УДК: 316.77:004.056(73)

Olga Zernetska,
Dr. Polit. Sc., Professor,
State Institution «Institute of World History,
National Academy of Sciences of Ukraine»

CYBERSECURITY ON US SOCIAL NETWORKS

Abstract. *The role and influence of social networks on American society is analyzed in this article. Cyber-attacks that threaten social activities as well as other risks for business, organizations, institutions, employers and employees are detected. Special attention is paid to changes of mass consciousness and private lives of American grownups and teenagers. The huge information stored in social networks is the wast field for cyber-attacks, huckers, abusers and so on. Social media expose users to predators like pedophiles and burglars; and spread false and potentially dangerous information. This problem is tightly interwoven with the problem of cybersecurity of institutions, businesses, politics, mass consciousness and individuals especially that of children and teenagers. Cybersecurity problems on American social networks such as Facebook, Twitter, are observed. The creation of national cybersecurity strategy of Ukraine with the emphases on humanitarian side of this issue is initiated. Influence of American social media on society (Facebook, YouTube, Pinterest, LinkedIn, MySpace, Twitter, Instagram, FriendWise, FriendFinder) is characterized in the article. The problem of children's and teenagers' cybersecurity on the social media networking sites is of utmost importance in the USA. It must be admitted that violence and crime has become a part of social and private lives of American adolescents. Shots on an urban street and a school building are real facts. What they see in films, video games, TV news and on the streets also come to them also through social media.*

Key words: *USA, cybersecurity, social networks, Facebook, Twitter.*

Communication revolution leads to the unprecedented possibilities for mankind at the beginning of the 21st century. To communicate freely using social networks becomes very popular all over the world and especially in the United States – the birthplace of the well-known social networks. The history of social networking sites is very short. The first social networking site is considered to be SixDegrees.com. It existed from 1997 to 2001. The new features of it were that users could create personal spaces and connect to friends online. The other social networking site was Friendster, created in 2002. It popularized social networking in the United States but was quickly outpaced by other social networking sites such as MySpace (2003), Facebook (2004), Twitter (2006), Pinterest (2009), and Google+ (2012).

Such American social networks as Facebook, YouTube, Pinterest, LinkedIn, MySpace, Twitter, Instagram, FriendWise, FriendFinder have their users not only in the USA, but all over the world. And it is quite understandable because the desire to communicate is one of the unattainable features of a human being. Facebook reached one billion monthly users worldwide on October 4, 2012, making it the most popular social networking site with one in seven people on the planet as members. 71% of online adults in the United States use Facebook.

Here are some other valuable statistics concerning Facebook:

- Worldwide there are over 1.49 billion active Facebook users which is a 13% increase year over year (as of 6.30.2015).
- Five new profiles are created every second.
- Facebook users are 76% female and 66% male.

- Every day, Facebook manages 4.5 billion «Likes», 4.75 billion content shares, and over 300 million photo uploads [3].

The latest research (September, 2014) obtained by American scholars and marketing firms in this field concerning other US social networks give such results: 51% of US adults use YouTube, 28% use Pinterest, 28% use LinkedIn, 26% use Instagram, and 23% use Twitter. Twitter has 288 million monthly active users and over 500 million tweets are sent daily. Among online adults, use of more than one social networking site increased from 42% in 2013 to 52% in 2014 [3].

Concept Web 2.0. has made it possible for people to communicate and connect using different kinds of social networks, connecting with their friends, relatives, families whenever they like. Social networking sites spread information faster than any other media. They allow people to improve relationships and make new friends, to help employers to find employees and job seekers to find work, to increase voter participation and so on. Social networking sites spread information faster than any other media. Law enforcement uses social networking sites to catch and prosecute criminals, Social networking sites help empower business and they are generally good for the American economy.

There are some striking facts proving how deeply social networking sites have been enrooted in lives of American users:

- Social networking sites are a top news source for 27% of Americans ranking below newspapers (28,8%), and above radio (18,8%) and print publications (6%).
- 35 heads of state, every US cabinet agency, 84% of state governors, every major candidate for US President, and more than 40% of top global religious leaders are on Twitter.
- 10% of people younger than 25 respond to social media and text messages during sex [3].

