Yadigar N. Imamverdiyev DOI: 10.25045/jpis.v07.i2.02
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

SOCIAL MEDIA AND SECURITY CONCERNS

Social media is not only a convenient platform of communication and file sharing, but also a socio-political impact and management tool, and an arena of confrontation and information warfare. Depending on the purposes of its users, social media can create a range of national security threats. The article describes a number of risk scenarios of the social media that can pose a threat to national security, and analyzes the methods of creating bots - the fake actors and managing them, and the experience of certain countries in this area. The article provides information on the available online services that can be used for social media monitoring and analysis.
Keywords: *social media, national security, social media monitoring, social media analytics, information influence, information warfare.*

Introduction

Social network services created on the basis of Web 2.0 ideology in a very short period of time, in the last decade, turned into a social media generating and distributing unique content from a convenient tool for communication and file sharing [1]. Today, social media includes blogs *(Blogger, LiveJournal),* micro-blogs *(Twitter, FMyLife),* social networking services *(Facebook, LinkedIn),* wiki-s *(Wikipedia, Wetpaint),* social bookmarking *(Delicious, CiteULike),* social news *(Digg, Mixx),* reviews *(ePinions, Yelp),* multimedia sharing *(Flickr, Youtube). Facebook, Twitter, YouTube* and other social media services have become an integral part of the online life of the majority of Internet users.

Social media has a number of advantages in comparison with traditional media: social media is available; requires minimal expense; is open to everyone - any person can connect to the global communication platform and can act as a source of information; is more dynamic and flexible; feedback opportunities are extensive - the audience has the opportunity to interact with a source of information; offers high degree of individualization; unites people in a single platform and allows to exchange large amounts of information.

Social media users have a quite diverse spectrum. Conventional users benefit from social media as a means of communication, acquaintance, sharing daily data and images. The affordable feedback opportunities of social media makes it an effective communication and impact channel. Recently, public authorities, political parties, civil society and private sector is trying to widely use the potential of social media [2, 3].

Social media brings some threats as well. The threats can be directed against the individuals and social groups, in general, against the state and society. Detailed information on the dangers of social networks, directed against individuals, is provided in [4], and specific recommendations are presented.

In recent years, the representatives of the state authorities in all countries of the world have repeatedly stated concerns regarding the threats that social media can pose to national security [5.6]. There are various risk scenarios - wide usage of social media by terrorists, external forces using social media as a mean to influence internal politics of the country and so on. There is also a practical basis for these concerns, and "Arab spring" has proved that social media is a strong weapon that can be used to divert the masses, dramatize events, and realize social changes and revolutions [7].

The main objectives of the information policy of the state authorities include to inform the citizens about their activities and to organize feedback with citizens by the means of mass communication. At the same time, government agencies are obliged to respond to information threats that can create conflict and social tension, can lead to the wrong public opinion and damage the reputation of the state authorities.

The article describes a number of risk scenarios of the social media that can pose a threat to national security, and analyzes the methods of creating bots - the fake actors and managing them, and the experience of certain countries in this area. The article provides information on the

available online services that can be used for social media monitoring and analysis.

Social media: risk scenarios

The main concern of some countries is related to the usage of social media by terrorist, extremist and radical groups. Almost 90% of the organized terrorism on the Internet is carried out through social media sites. Social media provides an opportunity for terrorists to address millions of people in a few seconds. Terrorist groups spread their appeals through YouTube, Facebook, Twitter and other sites, and involve tens of thousands of people to their ranks.

Sometimes, the countries find the way of solution in restricting access to certain social media sites. For example, officials of the European Commission demand more proactive regulation for the online participation of violent extremist groups in Google, Facebook, Twitter and other social media platforms. Officials propose to carefully consider the content posted by the users before uploading it, or to ban the entry of some groups to the social media platforms in general.

Tweets, sensitive to religion, are becoming widespread. People are attacking each other's religious values through social media. The circulation of images insulting religious and racial feelings in social media creates tensions among the masses.

Many politicians and public figures have pages on social networks. Social media is widely used as the means of political propaganda in election campaigns [8]. Some opposition politicians have earned their current status as a result of their active participation in social media. Blogs have become an important tool of political parties and public movements for highlighting actual events. Social media is also used as a convenient tool for organizing socio-political activities. Political parties, NGOs and hackers can pose a serious threat to political stability by using social media.

Social media can be used as a tool for exporting revolution *("Facebook revolution", "Twitter revolution")* to various countries. In 2009-2011, the political crises in Iran and several other Middle Eastern countries, the protests in Ukraine and Russia showed that social media can be used to mobilize protesters, and a small number of public opinion leaders is enough for it [9, 10].

