VULNERABILITIES IN SOCIAL NETWORKS

Colonel (ret.) Professor Gheorghe BOARU, Ph.D [*]
Lieutenant-colonel Adrian-Cristian DAVID, Ph.D [**]

Abstract: *The globalization of cyberspace, the expansion of networks and information systems has led world governments and international organizations to focus on securing cyberspace by establishing security policies and strategies and aspects of global compatibility and standardization.*

In the last decade we are witnessing the emergence of several social networks, which have added a new social dimension to the web, have the ability to create illusory collective identities, train energies that, put together, can generate phenomena difficult to control. They have become an effective tool in achieving a political goal, in overthrowing an illegitimate or abusive regime and in other contexts a real threat.

At the same time, social networks have become an important indicator for the secret services, identifying suspicious activities and providing clues on how to carry them out.

Keywords: *vulnerability, cyberspace, cybersecurity, social network.*

Introduction

The study of social networks emerged in the 19th century and focused on small networks of people and organizations. However, the development of Web 2.0 has greatly influenced the field and moved the focus from social sciences to multidisciplinary approaches centered in computing and automated systems. Indeed, the 21st century witnessed the birth of social networking platforms, which allowed people to communicate virtually regardless of time zone, location, ethnicity, gender, etc.

The new environment is associated with several concerns about freedom of communication and assumed trust that is sometimes misused leading to unpleasant cases that should be identified and treated wisely. The approach to a number of serious problems associated with social networks should not be ignored either.

[*] Entitled member of the Romanian Academy of Scientists; entitled member of the Academy of National Security Sciences, E-mail: boarugheorghe@yahoo.com.

[**] Ph.D, National Defense University "CAROL I", *E-mail: acdcristi@yahoo.com*.

The field of study focuses on recent technical advances and state-of-the-art technologies for the analysis of characteristic features and probabilistic modeling of complex social networks and decentralized online network architectures. Such research results in applications related to surveillance and privacy, fraud analysis, cybercrime, propaganda campaigns, as well as for online social networks such as Facebook.

With the widespread use of computers, communications infrastructure and the Internet, online social networks (***O****nline* ***S****ocial* ***N****etworks* - **OSN**)[1] also known as social networks (***S****ocial* ***N****etwork****s*** - **SNs**)[2], or online social media (**O**nline **S**ocial **M**edia-**OSM**)[3] , have gained immense popularity in recent years. Unfortunately, the very nature and popularity of OSN (SNs, OSM), have made their own "contribution" to fraud and abuse. OSN fraud refers to activities that result in harassment, loss of money, loss of reputation of a person or entity, loss of trust in the system or in a person, etc.

Due to the complex structure and flow of information in NSOs, as well as the relative anonymity of identity, the detection, control and prevention of frauds in NSOs are difficult, time consuming, error prone and require an unusually high level of technical finesse from investigators.

Due to the intensification of information flows per unit of time, which circulates through information systems, as an element of specificity of online work during the Coronavirus pandemic, the vulnerability of information systems (technical and human elements) has increased.

Continuing to perform online service tasks, employees (leaders of organizations and operators) may forget that they need to take some special technical and organizational measures and thus vulnerability to the

[1] Tansel Özyer, Sambit Bakshi, Reda Alhajj, Social Networks and Surveillance for Society, Lecture Notes in Social Networks, Publisher: Springer International Publishing, Year: 2019.

[2] Mehmet Kaya, Reda Alhajj, *Influence and Behavior Analysis in Social Networks and Social Media,* Series: Lecture Notes in Social Networks, Publisher: Springer International Publishing, Year: 2019.

[3] Mehmet Kaya, Suayip Birinci, Jalal Kawash, Reda Alhajj, *Putting Social Media and Networking Data in Practice for Education, Planning, Prediction and Recommendation,* Series: Lecture Notes in Social Networks Publisher: Springer International Publishing, Year: 2020.

confidentiality of the information with which they operate in this cyberspace. Aware of the importance and dependence of this cyberspace, greater security should have been ensured for him and for the information and communication systems that operate with information[4].