Together with the exponent growth of these communication platforms the enormous amount of personal information has been formed. The benefits of social networks are quite understandable. But social networkings also have a dark side and pose a tremendous risk to individuals, organizations and businesses. The huge information stored in social networks is the wast field for cyber-attacks, huckers, abusers and so on. Social media expose users to predators like pedophiles and burglars; and spread false and potentially dangerous information. This problem is tightly interwoven with the problem of cybersecurity of institutions, businesses, politics, mass consciousness and individuals especially that of children and teenagers. We try to investigate this issue using the newest research results in order to illuminate these burning problems.

Brief Literature Review. American scholars have already made very valuable findings in this sphere. Among essential monographs on using Internet as a new powerful tool in social movements and political campaigns are the books of M. Castells [4], J. Earl, K. Kimport [5], S. Issenberg [9], R. MacKinnon [11], J. Owyang 13]. The problems of new generations and their relations with the digital communication environment are profoundly detected by J. Palfrey, U. Gusser [14] and E. Pariser [15]. Psychological and sociological issues connected with personality identification in the jungle of social networks are analyzed by S. Turkle [21]. All the works mentioned above are so called «a must be reading». They are read by fellow-scholars, students and also by wide circles of American society. These books are on the top of literature ratings lists. Some of them have already got prestigious awards. All these facts testify the quality of these works and

show the deepest interest of the US readers to the problems of social media and American society enlightened in these books.

The main objective of the research is to examine the current state of analyzes of cybersecurity problems on American social networks concerning such issues as social activity, institutions, organizations, business, relations between employers and employees, changes in mass consciousness and private lives of American citizens paying special attention to the influence of social networking on children and teenagers, and extrapolating that all these problems are of vital importance for Ukrainian society of the digital age.

Results. Exploring the movement of senses in the global Internet sphere in one of our previous works we augmented the extraordinary fruitfulness and productivity of prefix «cyber» in the production of new meanings related to the development of the Internet which became a condensed expression of global multicultural domain in the age of information and communication. «Cybersecurity», «cyberspace», «cyber-attack», «cyber operation», «cyber power», «cyber invasion», «cyber war» are the concepts that have become an integral part of a new sphere of human communication and activity [8, 379-380]. Considering and analyzing evolution of cyber security on social media networks first of all we are to define the basic concept of the study: that is «cyber security». The American scholars define this basic concept as follows: «Cybersecurity is the protection of computers' electronic information and / or all digital networks from accidental or intentional unauthorized opening, transfer, termination, modification and destruction» [2]. We assert that in case of analyzing cyber security on social networks this definition is not enough. We propose a broader definition of cyber security concerning social networks: «Cybersecurity on social networks presupposes not only the protection of computers' electronic information and / or all digital networks from accidental or intentional unauthorized opening, transfer, termination, modification or destruction, but also safeguarding communication of their users from manipulation, abuse, theft, distraction and falsification of information».

We start with analyzing the concept of «social cyber-attack». It is a very dangerous malicious activity because it threatens social order, normal way of lives not only of the definite network community. It can also provoke ethnic tensions and become the source of different social and political conflicts. As an American scholar R. Goolsby emphasizes that social cyber-attack is not a new phenomenon. In the late 1980s and early 1990s, USENET groups, forums, and bulletin boards suffered the problem of «flame wars» instigated through «trolling,» new social behaviors and attacks that were designed to destroy nascent virtual communities by stirring up conflict. «Trolls» commonly attempted to reveal hidden divergences among community members. She warns users of social networks that sometimes using of «tralls»are very sophisticated: by jumping into an expected or «natural» excited signal, the hoax messages – the «false» signal – could hide among the stream of natural messages and be accepted, perhaps even if it was difficult to determine precisely the origin of those messages. This represents a sophisticated sort of attack. Social cyber-attacks are of two kinds: (1) pre-meditated, which are designed to create an excited signal in a social network, often under false pretenses, so as to benefit from the chaos and upheaval; and (2) opportunistic, which take advantage of an existing excited social network signal and, by manipulating it through various means, derive benefit. The creation of hoaxes, hate speech, and other attempts at crowd manipulation and exploitation reveal the darker side of the social media phenomenon; the targeted «social-cyber attack» is rapidly coming of age. Hot topics,

deep visceral concerns, false assertions, and irrelevant tangents were the hallmark of these altercations, which became known as «flame wars.» They destroyed many a small virtual community and damaged many a large one.