It is known that intelligence agencies obtain a significant portion of the intelligence information (according to some confessions 80%) from open sources. Intelligence methodology based on open sources *(Open Source Intelligence - OSINT)* includes search, selection and collection of information from open sources, as well as its coordinated and cross analysis. The main information sources include media, public reports of public authorities and private companies, official press conferences, various official statements, materials of various conferences and seminars, and so on. Social media is also a great opportunity for intelligence agencies [11]. In 2011, during the operations of *NATO* forces in Libya, social media was widely used as a mean of transmission of intelligence data in real time. The relevant information was processed in a special operation center created in Napoli, Italy [12].

Social media has a great military potential – the usage of mobile phones with *GPS* function provides unlimited opportunities. It takes a few seconds to share geo-information data of an object with its photo in social networks. Social media was used to help the identification of surface targets during air attacks of *NATO* forces in Libya operations in 2011. The information obtained from social networks and other Internet sources allowed online observation of the progress of the military operations [12].

Thus, social media has become a powerful tool of propaganda, disinformation, conscious manipulation, and collection of individual, business and intelligence information [13].

About the information impact mechanisms of social media

Although the social media phenomenon occurred in the last decade, its theoretical foundations were formed long before in the researches conducted in the world's foremost research centers on social psychology, media studies, social information science, social network analysis, complex networks, complex dynamics, complex systems, network wars etc. Social media reveals wide opportunities for experimental verification and real application of the results of these

researches. The research centers include Los Alamos National Laboratory, where the world's first atomic bomb was prepared, Stanford University, Mitchell Social Network Analysis Center of Manchester University, the Santa Fe Institute, *IBM, RAND Corporation* and others.

According to the views of the social network, humanity consists of a large number of societies, and each person is a member of a number of communities at the same time. The people who a person communicates with are, in their turn, also members of several communities. This chain of relationship creates a number of information channels covering all the mankind. Information can be spread through these channels at any scale as, according to the small world model, all the people are related with each other through common friends and usually the number of common acquaintances is not more than 6 [1].

Understanding the essence of network structures and distribution channels can lead to more effective results in terms of the impact on the audience. It is possible to influence the whole society, including decision-makers through the information published in media and accepted by the society in the right direction.

The mechanism of the information impact on society through network structure is identical everywhere: a customer determines the task, its executors build a network structure consisting of public organizations, journalists (or the whole media and media-holding), political activists, members of an informal movement, in some cases criminal and extremist groups for carrying out this task. They involve some of them with grants, some with promises of political promotion and others simply with money. The involvement of people addicted to the idea given to them plays an important role. They are the driving force, they are able to convince people and to lead them to any radical activities.

However, the peculiarity of the network warfare is that similar operations are not a sudden action, but there are more of them, they occur in different places at different times and carried out by different organizations. These actions jointly contribute to the overall result. The small actions are similar to bee's nest – a bee needle is not dangerous, but the more bees are, the more they sting, and it makes people run. The experts of *RAND* Corporation call this principle *"swarming"* or "herd principle" [14, 15]. "Herd" demonstrates itself as "micromovements", "stings", "reminders": media hype, discussions on various topics that are imposed on the society, various demonstrations, multitude of armed and unarmed physical confrontations. The pre-determined experts willingly express their desired opinions on the screen or on the Internet, the journalists publish scandalous articles, the human rights activists hold rallies and write open letters, and the lawyers give interviews about the arbitrary approach towards the persons who they defend and so on.

Fake actors of social media

"The Guardian" newspaper (UK) reported in 2011 that the US Department of Defense has created a special software to secretly manipulate the mood of social network members with the help of fake "online persons" [16]. Those fake persons had to intellectually influence the Internet users in order to contribute to the dissemination of American propaganda.

Defense Advanced Research Projects Agency of the US Department of Defense (DARPA) in 2011 announced a tender for the creation of the software within the framework of Social Media in Strategic Communication (SMISC) program, for such operations [17, 18]. These works could be considered as continuation of the "Operation Earnest Voice", OEV, carried out in Iraq in 2003.

It is possible to create a network of fake social media actors, which is connected to information phase of different countries with the help of software, created by Ntrepid company within SMISC. As a result of this work, the impression of the presence of real people in different countries around the world, not "Sock Puppets", is formed. Details of fake "autobiography", "characters" are created separately for each actor. The document about the online management service of identities says that each fake user profile, all the features of the character should be fully adequate from technical, cultural and geographical point of view. IP addresses for those fake profiles are camouflaged in a way that everything proves that fake actor has placed all the materials

in the displayed area. As a result, even experienced opponents become incapable of detection of the facts on manipulation with these fake online persons, they can easily gain the trust of local bloggers. Management service of online people created by Ntrepid allows one operator to manage more than 10 fake social media accounts. Operations management center is McDill airbase (Tampa, Florida, USA), where the US Central Command headquarter (CENTCOM) is located.

