Social engineering as the new deception game

Aurelian STOICA

National Institute for Research and Development in Informatics – ICI Bucharest

aurelian.stoica@ici.ro

Abstract: As the general interest in the cybersecurity field grew in the last years, more and more researchers focused on the social engineering topic. Most of the studies approached the technical aspects of the social engineering, establishing and describing categories of human enabled cyber-attacks and positioning the concept in the IT security environment, which helps in crafting defensive techniques. This paper argues that social engineering roots are deeply established in the intelligence field, and it should be studied and understood in its social influence dimension with the same importance as the engineering one. Furthermore, the research groups social engineering tactics into state-driven social engineering and privately driven social engineering based on their coordinating entities. The lack of technology layer in social engineering activities of the past (compared to today's flourishing digital ecosystem) was efficiently compensated by the higher degree of creativity of the people designing them, and the state apparatus support.

Keywords: social engineering, social influence, cybersecurity, deception, framing.

Ingineria socială - noul joc al înșelăciunii

Rezumat: Pe măsură ce interesul general pentru domeniul securității cibernetice a crescut în ultimii ani, tot mai mulți cercetători s-au concentrat pe domeniul ingineriei sociale. Majoritatea studiilor au abordat aspectele tehnice ale ingineriei sociale, stabilind și descriind categorii de atacuri cibernetice cu posibilități umane și poziționând conceptul mai degrabă în mediul de securitate IT, aspect care ajută în elaborarea tehnicilor defensive. Această lucrare susține că rădăcinile ingineriei sociale sunt stabilite în profunzime în zona de intelligence iar fenomenul ar trebui studiat și înțeles în dimensiunea sa de influență socială cu aceeași importanță precum în cea de inginerie. Mai mult, cercetarea grupează tacticile de inginerie socială în categoria de inginerie socială inițiată de actori statali și în categoria de inginerie socială de ordin privat, pe baza entităților care le coordonează. Lipsa componentei tehnologice în activitățile de inginerie socială din trecut (în comparație cu ecosistemul digital înfloritor de astăzi) a fost compensată în mod eficient de nivelul mai ridicat de creativitate al persoanelor care le-au proiectat și de sprijinul din partea aparatului de stat.

Cuvinte cheie: inginerie socială, influență socială, securitate cibernetică, înșelăciune, înscenare.

1. Introduction

As technologies developed at an exponential rate in the last decades, their impact on society became more and more prevalent. The abundance of social networking sites, mobile technology, and Internet access provided enormous opportunities for combined attack techniques, yielding a higher attack success rate. As the connectivity between people, computers and mobile devices increased constantly, we reached a point in the history of humanity where the development created the so-called network society (Castells, 1996/2009). In this interrelated ecosystem, human interactions are based on communication and they rely heavily on the technology, as it ensures almost instant speed, low costs and easy access for everyone. At the same time, interactions are designed based on the concept of power, with an assumed goal of influencing the others in the loop.

When the intended influence activity is also based on technical skills and is supported by technology, we could say that conditions for the social engineering occurrence are met. When

https://doi.org/10.33436/v31i3y202105

influence operations are perpetrated, they are usually targeting three main layers in a society (Pamment et al., 2018):

1. **Societal level targeting** – directed towards mass audiences;

2. **Sociodemographic targeting** – aimed at influencing groups;

3. **Psychographic targeting** – focused on individuals.

In the latter, the targets can be influential leaders, politicians or high-level governmental figures, but also normal citizens. The difference is in the intended goal: either extracting valuable, strategic information, or aiming to steal credentials (e.g., of a banking account) that could allow later access to financial resources. For this third layer, technical and social skills are put at work by individuals and groups, in an integrated approach that we call social engineering. Some authors go beyond the necessary technical skills to perform social engineering activities, stating that this is a fine art requiring almost the level of hacking skills (Alyoubi & Alyoubi, 2013).

Because many studies do not make a clear distinction between different processes of the social influence concept and social engineering notion, the concepts being frequently mixed, few theoretical clarifications should be made. Besides, social engineering is a relatively new term in the public opinion agenda and scientific researches (although mentioned a few decades ago) and considering this a milestone in the integrated research of social sciences and information security could create confusions. Social engineering is even interchanged with the deception concept, which is a phenomenon within the broader influence field, but cultivated and grown to expertise in the intelligence sector. Long before social engineering, there were advanced, organized activities of deception and disinformation, which are concepts particular to intelligence sector, that people easily use these days to identify more light concepts like persuasion or manipulation. This terminology gap needs to be addressed with the aim of better establishing the history, borders and accurate use of the phenomena mentioned frequently these days both in researches and cybersecurity reports. Social engineering tactics have long been studied and applied in organized environments, they were part of skilled influence campaigns and, with the support of technology, are revived these days in an optimized approach, that currently affects more categories of people than in the past.