R. Goolsby gives a valuable piece of advice to social media users: «All social media users need to develop a healthy skepticism about the messages that they receive, learn to check sources, and refine their skills of discernment. New technologies that assist users to better protect themselves are one part of the solution. Social media watchdog groups also play a role in the education of the user community, spreading the word about hoaxes, scams, and attacks very quickly and widely – if only users will pay attention» [8].

A growing body of studies have stressed that businesses and institutions have become targets of more and more sophisticated cyber-attacks. That induces top management to invest a lot of efforts and money to protect their organizations from hackers, to strengthen their data protection and so on because they are aware about the dark side of social networking that pose a tremendous risk for different kinds of organizations in today's globally interconnected world.

According to T. George an American researcher and practitioner who has more than twenty years of global information security experience to address social risks, there are a number of steps organizations can take, including:

1. Expand User Awareness Training. While social media attacks rely on the same lures seen in phishing and spam emails, it is important to expand an organization's end user security awareness training programs to cover the social engineering methods and techniques used in social networks. Users should be taught to be wary of social media requests from unknown individuals and provided with safety guidelines on how to use social networks in their work environment.

2. Create a Social Media Policy. Beyond extending an organization's security awareness training program, create a social media policy for employees. A social media policy can be a first line of defense to mitigate risk for both the organization and the employee. While many organizations may already have a confidentiality agreement in place, it might not be enough in the context of social media threats. Adding a few lines in the employee handbook to clarify that the confidentiality agreement covers employee interactions on social media sites and cross-reference to the security awareness training program might suffice. It is preferable, however, to create a separate social media policy that is accessible to employees so they are aware of its existence.

3. Leverage Social Media Threat Intelligence. Security professionals sometimes neglect threats as part of risk assessments to focus on known, more visible facts – vulnerabilities and control failures. However, as the volume of vulnerabilities that an organization is exposed to has exploded over the last years, it has become almost impossible to remediate all of them without vetting the impact and likelihood of exploitation. Since threats are used to take advantage of vulnerabilities, they are essential in the risk assessment process and can no longer be treated as a neglected step child [7].

Therefore, security operations teams should leverage threat intelligence to gather insight into the capabilities, current activities, and plans of potential threat actors (e.g., hackers, organized criminal groups, or state-sponsored attackers) to anticipate current and future threats. Some commercial threat intelligence services now provide offerings that focus specifically on social media threats which provide early warning indicators when it comes to social network attacks.

T. George concludes that for all the benefits that social media networks provide, organizations must recognize that they present a double-edged sword when it comes to

security. Therefore, a pro-active approach is necessary to prevent social media from becoming the next big cyber-crime vector which puts an organization's brand at risk [15].

As to social media platforms for enterprisers, C. Nerney [12], another well-informed author, dwells. There are real risks to using social media, ranging from damaging the brand to exposing proprietary information to inviting lawsuits. As to him, risk number one as well as for T. George, is lack of a social media policy. C. Nerney warns top management of American organizations about this: «This one's totally on you. Without a social media policy for your enterprise, you are inviting disaster. You can't just turn employees loose on social networking platforms and urge them to «represent». You need to spell out the goals and parameters of your enterprise's social media initiative. Otherwise you'll get exactly what you're inviting – chaos and problems» [12]. The second great risk is connected with employees' discourses and making different comments on a work-related social media accounts, because if the comment is made on a work-related social media account, then it's out there, and it can't be retrieved. The third danger comes from hackers. Sometimes hackers go right to the source, injecting malicious code into a social networking site, including inside advertisements and via third-party apps. Twitter is especially vulnerable to this method because it's easy to retweet a post so that it eventually could be seen by hundreds of thousands of people. The fourth risk comes out of social engineering. There are a lot of scoundrels in the Internet who find potential victims telling lies and trying to make friends in order to get a password from them. C. Nerney tries to prevent this risk explaining that social media has taken this threat to a new level for two reasons: 1) People are more willing than ever to share personal information about themselves online via Facebook, Twitter, Foursquare and Myspace, and 2) social media platforms encourage a dangerous level of assumed trust. From there it's a short step to telling your new friend about your company's secret project. Which your new friend really might be able to help with if you would only give him a password to gain access to a protected file on your corporate network. The fifth risk lies in the fact that numeral mobile applications have great threat for the cybersecurity of their users. For example, C. Nerney asserts that in early March 2011, Google removed from its Android Market more than 60 applications carrying malicious software. Some of the malware was designed to reveal the user's private information to a third party, replicate itself on other devices, destroy user data or even impersonate the device owner [12].