Thus, we consider that *"... in the analysis of a military intelligence activity, information can be considered* ***"raw material"****, "****purpose****", "****target****", "****weapon****" and that its protection is all the more important and complex"*[5].

In the military environment, the use of cyberspace, in addition to the many advantages it has, can become an extremely dangerous vulnerability for the security of technical systems and especially information (classified and / or unclassified). It is considered that: *"The existence of this virtual environment or "****cyberspace, recognized as a conflict environment, is based on the successful exploitation of data and information dependence****", manifested at the level of military structures, all the more so as they act in a hybrid conflict environment. In addition to automating actions and digitizing military forces, civil society has made and continues to make a major contribution to increasing the size and definition of cyberspace as the fifth largest conflict environment, along with the terrestrial, air, maritime and cosmic environments"*[6].

In fact, the problem is not new at all. *"Thus, in 1985, a 25-year-old Chinese soldier, Shen Weiguang, wrote an essay entitled "The Information War." In this paper he spoke of notions such as "frontier of information", "intelligence factory", "computerized army", "intelligence police", "fight at home" and described information as an all-encompassing feature of society"*[7].

In addition to the problems specific to the information war, new challenges arose from the Coronavirus pandemic. In fact, whether it is the

[4] Gheorghe BOARU**,** *Pandemia de coronavirus și securitatea cibernetică,* în Revista de Științe ale Securității Naționale, nr. 1/2020, p. 20.

[5] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare*, Editura Universității Naționale de Apărare „Carol I", București, 2018, p. 6.

[6] Gheorghe BOARU, Benedictos IORGA, *Implicațiile participării forțelor militare românești la operațiile de tip coaliție, asupra evoluției și dezvoltării sistemului militar național de comunicații și informatic,* Editura SITECH, Craiova, 2020, p. 236.

[7] Gheorghe BOARU, *Războiul informațional – un obiectiv al securității naționale*, Revista Academiei de Științe ale Securității Naționale nr.2/2019, p. 29.

COVID-19 crisis or another emergency, these 33 suggestions reinforce good security practices and habits. We cannot say with evidence that the SARS-CoV-2 virus is produced in the laboratory by the world actor X or Y and used as a "biological weapon", but we can say with certainty that computer viruses are the result of the work of skilled computer scientists who, for a certain individual or group interest, cause direct or collateral damage to normal users but who do not know or do not comply with the basic "hygiene" rules.

1. Social networks, short history

To facilitate remote access, meaning the ability for a user to connect to a computer located in another geographical location, hundreds or even thousands of kilometers away, and to use certain resources - programs, files, database - in 1969, a computer network comprising four message switches was established at the universities of Los Angeles, Santa Barbara, Stanford and Utah. This is the ARPANET network, which is at the origin of the Internet.

After the first public demonstration of the ARPANET network, in 1972, the idea arose to create a global computer network to cover communication needs.

ARPANET became an international network in 1973, when it consisted of 40 computers, crossing national borders. In 1977, the University of Wisconsin added the e-mail service to the network, which will bring the largest number of users, in 1979 the Usenet service was created - a news network, and 1983 is considered the essential moment in creating the Internet, by introducing the protocol (rules) of communication between computers, called TCP / IP (**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol), well adapted to the interconnection of different networks, which created the premises for the leap from the interconnection of autonomous computers to the interconnection of either local area (LAN) or wide area (WAN) networks.

"For a long time, scientists have largely overlooked the strategic role of computer networks. An initial reason seems to be that infrastructures are usually defined by their invisibility, with most hardly noticing them and

especially when they fail, so that the hidden size of the infrastructure would imply the generic disinterest of researchers in on this subject"[8].

In the early 2000's, social networking sites achieved great success and great sympathy from Internet consumers. In 2002, Friendster laid the foundations of the phenomenon of online social networks. Founder Jonathan Abrams aimed to change the way people communicate and change the face of the Internet through this site. However, Friendster's basic idea was much better implemented by a site that appeared a year later. It is about the famous Myspace, which would have the supremacy in the social-networking field until the rise of Facebook.

