sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 1 2020

AN INTELLIGENCE PERSPECTIVE ON PRIVACY AND DATA PROTECTION RISKS IN SOCIAL MEDIA

Andrei ȘANDOR

NATO HUMINT Centre of Excellence, Oradea, Romania
andrei.sandor@natohcoe.org

Abstract: *Since the emergence of Internet and social media, new Intelligence branches have flourished, like CYBERINT (Cyber Intelligence), OSINT (Open Source Intelligence) or SOCMINT (Social Media Intelligence), with the aim to exploit different dimensions of the virtual world. These Intelligence-related disciplines may inquire personal information, statements and conversations posted voluntarily on websites or social platforms in order to profile people, identify social networks and organizational structures, and uncover vulnerabilities and threats/ risks that can jeopardize the security of individuals or organizations. In this respect, the Internet - as environment - can provide valuable information from both technical and social side. This is why the World Wide Web is and will remain an important place to search for data and information that can be processed into Intelligence, and represents the reason why people working in sensitive domains (e.g. Intelligence) should be aware of their vulnerabilities and the risks and threats posed by this environment.*
DISCLAIMER*: This paper expresses the views, interpretations, and independent position of the authors. It should not be regarded as an official document, nor expressing formal opinions or policies, of NATO or the HUMINT Centre of Excellence.*

Keywords: CYBERINT, OSINT, social media, social engineering

1. Introduction

As history demonstrates, Intelligence collection evolved and adapted as social trends and technology developed. These two factors, society and technology, are in a close relationship, as we can remark the case of social media, where the individual or professional presence/ activity may become part of the social behaviour of a person.

The most important factor that shaped modern Intelligence is definitely technology, with the advent of WEB 2.0, social media, and smart technologies.

Web 2.0 comes with a new way of information spreading, as social media allows the Web to move from data and applications to user interaction and experience [1]. This means that the modern World Wide Web does not restrict Internet users just to read data or information but also allows them to share on different platforms their thoughts, opinions, personal data, and so on.

All this freedom of data sharing comes with big risks regarding personal and organizational security, as new opportunities for information collection and analysis occur.

The main *Intelligence* or *Competitive Intelligence* related branches that benefit from the Web 2.0 development are CYBERINT, OSINT, and social engineering, the last one being analysed from the perspective of Intelligence collection, and not regarded as criminal activity in cyberspace.

DOI: 10.2478/kbo-2020-0023

2. CYBERINT in social media – technical means for Intelligence gathering

CYBERINT is a discipline of acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain [2]. As the cyber dimension became common space, as extension or reality replica for various activities, both from a technical and social point of view, CYBERINT may overlap with traditional Intelligence collection disciplines like SIGINT or HUMINT.

Commonly, cyber operations are encountered in three major forms: computer network defense, computer network attack, and computer network exploitation [3]. In this paper, we refer in particular to the individual/ organisational risks emerging from computer network exploitation, where we consider the computer as any device that may connect to other device or to a cloud and the network – the Internet.

From this technical perspective, the most common vulnerability for both personal and social platform equipments is represented by gaps in software or hardware design. For any equipment, at a moment of its lifecycle, security vulnerabilities may occur, as technology develops.

Devices can send information or can be scanned in order to obtain data that may be used for Intelligence processing. The most important elements that facilitate data collection are connectivity and poor security. These may reveal data processed by the sensors that every device has, as we can see the example for smartphones in figure 1.

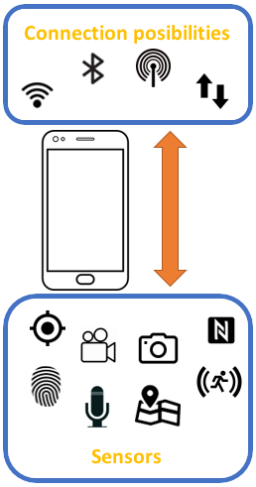

Figure 1: Sensors and connectivity features of a smartphone

In addition, the use of Internet and social platforms may reveal personal data about users. By living in a media-saturated social world, we leave behind footprints of our media use [4], both on our devices and the platforms we use. This creates two vulnerable points where information gathering activities can be focused on: the individual devices, or the platform that provides a service.

Personal devices are often set up with minimum security settings (in order to be comfortably accessed by their users), and this may represent a risk for personal data exposure and further exploitation by external entities.

Regarding social platforms, all of them store data in cloud, on more than one server. All social media data provided by users and usage-related data stored on the servers - property of private companies - are exposed to the resident country rules and their potential use for financial gain, as long as companies can exchange users' data for a benefit.

3. OSINT in WEB 2.0

With the advent of Web 2.0, we can remark an exponential growth of data available on the World Wide Web, as well as a social trend to publicly (or, in the best case, in an inferred protected way) share data that may be of interest for Intelligence organizations.

The huge quantity of data readily available online and its exponentially growing volume is a challenge for OSINT processing, in the effort to split valuable data from old, obsolete information, and disregard fake news or other irrelevant contents.