A lot of research detecting how using social media can harm job stability and employment prospects proved such negative facts: job recruiters reported negative reactions to finding profanity (61%),poor spelling or grammar (54%), illegal drugs (78%), sexual content (66%), pictures of or with alcohol (47%), religious content (26%) on potential employees' social media pages [10].

The other aspect of investigations made by different researchers concerns such facts as how social networking sites harm employees' productivity. The data are alarming: 51% of people aged 25-34 accessed social media while at work. Two-thirds of US workers with Facebook accounts access the site during work hours [23]. Even spending just 30 minutes a day on social media while at work would cost a 50-person company 6,500 hours of productivity a year [6]. 51% of American workers think work productivity suffers because of social media [19]. That is what concerning loss of jobs and loss of productivity in American society in connection with social media networks. But negative aspects of using social media networks for individual matters become great obstacles in private lives of American families. That concerns all: grown-ups, children, teenagers.

First of all let's pay attention to the private relations of parents in the family. It is a well-known fact that the amount of divorces is high in the United States. The cases of divorces in the American courts feed a whole army of lawyers, whose specialty is divorces. Now Americans must be aware that information about an affair posted on Facebook, for example, «can lead to and be used against someone in divorce proceedings because the information, once posted, can never be completely deleted. Facebook was named as a source of information in one-third of all divorces filed in 2011» [24]. Generally speaking this information is valuable globally because sooner or later both the level of development of social networking and the level of legislature in many countries all over the world will make it possible to use texts and videos from social media sites as valid proofs in courts' procedures.

It also must be known to the general public that the Library of Congress has been archiving all public tweets from Twitter's March 2006 inception forward [18]. Our advice is to bear in mind that these tweets shall be saved there forever. That's why you must think twice before sending every tweet.

The problem of children's and teenagers' cybersecurity on the social media networking sites is of utmost importance in the USA. It is seriously discussed and researched. There are sites in the Internet trying to help parents and grandparents to understand the youth culture and to minimize the risks which are waiting for their children and teenagers, such as online predators, cyberbyllies, ruined reputations and other dangers. The difficult task for parents is to teach their teens to socialize safely online.

It must be admitted that violence and crime has become a part of social and private lives of American adolescents. Shots on an urban street and a school building are real facts. What they see in films, video games, TV news and on the streets also come to them also through social media. A 2015 study, «How to Cope With Digital Stress: The Recommendations Adolescents Offer Their Peers Online» examines comment threats shared among adolescent peers to better understand how young people advise each other when it comes to online bullying. The authors identified six major digital stressors: 1) Public shaming and humiliation. 2) Impersonation (Using digital platforms to pretend to be another person usually «for the purpose of slandering, mocking or embarrassing the impersonated»). 3) Mean and harassing personal attacks. 4) Breaking and entering (Using another person's online account or digital devices without permission.). 5) Pressure to comply (Experiencing pressure «to grant access to accounts or nude photographs»). 6) Smothering (Excessive contact via online messaging in which «the content of messages is not intended to hurt nor harm, but the quantity is itself problematic») [20].