The diagram of the most used social platforms is presented in figure 1:

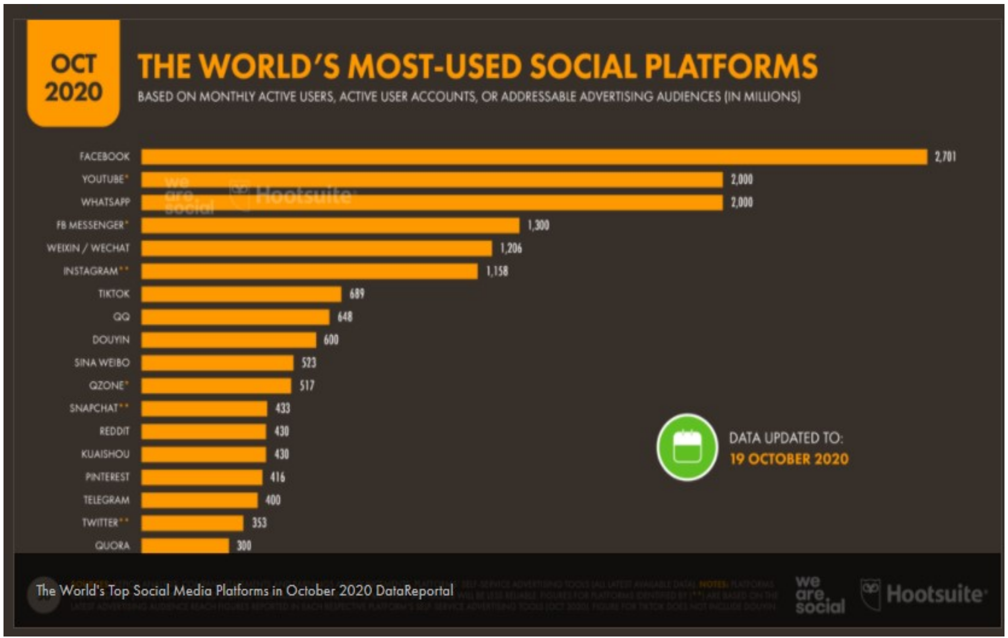

Figure 1. World top of social media platforms in October 2020[9]

[8] Paolo BORY, The Internet Myth:From the Internet Imaginary to Network Ideologies, Editura University of Westminster Press, Londra, 2020, p. 28.

[9] https://datareportal.com/social-media-users, accessed at 03.12.2020.

Founded by Tom Anderson, Brad Greenspan, Chris DeWolfe and Josh Berman, Myspace offered users the ability to create an international network of friends or post videos, pictures or music. The success of the site attracted the attention of News Corporation, which would acquire it in 2005. In 2006, Myspace surpassed Google in the top of the most visited sites in the United States and had over 100 million active users. The decline of the social network Myspace began in 2008, when it began to lose ground to its new rival, ***Facebook***.

Facebook, the new "king" of social networks, has come a long way to this status of a global phenomenon. Created in 2004 by student Mark Zuckerberg, Facebook was originally designed as a university network for students. It then expanded to company employees and with the introduction of new features such as chat, video calling, games, applications and access to mobile phones, Facebook has gradually become a multi-billion-dollar business. Facebook has over 2.7 billion users and is vying with Google for the first position in the top of the most visited sites in the world. The increase in the number of active users was spectacular, as can be seen in the graph in Figure 2.

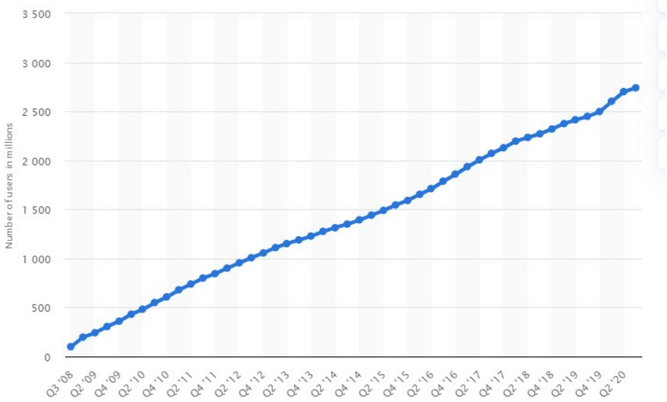

Figure 2. Number of active users / month worldwide 2008-2020(in millions)[10]

[10] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/, Published by J. Clement, Nov 24, 2020, accessed at 03.12.2020.

