуер за злонамерени актове към чужди правителства. Най-често зловредния софтуер се използва за кибер шпионаж или да повлияят на настроенията на населението и породи несъгласие с правителството.

Извличането на информация и добиване на разузнавателни данни от социалните медии е много важна дейност за разузнаването. Има редица инструменти за анализ на голямо количество събрани данни от социалните мрежи и картографиране в реално време на тенденциите в различните страни за конкретни събития и новини, като протести и социални движения. Всичко в Интернет може да бъде обект на извличане на данни, като социалните мрежи представляват съответна част от данните, които се движат в Интернет, което ги прави източници на голям интерес за всякакъв вид анализ. Социалните медии в много случаи не само осигуряват сурови данни за разследване, но също така и връзките между подгрупи на информация. Това може да бъде много полезно за събиране на разузнавателни данни и прогнози (например, когато един политически лидер е на посещение в друга държава и т.н.).

Кибер шпионаж

Едно от основните военни предназначения на социалните медии е кибер шпионаж. Той включва:

- подмяна на самоличност: способността да се представяте за друг потребител за да извлечете информация;
- създаване на фалшив профил, който не съвпада със съществуващ човек;
- Malware-базирани атаки: използване на зловреден код, за да се компрометира машина на жертвата и открадне чувствителна информация.

Споделянето на линк на един компрометиран уебсайт може да позволи на някой хакер да използва уязвимост в браузъра на потребителя, за да получат контрол над неговия компютър.

Кибер шпионажа чрез социалните медии се основава главно на извличане на данни, чрез свързани мрежи от контакти. Използването на социалните медии може да бъде полезно за кибер шпионажа и кибер разузнаването в етапа на подготовка за психологическите операции.

Услуги като Twitter и Facebook вече са често използвани за геополитически анализ на така наречените "протести" в различни страни. Приемането на техники за извличане на данни за контакти и анализ на връзките дава възможност да се установят връзките между различните лица. Също така може да се установят и частни контакти, които се споделят само с шепа хора.

Ето няколко примера: Имаше един много нашумял случай с висш командир на НАТО на който беше направен фалшив профил във Facebook най-вероятно от китайски шпионин и с чийто акаунт се бяха натъкнали някой от колегите му в НАТО и споделят информация, която е контролирана в акаунта от шпионина[6].

През май 2012 г., няколко дни преди втория тур на президентските избори във Франция, кабинета на Оланд е заразен от зловреден софтуер Flame разпространяван във Facebook. Нападателите споделили линк към заразен сайт, който е реплика на Енисейския дворец, а е бил създаден с цел инфектиране на машините за събиране на потребителски идентификационни данни[8]. Всички машини, които са били част от президентската мрежа, включително редица от най-близките сътрудници на Саркози, са били заразени от агента Flame.

Хакерски атаки

Много хакери са заинтересовани от използването на социални медии, най-вече защото те биха могли да разпространяват зловреден код сред

широка аудитория (Malware-базирани кибератаки), която е слабо информирана за тяхната дейност и различните кибер заплахи. Повечето случай на целенасочени атаки са примери на „социално инженерство“. Фишинг атаките са доста по-малко в практиката.

Във военен контекст, използването на социалните медии може да позволи на хакери да наемат голям брой ботове и да проведат успешна атака срещу цели от критичната инфраструктура. Доста често социалните мрежи се използват за насочване на определена общност или физически лица да се сдобият с някой вирус и да получат т.н. зомбирани компютри без да знаят. В последствие това да се използва в кибер шпионажа.

Според IBM социалните мрежи са доминиращите цели при осъществяване на имейл фишинг и основен метод на инфекция[9]. В последните няколко години повечето широко мащабни атаки се причиняват от зловреден софтуер разпространяван, чрез социални медии, най-вече за бот набиране и за скриване на инфраструктурата за управление и контрол на трафика.

Най-общо злонамерените кодове в социалните мрежи могат да бъдат групирани в следните категории:

- Софтуер за кражба на акаунт в социалните мрежи – често става посредством фишинг и предложена фалшива форма за идентификация. В много случаи, тази проста схема е напълно достатъчна за набиране на лична информация, като имейл, парола и телефон.
- Злонамерен софтуер на 3-та страна, които са като задни вратички, чрез уязвимостите в Интернет браузъра или плъгините на използваните приложения.

И двете категории до голяма степен се използват от кибер престъпници, но те също така биха могли да бъдат приложени от групи военни хакери за да заразят голям брой машини и създадат ботнет мрежа за последваща DDoS атака срещу противников обект.

Най-популярният пример за социален зловреден софтуер е Koobface, който се разпространява, чрез популярни социални мрежи като Facebook, MySpace и Twitter, като спам платформите с много заразени URL адреси, които сочат към компрометирани сайтове[3]. Когато потребителите кликнат върху тези връзки, предложени например, чрез съобщение в платформата, той се пренасочва към някой компрометиран сайт използван, за да се види уязвимост в браузъра и да му се лепне заразен софтуер.