In this respect, probably the most important opportunity for Intelligence gathering (and associated risk for personal data processing by external entities) in Internet environment is Big Data analytics. Big Data analytics, as well as the analysis of smaller datasets, can reveal descriptive, predictive and/or prescriptive insights about entities, phenomena, or processes [5]. This type of analysis can use voluntarily shared data by individuals or collected by specific technical data gathering means and involves a huge volume of data with a wide range of data type – images, videos, text, or activity patterns.

Big Data analysis is facilitated by the continuous development of the modern systems' processing capacity; by comparison, analysing big data by humans is almost impossible due to the high volume of information to be handled.

An important opportunity for OSINT collection is represented by the possibility to reveal the social sentiment of a group. This is very important, because Intelligence products related to the social sentiment may offer decision makers an advantage at strategic level (figure 2); at the same time, the targeted organizations or communities are placed in a vulnerable position.

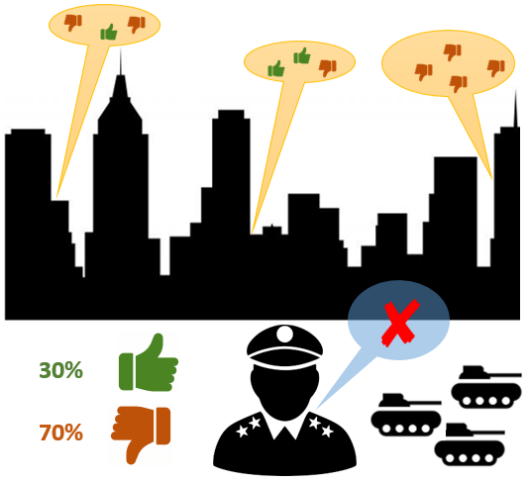

Figure 2: Decision based on social sentiment in military operations

By gathering information related to social sentiment, organizations can also acquire real-time data on warfare-related actions, as part of their early warning efforts [6].

Another Intelligence collection opportunity that exploits data exposure is represented by mapping platforms. Such platforms offer users the possibility to upload photos or comments on maps, making possible an enhanced evaluation of a target area.

A particular approach on mapping in the advent of Web 2.0 talks about social mapping as a method of modelling, visualization and graphic representation of any spatially localized information, serving the purpose to gain knowledge on the represented phenomena [7]. It is obvious that data gathered are more valuable for analysts if added to a map. This way, as a result of information processing, social or security-related aspects tagged to maps offer a higher level of understanding the environment and support foresight analysis.

Being aware of the opportunities that social platforms features offer to Big Data analytics we can expect manipulative actions oriented towards influencing personal perceptions, motivations, or actions.

4. Social engineering

Social engineering has both technical and psychological sides, the latter being the

most important. So, by exploiting human errors, social engineering can be used to gather private data from organizational/ private networks.

Researchers in cyber security warned that apart from focusing on technology development, the human factor should be also considered when combating cyber threats [8]. Our lives are in a close connection with technology, and often the weakest link in the chain of security within organizations that uses computer systems is the human.

From the social perspective, the technique used in social engineering is persuasion, based on the following principles: reciprocation, consistency, liking, social proof, scarcity, authority [9]. Often these principles of social engineering try to exploit some desired or positive human traits.

Social engineers may pretend to be somebody important like a big boss from headquarters, an inspector from a government agency, a top customer of the organization, or someone else who can assault fear into the heart of regular employees [10]. By this technique, they use the principle of authority, trying to obtain information by intimidating people.

Social proof is a psychological phenomenon that occurs in social situations when people are unable to determine the appropriate mode of behaviour [11]. This way, social engineers can use persuasion techniques in order to create an appropriate image of a situation where the victim will do something in the expected way.

Social engineers use reciprocation, consistency, liking, or scarcity to obtain information from people sensitive to these natural principles and possessing a low level of security culture. All of these principles reflect the way people feel about getting in touch with someone and can be used in a very complex manner to persuade someone to follow a prescribed behaviour.

Social engineering attacks are likely to happen against organizations without proper and well-defined processes, or with regulation gaps. If there are precise procedures for every possible situation and the members of the organizations are well trained, obey security rules and respect procedures, a social engineering attack that is trying to exploit human error is unlikely to happen.

From the technical point of view, we can classify social engineering according to the environment (impersonation in the real world, phishing or vishing in the cyber environment, baiting, tailgating and so on) and to the tools (for link analysis, forensics, spoofing, GPS tracking, and others) used for data or information gathering.

Phishing represents a form of social engineering that implies the disguise of the social engineer's identity in the cyber environment as being a trustworthy entity.

Baiting is conducted through exploiting the greed or curiosity of people to click on a winning banner, to open a link or to check the content of a "lost" memory USB.

Tailgating or piggybacking represents the situation in which the social engineer enters an unauthorized area passing by with an authorized person that is granting access.