Open information on the establishment of similar structures in several countries can be found. For instance, the information about the plans for the creation of software and hardware complex for "monitoring and analysis of the military-political, socio-economic and socio-political situation in the country and the world" on the basis of data collected from various open sources for the Ministry of Defense of Russia was reported in the press.

Federal Intelligence Service of Germany, in the next five years, plans to spend 300 million euros on the creation of technologies that enable real-time monitoring and analysis of social networks outside the country, as well as capturing and decoding network traffic. The program, main objective of which is the early detection of cybercrime, has been named as "Strategic Technologic Initiative" (Strategische Initiative Technik, SIT).

A brief overview of the SMISC program

Explanatory document for the tender of SMISC program states: "the conditions of the operations conducted by armed forces are rapidly changing under the influence of blogs, social networks, file exchange services (such as YouTube) and mobile technologies. The wide spread of social services can have a deep impact on the nature of the conflicts. The efficient use of these services will enable the armed forces to more efficiently conduct information support for operations ".

The main objective of the SMISC program is the use of new social network science built on the basis of emerging technology. In a particular case, SMISC will create the automated and semi-automated tools and means to support the systematic use of social media on the datum scale by the operators and ensure the timely implementation of the four specific targets of the program:

1. To reveal the formation, develop and spread ideas and concepts; identify, classify, evaluate and follow purposeful or misleading (deceptive) information and disinformation.
2. To reveal structures and influence operations of persuasive campaigns on social media websites and communities.
3. To identify participants of the persuasive campaigns and their intentions, and to evaluate the effects of these campaigns.
4. To conduct opposite operations against the revealed operations of enemies.

Technology sectors of SMISC are grouped according to the above stated four key targets:

1. linguistic tips, information flow templates, topic trend analysis, narrative structure analysis, mood detection and intellectual analysis models of opinions;
2. observing concepts and ideas in society, graph analysis / probability judgment, character detection;
3. stimulation of individuals, modeling of newly established communities, trust analysis, modeling of network dynamics;
4. automatic generation of content, social media bots, crowd sourcing.

Studies show that traditional approaches with static graph models to social media modeling usually have wrong results. Therefore, it is necessary to take into account the *dynamics of behaviors* and SMISC is interested in the use of many tools to implement it [18].

Social media monitoring tools

The rapid increase in popularity of social media and rise of its economic and socio-political role requires the establishment of information systems for its monitoring and analysis [19].

However, there is a lack of data for social media monitoring and analysis systems for government bodies, as they were launched in 2010, and are not widespread yet [20]. Currently,

most of the introduced social media monitoring tools in the market are focused on business issues. They identify how many times the names of certain brands, companies, products or services have been mentioned in social media, users' attitudes towards them (positive, negative, neutral), detects the tone of opinions, divides the authors of opinions into segments according to gender, age, location, interests and etc.

It should be mentioned that there are several monitoring tools in popular social network services. For instance, *Facebook Insights, Google Analytics, Twitter Analytics, Analytics LinkedIn, Pinterest Analytics*. Currently, web portals in English, such as *SumAll, Sysomos, UberVU, SproutSocial,* in Russian, such as *YouScan, Brand Analutics, Babkee, BrandSpotter, Buzz Look, IQBuzz, SemanticForce, Wobot, Крибрум* etc., offer social media monitoring services. Following paragraphs provide brief information on some of the monitoring systems.

Seesmic *(seesmic.com)* - free service for social media monitoring. It supports *Twitter, Facebook, LinkedIn, Chatter, Google Buzz, Ping.fm*. *Seesmic* has application programs for the Internet, personal computers, *iPhone, Android, Windows Mobile*. In essence, *Seesmic twitter* – is client, was created using *Adobe Air library*, therefore could work on many platforms.

Socialmention *(socialmention.com)* – is a free platform for the search and analysis of information on social networks. *Socialmention* searches meets on selective services or all social media that it supports. Besides, analysis of reminder and tones, related keywords, popular sources and etc. are included. *Socialmention* contains more than 100 social media sources including networks, social bookmarks, blogs, forums, social services.

Hootsuite *(hootsuite.com)* – is multifunctional service working with social media. The emphasis of service was on *Twitter*. Hootsuite enables working with *Facebook, LinkedIn, MySpace* and *Foursquare*, and *WordPress* blogs and could connect to *Ping.fm. Hootsuite* has several opportunities to work with different analysis. For instance, it is possible to connect to *Google Analytics*. *HootSuite* works on a number of mobile platforms: *iPhone, Android, Blackberry*. Mobile applications are free.