With more than 2.7 billion monthly active users, starting in the second quarter of 2020, Facebook is the largest social network in the world. In the third quarter of 2012, the number of active Facebook users exceeded one billion, making it the first social network to ever do so. Active users are those who have connected to Facebook in the last 30 days. In the last reported quarter, the company said that 3.14 billion people used at least one of the company's main products (Facebook, WhatsApp, Instagram or Messenger) every month.

The technologization of human life and activity has made the need for communication of the more than **7 829 622 000**[11] people around the world to be provided by these social networks more and more.

The distribution of the number of users on geographical areas and continents shows us that there are countries with a leading position but also countries, in fact with a very large population, which are not in this ranking. We believe that the explanation can be found in the type of political regime in the country, not only in the degree of cultural and technological development (China, the Russian Federation, North Korea, ...).

Figure 3 shows the countries with the most Facebook users in 2020:

[11] *www.worldometers.info* accessed at 03.12.2020.

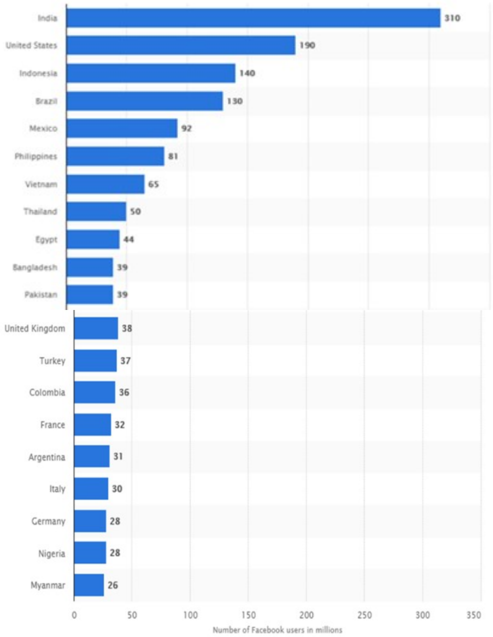

Figure 3. Leading countries based on October 2020 Facebook audience size (in millions)[12]

Another example of a successful social network is **Twitter**, which was created for the rapid, mass spread of short textual news. It did not take long to reach a high level of popularity. Launched in 2006, Twitter began to become a commercial success after just one year. What distinguishes it from other competitors is the minimalist style, the ability to communicate only through short messages limited to 140 characters.

"Twitter provides multi-nodal data containing text, images and videos, as well as contextual and social metadata, such as temporal and spatial information, connectivity information and user interactions. This user-generated data plays a significant role in creating and optimizing

[12] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/, Published by J. Clement, Nov 24, 2020, accessed at 03.12.2020.

public opinion and reactions to contemporary issues. Twitter data can be used for predictive analysis in many areas, ranging from personal and social to public and political health. Predictive analysis of Twitter data includes a collection of techniques to extract information and data models and predict trends, future events and actions based on historical data"[13].

The total number of users reached 340 million[14] in October 2020. As of the first quarter of 2020, Twitter has 166 million monetizable Daily Active Users (mDAU) that can be monetized.

Twitter defines mDAUs as "people, organizations, and other organizations ... that can display ads." This represents an increase of 24% over the previous year, the largest year-on-year increase. Twitter is giving this boost to product improvements and online discussions about the COVID-19 pandemic.

This makes Twitter the 13th most used social networking platform, with about 340 million users. Because Twitter does not publish general monthly active user data (MAUs), this figure is based on the platform's audience coverage.

Among the most influential social networks we can also name Hi5. Although it did not enjoy many fans in the United States (country of origin), Hi5 has long held the supremacy in the field of social networks in Romania. The site attracted like a magnet a lot of young people eager to make online albums with personal pictures and new acquaintances. Although limited in terms of features compared to other profile sites, Hi5 was overtaken by Facebook in Romania only in 2011.