Parents and teachers acknowledge how important it is for teenagers to cope with digital stress and traumas. An estimated 92% of teenagers go online daily and near a quarter reports being online almost constantly. A future challenge in this aspect lies in the sphere of public health and skills of socializing. The Millennial generation, born between 1980 and the mid-2000 are of great interest for American politicians, researchers and marketers because this age group is the most educated generation and the largest in the U.S. labor force. They are also called Generation Y. This is the first generation to grow up with the Internet, sell phones, smart phones and tablets feeling as if they always have been on the planet. They perception of life differs greatly from those of their parents. These psychological and digital divides separating them must be taken into account.

Many of American teenagers express tiredness of all these new technological communication tools. They feel that being constantly online change them, spoil their

character. In a column by M. Price-Mitchell from «Psychology Today» there are vital thoughts from their essays. Pupils of the tenth grades points out such disadvantages of social networking: 1. Lacks of emotional connection. 2. Gives people a license to be hurtful. 3. Decreases face-to-face communication skills. 4. Conveys inauthentic expression of feelings. 5. Diminishes understanding and thoughtfulness. 6. Causes face-to-face interactions to feel disconnected. 7. Facilitates laziness. 8. Creates a skewed self-image. 9. Reduces family closeness.10. Causes distractions. [17].

These are very sincere answers given by teens. They have to induce researchers – sociologists, anthropologists, historians, linguists, medicines, especially physiologists to investigate deeply the characters and social behavior of Millennial generation. Atomization of teenagers instead of socialization, loneliness among their peers, growing inability to communicate face-to-face with classmates are some of the disturbing traits of growing American generation. Pitifully, but there is a global trend both in the advanced societies with digital economy and in the states with the transformative economy such as Ukraine that is characterized by a deep digital divide between youth and older generation.

Conclusions. Social networking security threats must be considered with all possible seriousness. The conducted analyses of American social media (Facebook, YouTube, Pinterest, LinkedIn, MySpace, Twitter, Instagram, FriendWise, FriendFinder) proves that they have tremendous influences on all walks of American life, on all age groups of population. The cybersecurity issues must be of the first priority not only for American scholars and pro-active Internet organizations, but for the country as a whole.

Our concern addressed in that paper is that Ukraine must timely and seriously tackle this problem. It is necessary to create a national policy on cybersecurity bearing in mind that military strategy is not enough to secure lives and souls of new generations of children and adolescents. High and secondary schools together with the researchers of the National Academy of Sciences of Ukraine should and could join their efforts to meet digital future as a way out of stagnation. These enlightening, pedagogical and humanitarian strategies must be based on scientific researches of the highest level. New young generation must be well-educated and psychologically prepared to cope with the challenges of the global economy and network society to feel themselves not as «a lost generation of the 21st century» but as well-educated people who can not only connect with each other by new technological digital devices but to communicate with each other and with the whole world face-to-face as equals.

Literature

1. Зернецька О. В. Рух смислів у глобальному Інтернет-середовищі / О. В. Зернецька // Смислова морфологія соціуму / За ред. Н. Костенко – К.: Інститут соціології НАН України, 2012. – 421 с.

2. America's Cyber Future. Security and Prosperity in the Information Age. Ed. by Kristin M. Lord and T. Sharp. – New York: Center for a New American Security, 2011. – Vol. 1.

3. Are Social Networking Sites Good for Our Society? [Electronic resource]. – URL: http://socialnetworking.procon.org.

4. Castells M. Networks of Outrage and Hope: Social Movements in the Internet Age / M. Castells. – Cambridge, UK: Polity, 2012. – 342 p.

5. Earl J., Kimport K. Digitally Enabled Social Change: Activist in the Internet Age / J. Earl, K. Kimport. – Cambridge, M. A.: MIT Press, 2011. – 272 p.

6. GFI Software. Social Networking at Work: Thanks, but No Thanks? [Electronic resource]. – URL: www.gfi.com.

7. George T. The Next Big Cyber-Crime Vector: Social Media / T. George. [Electronic resource]. – URL: http://www.securityweek.com/next-big-cyber-crime-vector-social-media.

8. Goolsby R. On Cybersecurity, Crowdsourcing, And Social Cyber-Attack / R. Goolsby. [Electronic resource]. – URL: https://www.wilsoncenter.org/sites/default/files/127219170-On Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf.