Twitalyzer *(twitalyzer.com)* – is analytical program-client for *Twitter.* and enables to monitor the number of links, to analyze the positive and negative comments, and to divide the audience into segments. Twitalyzer has been integrated with *Google Analytics* system and works with interactive diagrams and graphic tools.

TweetDeck *(tweetdeck.com)* – is tool for the monitoring and management of information on social networks like *Twitter, Facebook, MySpace, LinkedIn*, supports various filters, including filtering based on keyword, works on different platforms.

Despite existing and new services emerging each month, as well as presented opportunities, the whole social media monitoring systems are based on typical software [21-23].

Conclusion

Along with functions as communication, information, and exchange of views, recently, social media is widely used as information impact tool, and becomes the stage for information confrontation and information warfare. Monitoring and analysis of social media data, without violating human rights and freedom of expression, enable to take the pulse, set the mood and detect expectations of the society. It creates ground for effective dialogue for the government with citizens, private sector, political parties and movements, civil society institutions. Social media analysis enables to timely detect emerging threats and implement counter-measures.

References

1. Alguliyev R. M., Imamverdiyev Y. N. Abdullayeva F. C., Social Networks. Baku, "Information Technology" Publishing House, 2010, p.287
2. Wright D. Hinson M., Examining how public relations practitioners actually are using social media // Public Relations Journal, 2009, vol. 3, no. 3, pp. 1-33.

3. Under the general editorship by Alexeyeva E.G. Impact through social networks, M., Foundation "FOCUS-MEDIA", 2010, p.200
4. Hogben G. (ed.) Security issues and recommendations for online social networks. ENISA Position Paper No.1, October 2007, 33 p.
5. Montagnese A. Impact of social media on national security. Centro Militare di Studi Strategici: Research Paper 2011 STEPI - AE-U-3. 2012, 36 p.
6. Chen Y. Research on social media network and national security. W.Du (ed.) Informatics and Management Science II, Lecture Notes in Electrical Engineering, 2013, vol. 205, pp 593-599.
7. Khondker H.H. Role of the New Media in the Arab Spring // Globalizations, 2011, vol. 8, no. 5, pp.675-679.
8. Adamic L. A., Glance N. The political blogosphere and the 2004 US election: divided they blog / Proc. of the 3rd international workshop on Link discovery, 2005, pp. 36-43.
9. Elson S. B., Yeung D., Roshan P., Bohandy S.R., Nader A. Using social media to gauge Iranian public opinion and mood after the 2009 election. RAND Corporation Technical Report. 2012, 110 p.
10. Tan Z., Li X., Mao W. Agent-based modeling of netizen groups in Chinese Internet Events // Quarterly SCS M&S Magazine, 2012, pp. 39-45.
11. Baluev D.G., Kaminchenko D.I. The political role of the "new media" in the Libyan conflict // Bulletin of the Nizhny Novgorod University Lobachevski N.I .2012, No 2 (1), pp.307-313.
12. Levesque J. Social media "Tactical intelligence collection": Spying and propaganda using Facebook, Twitter. February 15, 2012.
13. Gubanov D.A., Novikov D.A., Chkhartishvili A.G. Social networks. Models of information influence, control and confrontation. Moscow: Publishing House of Physical and Mathematical Literature, 2010, 228 p.
14. Arquilla J., Ronfeldt D.F. Networks and netwars: the future of terror, crime, and militancy. Rand Corporation, 2001. 5 p.
15. Cebrowski A.K., Garstka J.J, "Network-centric warfare: Its origin and future." U.S. Naval Institute Proceedings, January 1998, 10 p.
16. Revealed: US spy operation that manipulates social media, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks
17. Social Media in Strategic Communication (SMISC), http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_%28SMISC%29.aspx
18. Social Media in Strategic Communication (SMISC), http://www.darpa.mil/opencatalog/SMISC.html
19. Sykora M.D. et al. National security and social media monitoring: A presentation of the EMOTIVE and related systems / European Intelligence and Security Informatics Conference, 2013, pp. 172-175.
20. Batrinca B., Treleaven P. C. Social media analytics: a survey of techniques, tools and platforms // AI & Society, 2015, vol. 30, no. 1, pp. 89–116.
21. Pang B., Lee L. Opinion mining and sentiment Analysis // Foundations and Trends in Information Retrieval, 2008, vol. 2, no. 1-2, pp. 1-135.
22. Aliguliyev R.M. A new sentence similarity measure and sentence based extractive technique for automatic text summarization // Expert Systems with Applications, 2009, vol. 36, no. 4, pp. 7764–7772.
23. Karthik K., Kollias G., Kumar V., Grama A. Trends in Big Data analytics // Journal of Parallel and Distributed Computing, 2014, vol. 74, no. 7, pp. 2561-2573.