Facebook, MySpace, Twitter, TikTok and many other international online communication and social networking sites have become ideal virtual places for reunions with old friends or opportunities to meet new friends or people with the same concerns, passions and even business. However, behind such networks, which are developing and branching out at an unsuspected speed every moment, there are also dangers that we must be fully aware of before we can enjoy contact with the world.

[13] Nitin AGARWAL, Nima DOKOOHAKI, Serpil TOKDEMIR, Emerging Research Challenges and Opportunities in Computational Social Network Analysis and Mining, Editura Springer International Publishing, New York, S.U.A., 2019, p. 68.

[14] https://www.omnicoreagency.com/twitter-statistics/, accessed at 03.12.2020.

2. Virtual criminals in social networks

Social networking sites have created a real revolution in communication, and in addition to this obvious aspect, the technology in the field is constantly evolving. As a result, most users do not know the basic measures to protect the information held in their computers. Regular users, without advanced knowledge of online protection, comfortably access social networks from the relative shelter of their home or work, thus considering that they enjoy anonymity that would provide a certain degree of security. This largely explains why most of them find out one day that they have shared personal information with people they know too little or even unknown, whom they have chosen from the list of friends of other acquaintances on the Internet.

It should also be acknowledged that, with the development and evolution of communication technologies and the Internet, the methods of virtual criminals have kept pace with them and in some respects have even surpassed them. These cybercriminals have spread social media at an unprecedented rate in recent years, and the trend is growing.

In an article published at the beginning of the Coronavirus pandemic[15], a kind of simplified general guide was elaborated in which 33 recommendations were made, but also advice adapted to the Romanian situation (and not only) regarding cyber security. These suggestions focus on practices and things that individual Internet users but especially organizations can do.

It is appreciated that at the institutional level "*the global and multidimensional nature of the problem of information security, recognizing the need for security governance to be developed to combat the cyber threat and that, in this action, many more levels must be engaged, actors, institutions and people involved in the cyber ecosystem*"[16].

The foremost crimes committed on the Internet concern copyright infringement, in particular the protection of programs, information,

[15] Gheorghe BOARU, Pandamia de coronavirus și securitatea cibernetică, în Revista de Științe ale Securității Naționale, nr. 1/2020, pp. 19-43.

[16] Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană*, în Revista Academiei de Științe ale Securității Naționale, nr. 2/2017, p. 68.

databases, etc., computer fraud, unauthorized access to computer systems and other offenses committed through communications networks.

The biggest danger of these cybercrimes is their cross-border nature. Unauthorized access, regardless of the author's motivation (e.g., the pleasure of infiltrating or defying the security system) is dangerous because it can lead to errors, failures, blockages or even abnormal shutdowns of the computer system.

Cybercriminals theoretically use two major *tactics* to exploit social networks. In practice, these two methods are most often used together.

Hackers are specialized in *exploiting vulnerabilities* in operating systems to have the opportunity to install unwanted software on computers or state-of-the-art mobile phones.

Second, hackers who are specialized in parasitizing and exploiting the opportunities offered to anyone by social networks have become skilled enough to manipulate people on their friends list to gain various benefits. Unfortunately, in this whole story, people are the weak link, and cybercriminals are betting on that. They often manage to fool people without knowledge in the field and thus manage to bypass the passwords or primary means of security in their computers. Their actions are so skillful that, in the eyes of the common man, they seem legitimate and harmless.

In principle, there are three major types of **attacks** that occur on social networks. The first refers to **drive-by** downloads, which describe two situations: either a person downloads a seemingly legitimate software, but it has malicious consequences for the host computer, or its download is done without the knowledge of the person concerned.

Another threat would be a request to start a download, which looks like a **necessary plug-in**, such as QuickTime or Flash, but turns out to be malware in the end.

The third type of threat is **study-based fraud**. In this case, the victim is asked to complete a questionnaire with the personal information from which the data is extracted and used for unauthorized purposes. For example, once a telephone number is obtained through such practices, it may receive telemarketing calls or the information provided may be passed on to data collection companies.