9. Issenberg S. The Victory Lab: The Secret Science of Winning Campaigns / S. Issenberg. – New York: Crown, 2012. – 384 p.

10. Jobvite. 2012 Social Job Seeker Survey. [Electronic resource]. – URL: www.jobvite.com.

11. MacKinnon R. Consent of the Networked: The Worldwide Struggle for Internet Freedom / R. MacKinnon. – New York: Basic Books, 2013. – 352 p.

12. Nerney C. 5 Top Media Security Threats / C. Nerney. [Electronic resource]. – URL: http://www.networkworld.com/article/2177520/collaboration-social/5-top-social-media-security-threats.htm.

13. Owyang J. Snapshot of Presidential Candidate Social Networking Stats: Nov 3, 2008 / J. Owyang. [Electronic resource]. – URL: http://www.web-strategist.com/blog/2008/11/03/snapshot-of-presidential-candidate-social-networking-stats-nov-2-2008.

14. Palfrey J. and Gasser U. Born Digital: Understanding the First Generation of Digital Natives / J. Palfrey and U. Gasser. – New York: Basic Books, 2008. – 384 p.

15. Pariser E. The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think / E. Pariser. – New York: Penguin Books, 2012. – 292 p.

16. Pew Research Center. Social Media Update 2014. [Electronic resource]. – URL: http://www.pewinternet.org/2015/01/09/social-media-update-2014.

17. Price-Mitchell M. Disadvantages of Social Networking: Surprising Insights from Teens / M. Price-Mitchell. [Electronic resource]. – URL: www.blogs.loc.gov.

18. Raymond M. How Tweet It Is!: Library Acquires Entire Twitter Archive / M. Raymond. [Electronic resource]. – URL: www.blogs.loc.gov.

19. Schepp D. Employees Admit Social Media Is a Waste of Their Time [Infographic] / D. Schepp. [Electronic resource]. – URL: www.jobs.aol.com.

20. Stephens R. How Adolescents Cope with Digital Stress / R. Stephens. [Electronic resource]. – URL: www.blogs.loc.gov.

21. Turkle S. Alone Together: Why We Expect More from Technology and Less from Each Other / S. Turkle. – Basic Books, 2012. – 354 p.

22. Tuchman S. Divorce and Social Networking Sites / S. Tuchman. [Electronic resource]. – URL: www.goodtherapy.org.

23. Wire N. Social Media Report 2012: Social Media Comes of Age / N. Wire. [Electronic resource]. – URL: www.blog.nielsen.com.

24. Zephoria. The Top 20 Valuable Facebook Statistics. [Electronic resource]. – URL: https://zephoria.com/top-15-valuable-facebook-statistics.

Ольга Зернецька, доктор політичних наук, професор, Державна установа «Інститут всесвітньої історії НАНУ», Україна.

КІБЕРБЕЗПЕКА У СОЦІАЛЬНИХ МЕРЕЖАХ США

Анотація. *У статті аналізується роль і вплив соціальних мереж на американське суспільство. У XXI ст. це виявилося одним із пріоритетних завдань Сполучених Штатів Америки. Геополітичні трансформації інколи заставляють швидкими темпами реагувати на інформаційні виклики, які постають перед державою. Не менш важливе вивчення поставлного завдання слід розглядати в рамках запобіганню терористичним актам, стихійним маніфестаціям тощо. Кібербезпека у соціальних мережах сьогодні стає наріжною проблемою кожної країни Світу. Від такої безпеки залежить рівень спокою і миру в суспільстві, стабільність в економічній сфері, політичному середовищі тощо.*

У науковій розвідці досліджуються кібератаки, які загрожують соціальній активності, так само, як і інші ризики для бізнесу, організацій, інституцій, роботодавців та працівників. Особлива увага приділяється змінам у масовій свідомості та у приватному житті американських дорослих та підлітків. Здійснюється аналіз проблем кібербезпеки у соціальних мережах Facebook, Twitter та інших. Ініційовано розробку національної стратегії кібербезпеки України з акцентом на гуманітарному аспекті цього питання.

Ключові слова: *США, кібербезпека, соціальні мережі, Facebook, Twitter*