Въпреки, че до скоро IRC мрежите бяха най-често заразени със зловреден софтуер, напоследък много от boot майсторите започнаха да използват Facebook и Twitter за да скрият заразен код в социалните мрежи. Поради наличието на голям обем на данни в тях, съхранявания зловреден код е трудно да се локализира, което е идеалната среда за скриването му.

Кибер информационните операции

Понятието идва от английското Cyber Information Operations (CIO). От него се подразбира, че това са операции за създаване на положително отношение към даден клиент в Интернет пространството. Постига се чрез насърчаване на положителни изявления за клиента, които взимат надмощие над отрицателните сведения във връзка с неговата дейност.

Централно място в процеса на **планиране на концепцията за кибер информационните операции** заемат възможните проблеми, които пораждат спорове в обществото по дадената област. По-просто казано се изразява гражданко несъгласие по определени въпроси, например, за добива на шистов газ, чрез инжектиране на вода под високо налягане, се спори дали е опасно или безопасно? Консенсусът по спорния въпрос се достига под влиянието на положителните коментари, които взимат надмощие над негативните послания. Това е основната на цел на CIO.

С все по-голямото разпространение на социалните медии в нашия живот, частните лица и граждански групи стават все по-силни във формирането на **негативни онлайн настроения** по различни важни за

държавата въпроси. Въпреки, че в по-голямата част от случаите хейтърските коментари не са верни, те имат изключително вреден ефект върху репутацията на облъчения индивид или организация.

Често този вид коментари са анонимни с цел техните автори да не носят юридическа отговорност за тях и за да не дават възможност за отговор. С помощта на кибер информационните операции се позволява на клиента да се противопостави на негативните настроения със свои положителни изявления.

Възможните сценарии на провеждане на кибер информационните операции се разделят на две нива:

- Смекчаване – това ниво се постига, чрез популяризирането на положителни изявления за клиента, които да завземат първата страница с резултатите на търсачките по определените ключови думи за клиента.
- Премахване – пълно премахване на лошите коментари или обезсмислянето им, чрез отговор на контекстуален въпрос на високо равнище.

Какви могат да бъдат показателите за успех на дадена кибер информационна операция? Основната цел на една такава операция е да се изключат негативните коментари от първата страница с резултатите от търсене на Google. Изследванията на SEO специалистите показват, че 90 % от хората посещават само сайтовете класирани на първо място и съответно не могат да се повлияят значително от останалите[8]. CIO се стреми да насърчава положителните над отрицателните мнения в рамките на социалното медийно пространство с цел формирането на положително отношение за даден клиент.

CIO използва много специфичен набор от **технологии и методики за постигане на целите** , които включват:

- Анализ на целевата аудитория – най-важният фактор за успеха в манипулирането на дадена група от хора е опознаването на целевата

аудитория, най-вече какво ще и се хареса и какво не? Ключова част от CIO е да се идентифицират преобладаващите вярвания, основни ценности и болезнени точки за манипулация на даденото общество.

- Анализ на социалните мрежи – благодарение на определен софтуер може да се определят най-влиятелните играчи в рамките на една социална мрежа. Чрез тяхното повлияване може да се влияе и на останалите членове на това общество.
- Облъчване на аудиторията с положителни мнения и коментари, които да се оптимизират от SEO гледна точка и да завземат първата страница на Google.
- Хакинг, кибер престъпления и премахване на активните заплахи, там където не е възможно да се избутат по методите за оптимизация на търсачки.

Изводи

Социалните медии имат значителна роля във формиране на нагласите на обществото и решенията на държавното ръководство, поради което са станали обект на киберпрестъпниците, военни операции и разузнавателни служби.

Без съмнение, социалните медии са от стратегическо значение за военния сектор, тъй като те предлагат огромно количество информация, която може да бъде анализирана с помощта на различни инструменти. Те биха могли да бъдат използвани, като мощно оръжие за събиране на информация, кибер шпионаж, а също така и като активен компонент в ботнет инфраструктура. Поради което е необходимо да се инвестират повече средства в създаване на системи за ранно предупреждение и идентифициране на кибер заплахите.

Армията има нужда да се отвори към социалните медии, но това трябва да се направи съзнателно, чрез предварителна подготовка на военни формирования и интернет ресурси от мирно време. Военния персонал и

техните семейства трябва да бъдат обучени как да управляват социалните си профили. Винаги трябва да се има в предвид, че социални медии са мощни ресурси, които могат да носят със себе си и невероятен брой заплахи.

Библиография:

1. Национална стратегия за кибер сигурност „Кибер устойчива България 2020” София, Министерски съвет, 2016;
2. ENISA Threat Landscape Report 2016. 15 Top Cyber-Threats and Trends. Final Version 1.0, 2017;
3. Baker, P. Psychological Operations within the Cyberspace domain. 2010
4. Baltazar, J, Costoya, J. Flores, R The real Face of Koobface: the largest web 2.0 botnet explained. 2010
5. http://www.defense.gov/home/features/2009/0709_socialmedia/
6. http://resources.infosecinstitute.com/social-media-use-in-the-military-sector/
7. http://www.darpa.mil/
8. https://postvai.com/internet-analizi/voenni-socialni-medii.html
9. https://www.ibm.com/security/xforce/