For example, Facebook attacks have three modes of propagation. There are attacks based on **manual sharing**, when someone inadvertently distributes a malicious link. This pattern involves *copy-paste* attacks, and allows attackers to post multiple links on the "victim" screen.

Another form of attack is called **Like-Jacking**. In this case, the link posted on the screen directs you to a site that involves answering a **Captcha-type**[17] security question. In reality, the user presses a hidden **Like** button, which also scans the mouse movement, so that it does not matter where the mouse cursor is positioned when pressed.

A third method is similar to the previous one, only it is based on the comments side. It hides a comment box under a **Captcha**, which then re-posts the malicious link on the screen, to fool the victim's friends as well.

On Twitter there is the **spam method** through direct messages and Twitter-bot responses that send the victim the malicious link. Spammers gain access to a friend's registration data through a **phishing** attack. Phishing is a form of internet fraud, in which criminals create fake copies of popular sites (an e-mail service, an online banking website, a social network, etc.), where they try to lure users. They, being confident, enter registration data and passwords on these sites, as they usually do, but the information reaches cybercriminals. They can then use stolen personal information, bank account data or passwords to steal users' money, send spam and malware through their compromised email account or social network, or they can simply sell stolen data and passwords to other criminals.

Among the most used methods of attacking users, are the following (the names are those used in the specialized international language):

Baiting**:** transmitting a USB device or other type of storage device already infected with malware that will reach the victim's computer (Trojan horse principle) and provide the attacker with all stored information;

Click-jacking**:** consists of hyperlinks cleverly hidden under a legitimate link that is clicked with all confidence. The following is the installation of a malware program on the computer, or the transmission of the victim's personal data to the virtual criminal. Click-jacking experts

[17] Automatic method of determining whether a site visitor is human or not. The name comes from the expression „**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part".

usually install their traps under virtual *Like* or *Share* buttons on social networks;

Cross-Site Scripting (XSS): consists of installing a malicious code on a trusted site. A Stored XSS attack occurs when malicious code gets permanently installed on a server, which will infect any computer that accesses that server. A Reflected XSS attack consists in a user accessing an infected link, the malicious code being sent to the server, from where it is sent back to the victim's browser. The computer considers that code to be secure, from a reliable source;

Doxing**:** is a form of theft in which a person's identity, including full name, date of birth, address and personal photos are removed from the person's profile page, on a social network and made public;

Pharming**:** consists in redirecting the user from a legitimate site to a fraudulent one, in order to extract personal data;

Phreaking*:* consists in obtaining unauthorized access to telecommunications systems;

Scam: refers to fraudulent transactions and business through which victims are persuaded to provide sums of money, personal information or various services in exchange for huge benefits. Cybercriminals often use links to impact news or sporting or artistic events as bait for people who end up accessing infected sites. The scam category also includes online scams in which users are tricked into donating money to fake charities;

Spoofing: consists in misleading computers or even users by hiding the real identity of the attacker. Email spoofing uses a fake email address or simulates a real address. IP spoofing is used to hide the real IP address of the offender's computer.

3. Protest movements coordinated on social networks

Social networks play an important role in the new public sphere. Initially, the virtual domain consisted of small communities, operating independently of each other, like closed groups. Social networks have united these groups, favoring the rapid spread of information to all users.

"The structure of the network can have an impact on the behavior and performance of the actors that form it. For example, actors may be influenced by their neighbors due to various factors such as competition and

cooperation and, in turn, influence other actors. This type of modified attributes composes the virtual behavior"[18].

Social networks such as Facebook or Twitter have become a weapon in the hands of protesters/revolutionaries who use them to organize protest movements. They allow the organizers, at very low costs, to involve a very large number of people in a protest movement, they allow a revolutionary group to spread not only its ideological message, but also its training program and operational plan. The call to protest, at a given moment, can be made in a few seconds and there is no need to prepare a demonstration in advance for a specific date.