Spoofing represent in a general manner the disguising of an identity from a technical point of view. Spoofing is widely used by hackers or social engineers to mask their identity or to seem to be someone else.

The technical part of social engineering is actually not as complex as system exploitation from a CYBERINT perspective, for example. Social engineers use tools like SET – Social Engineering Toolkit, an open source framework that facilitates social engineering activities, offering multiple attacking options, as we see in figure 3.

Figure 3: Options from SET, Kali OS

Social engineering may overlap until a certain point with Intelligence data collection in social media, by using communication means offered by those platforms [12]; this approach opens further discussions regarding HUMINT in cyber or cyber-HUMINT operations that can use social engineering principles.

What is to be retained from the perspective of personal protection when interacting trough social media is to firstly check the real identity of the counterpart, by simply contacting him through verified communication means (e.g. phone) or establishing video contact with the person you are supposed to know. Advanced methods (like IP checking) can further offer a relevant insight in this respect.

5. Conclusions

The development of Web 2.0 opens new opportunities for Intelligence collection from a multidisciplinary perspective, hand in hand with the risks and vulnerabilities represented by personal or organizational data exposure. As the main feature of Web 2.0 – also called the Participative or Social Web, is adding media on platforms just at a login distance, the role of people in the cyber environment is more and more important.

People can choose what to share on social media and they need to pay attention to the new online socialization in order to avoid sensitive data disclosure. Even if they use a username and password in order to restrict general access to their data, social media users should assume that every data posted on the platform can be accessed by an interested entity.

The social aspect of the modern Internet makes possible the exploitation of cyberspace not just from a technical point of view, but also from a social perspective; this creates development opportunities for disciplines like Counter Intelligence and HUMINT.

The most important aspect to counter Intelligence collection in social media is education. If people have knowledge on security aspects in cyber environment, Intelligence collection can be critically limited.

Well-determined organizational processes are another feature that can oppose intelligence collection activities, specifically social engineering attacks against companies or governmental institutions. This means that every member of an organization knows what to do, what his responsibilities are, and is less likely to make a mistake through which to reveal valuable or sensitive data.

Due to advanced technical collection possibilities and social link analysis, people should make a clear distinction between the personal and the professional life. If devices intended for work are used for personal purposes or vice versa, important data can be unwillingly revealed.

On the other hand, as Social Media and the Internet are constantly evolving, Intelligence services (as well as economic competitors, or petty cyber criminals) are prone to always search for collection opportunities and enhanced methods and tools that bring new risks and vulnerabilities against personal and organisational data protection.

References

[1] Surya NEPAL, Cecile PARIS, Atham BOUGUETTAYA, Trusting the Social Web: issues and challenges, World Wide Web, Vol. 18, No. 1, pp. 1-7, p. 3, 2015.

[2] Jared ETTINGER, Cyber Intelligence Tradecraft Report. The State of Cyber Intelligence Practices in the United States, Carnegie Mellon University, Software Engineering Institute, p.113, 2019.

[3] Robert M. CLARK, Mark C. OLESON, Cyber Intelligence, Intelligencer: Journal of U.S. Intelligence Studies, Vol. 24, No. 3, pp. 11-23, p.14, 2018.

[4] Andreas HEPP, Andreas BREITER, Digital traces in context, International Journal of Communication, No. 12, pp. 439-449, p.439, 2018.

[5] Adrian BARBU, Tudor RAȚ, Big data analysis through the lens of Business Intelligence – world conflict incidents case study (1989-2016), Revista Română de Studii de Intelligence Studies, No. 17-18, pp. 157-164, p.159, 2017.

[6] Elena SUSNEA, A real-time social media monitoring system as an Open Source Intelligence (OSINT) platform for early warning in crisis situations, International Conference Knowledge-Based Organization, Vol. 24, Issue 2, pp. 427-431, p. 429, 2018.

[7] Marat Rashitovich SAFIULLIN, Polina Olegovna ERMOLAEVA, Oleg Petrovich YERMOLAEV, Renat Nailevich SELIANOV, Current Perspectives on Social Mapping of Urban Territories, Asian Social Science, Vol. 11, No. 6, pp. 207-213, p. 207, 2015.

[8] Ana BADEA-MIHALCEA, People and Machines: Dealing with Human Factor in Cyber-Security, Considerations on Challenges and Future Directions in Cybersecurity, pp. 143-154, p. 207, 2019.

[9] https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/42-persuasion-techniques, accessed 21.02.2020, 15:45.

[10] Neetu BANSLA, Swati KUNWAR, Khushboo JAIN, Social Engineering: A Technique for Managing Human Behavior, Journal of Information Technology and Sciences, Vol. 5, Issue 1, pp. 18-22, p. 10, 2019.

[11] https://www.social-engineer.org/framework/influencing-others/influence-tactics/social-proof/, accessed 21.02.2020, 14:45.

[12] Keith Gregory LOGAN, Homeland Security and Intelligence, Second Edition, p. 161, 2018.