This has become a problem for some leadership structures, especially the undemocratic ones, who have found that these networks have become important tools to support revolutions. At the same time, governments and intelligence services can easily monitor social networks to find out the latest information about the users they are following, for example through their Facebook accounts, which provide images, contact lists and location information.

However, such events are not the only contribution of social networks. They also allow a rapid flow of information between people, revitalizing areas such as marketing, journalism or political communication. They also strengthen social cohesion around causes, fostering involvement and facilitating social action. A new environment, with its own advantages and disadvantages, social networks have sometimes become the object of criticism, because they are a tool for communicating ideas and attitudes that can easily circulate.

A significant example, which shows the advantages and disadvantages of social networks is published by ECONOMICA.net on *http://www.economica.net/prezenta-soldatilor-rusi-in-ucrainadeconspirata-de-pasiunea-lor-pentru-retelele-of-socializare_85216.htmlixzz3CuNLWrJK*.

The appetite of the Russian military for social networks has put Moscow in an embarrassing situation, after one of them posted on Instagram two photos located in Ukraine, and others posted comments showing that

[18] Reda ALHAJJ, Jon ROKNE, Encyclopedia of Social Network Analysis and Mining, Ediția a doua, Editura Springer International Publishing, New York, S.U.A., 2019, p. 14.

Russian army units are present on the territory of this country, despite official denials from the Kremlin.

According to the American news site BuzzFeed, the first photo posted by soldier Alexandr Sotkin was located in the village of Volocino, in Russia, where it seems that the unit he belongs to is stationed, and then to post two more pictures, but they are located ten kilometers away on the territory of Ukraine. It is true that the location of photos posted on the Internet can be falsified, but the one who does such an operation needs advanced coding knowledge. In the description of another photo, located in the village of Volocino, the soldier says that he spent the day sitting on a chair, listening to music and taking care of "Buk". The latter word can refer to the name of an anti-aircraft missile, exactly the model used by pro-Russian separatists in eastern Ukraine to shoot down Malaysia Airlines on July 17, 2014.

Other Russian soldiers also posted on the Russian social network Vkontakte, photos without location, but whose descriptions confirm Kiev's accusations that the Russian army fired on Ukrainian positions. One of them wrote on July 23, 2014 that he fired all night at Ukraine, under a picture in which several shells can be seen. The next day he suspended his account, after accusing it of being hacked. On the same social network, another Russian soldier had posted a few days earlier two photos with multiple ground-to-ground missile launchers "Grad", along with the comment "Grad directing to Ukraine", and another even published the route map of its unity towards the Ukrainian border.

Russia's Defense Ministry declined to comment, and Russian Communist MP Vadim Soloviev initiated a bill to limit Russian military access to the Internet, saying such posts were *"a danger to Russia and could be used by Westerners for action." espionage and misinformation"*[19].

In fact, US intelligence officials, quoted by the Washington Post, said that some information proving Russia's military aid to separatists in Ukraine, including in the downing of the Malaysian plane, was collected from social networking sites.

The advantage of the Internet is the globality of communication, and one of the disadvantages is that any type of communication can be

[19] https://www.refworld.org/docid/57726a114.html, accessed at 02.10.2020

intercepted. The Internet, as a scene of interests and as a means of communication, offers opportunities to obtain information that may harm national security or the interests of certain secret services, in the event of non-compliance with strict security rules by users.

Conclusions

The development of social networks has allowed the collection of behavioral data at an unprecedented level of volume and complexity. Accurate prediction and detection of user behavior are key techniques for many media applications, such as referral systems (RSS), personalized search, and social marketing. Behavior modeling in the desired direction to attract profit is significant in real applications and systems.

The expansion of social networks has allowed the dissemination and search for information to take place in an uncontrolled manner. Users, free to post information in the absence of any legal restrictions, have often come into conflict with the defensive actions taken by the governments of nation states, invoking the right to free speech.

The social network can bring information where it is needed but also offers criminals new ways to anonymize their actions. From the theft of personal, confidential data to economic fraud, blackmail and terrorism, a whole range of serious criminal offenses have been transposed into cyber. Of course, the most worrying are those targeting critical infrastructure, i.e., those IT services and systems that are vital to a state and decommissioning or destroying them can have particularly serious consequences.

Cybercrime complicates traditional law enforcement and law enforcement efforts due to their mediation through complex technologies for which the staff involved have neither the technique nor, often, the necessary training. On the one hand, this has led to greater cooperation between the structures involved in harmonizing responses, as well as to an increasing influence of multinational police organizations such as Interpol. However, structures that fight cybercrime face a variety of problems such as:

- the perception among law enforcement that cybercrime consists of minor offenses with limited impact;
- lack of legislation applicable to forms of cybercrime;
- the novelty of many forms of cybercrime that last over time and the low capacity of authorities to respond;

- low reporting of cybercrime, which influences the allocation of resources.

There are, no doubt, other vulnerabilities and opportunities aimed at stimulating the analysis of social networks. Moreover, technology is becoming cheaper and more sophisticated at the same time, with individuals, companies and organizations benefiting more and more from its results. At the same time, at an even faster rate, the number of vulnerabilities that can be identified by both those seeking material benefits and terrorists or nation states directly interested in obtaining information is increasing.

BIBLIOGRAPHY

AGARWAL N., DOKOOHAKI N., TOKDEMIR S., *Emerging Research Challenges and Opportunities in Computational Social Network Analysis and Mining*, Editura Springer International Publishing, New York, S.U.A., 2019.

ALHAJJ R., ROKNE J., *Encyclopedia of Social Network Analysis and Mining*, Ediția a doua, Editura Springer International Publishing, New York, S.U.A., 2019.

BOARU G., IORGA I. M., *Securitatea sistemelor informaționale militare*, Editura Universității Naționale de Apărare „Carol I", București, 2018.

BOARU G., IORGA B., *Implicațiile participării forțelor militare românești la operațiile de tip coaliție, asupra evoluției și dezvoltării sistemului militar național de comunicații și informatic,* Editura SITECH, Craiova, 2020.

BOARU G., *Pandemia de coronavirus și securitatea cibernetică,* în Revista de Științe ale Securității Naționale, nr. 1/2020, pp. 19-43.

BOARU G., *Războiul informațional – un obiectiv al securității naționale*, în Revista Academiei de Științe ale Securității Naționale nr.2/2019, pp. 23-37.

BOARU G., *Securitatea cibernetică în Uniunea Europeană*, în Revista Academiei de Științe ale Securității Naționale, nr. 2/2017, pp. 65-79.

BORY P., *The Internet Myth:From the Internet Imaginary to Network Ideologies*, Editura University of Westminster Press, Londra, 2020.

FANG B., JIA Y., *Online Social Network Analysis*, Ediția a treia, Editura Walter de Gruyter GmbH, Berlin, 2019.

KAYA M., ALHAJJ R., *Influence and Behavior Analysis in Social Networks and Social Media*, Series: Lecture Notes in Social Networks, Publisher: Springer International Publishing, Year: 2019.

KAYA M., BIRINCI S., KAWASH J., ALHAJJ R., *Putting Social Media and Networking Data in Practice for Education, Planning, Prediction and Recommendation*, Series: Lecture Notes in Social Networks Publisher: Springer International Publishing, Year: 2020.

ÖZYER T., BAKSHI S., ALHAJJ R., *Social Networks and Surveillance for Society, Lecture Notes in Social Networks*, Publisher: Springer International Publishing, Year: 2019.

Guide - Security in social networks and parental control in the online environment – Bitdefender.

Electronic sources

https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/;

https://www.worldometers.info › wor....;

https://www.refworld.org/docid/57726a114.html;

https://datareportal.com/social-media-users;

https://www.omnicoreagency.com/twitter-statistics/;

http://download.cnet.com/8301-2007_4-57456546-12/how-attacks-on-social-networks-work/;

http://www.economica.net/prezenta-soldatilor-rusi-in-ucraina-deconspirata-de-pasiunea-lor-pentru-retelele-de-socializare_85216.html-#ixzz3CuNLWrJK;

https://www.refworld.org/docid/57726a114.html;

www.nato.int.