2. Literature review

Many papers on social engineering, either academic or technical reports, devoted an impressive effort to position the concept in the historical framework, as there are different approaches in this respect. The term was first mentioned in a 1842 book, written by the British economist John Gray, on the topic of replacing the gold as a standard for exchange with a currency. For Gray, the political and social engineers play a role in curing society similar to that of the mechanical engineers repairing a steam engine (Hatfield, 2017).

One of the most recent and comprehensive definitions of social engineering is the one included in the glossary of the European Union Agency for Cybersecurity, as the techniques used to convince a target to reveal information or perform actions whose reasons are illegitimate (ENISA, 2021). It considers both the role of psychological manipulation to penetrate an IT system and of the technologies supporting the manipulation process, like credentials used later for attacks. In other views, social engineering is defined as the deception used to manipulate people with the aim of obtaining an information or performing a specific action (Mann, 2008). Extending the framework, one study considers that social engineering stands on three main pillars: influence, persuasion and manipulation used in the process of deceiving people about who is or is not the social engineer (Mitnick & Simon, 2002). Other definitions of the concept put an accent on its capability to trick users to make a poor trust decision (Rains, 2020), underlining the impressive number of this type of malicious attacks and also their high success rate. This is definitely a reason for the solid scientific interest on this topic raised among the researchers from both social sciences and information security fields.

One particular view – that will be further detailed – consider social engineering as manipulation of a target person to act in a way that isn't in their best interest (Hadnagy, 2011). Such an approach is an exponent of a wider category of studies that interchange the social engineering concept with the social influence one, considering them equal processes. In addition, arguing that social engineers could all be hackers, penetration testers, identity thieves, disgruntled employees, executive recruiters, sales people, governments, doctors, lawyers and psychologists (Reynolds, 2015) is a forced terminological and conceptual approach, that could potentially emerge from a misunderstanding of the theoretical distinctions of the psychosociological processes functioning.

Studies coming from the information security domain put in the same basket of social engineers people with malicious intentions and natural skills for tricking together with trained professionals in deception, which is a challenging comparison. In fact, many authors interested in social engineering often misuse the terms when invoking phenomena such as influence, manipulation, persuasion, deception, and social influence components in general, although there are well-known theoretical delimitations between those concepts. There are academics for whom influence, propaganda, persuasion and manipulation are the same, with common roots in the communication studies (Muchielli, 2000). But distinctions between the influence phenomena exist and were clearly pointed out in extensive researches that underline the important role of ethical aspects and the negative impact on the victim when categorizing them (Chelcea, 2006).

I therefore sustain that exploiting human psychology is a must in the social engineering activities, but opposed to the views that consider every act of influence as social engineering, the main goal should be obtaining access to key systems, data and facilities, in order to exfiltrate strategic/valuable information or financial gains with the support of technology. Such an offensive activity has its own cycle of life, composed of several stages, the most important being:

1. Information gathering;
2. Developing relationships;
3. Exploitation;
4. Execution.

with various motivations such as financial gain, self-interest, revenge or external pressure (Allen, 2006). I agree with and endorse Mitnick & Simon statement that the important points in the process of defining a social engineer are its technical knowledge and skills in computer & phone systems (2002). The technology layer base of an individual involved in social engineering activities and the main goals established in the process are shaping the differences between a profile of an expert in the field and people with other interests engaged in known social influence processes acts. For others, the social engineering exploits human vulnerabilities when attacking a cyber security target, but it is not necessary to use in the process technical tools and exploit technical flaws (Wang, Zhu & Sun, 2020).

As most of the definitions invoke the influence process involved in the human interactions, it should be mentioned that maybe one of the most structured descriptions belongs to Robert A. Dahl, stating that influence occurs when a person has power over another to the point where the latter is doing an action that he/she wouldn't otherwise do (Dahl, 1957). Expanding this power-related view to the social environment, I resonate with one particular definition that considers social influence as an asymmetrical action between two social entities, one having the goal of changing the attitudes and beliefs of the other (Elinschi & Ciupercă, 2003). Influence can occur either in the form of one individual trying to convince another to change their view or trying to make a group act in a desired direction or in the form of a group socially pressing an individual to adopt a decision. While recent studies in social engineering (Wang, Zhu & Sun, 2021) place social influence as an effect mechanism on the same level with persuasion and deception, I would consider social influence as the general framework where specific processes such as persuasion or manipulation take place in order for the social engineering activity to succeed.

In most of the social engineering activities, authors underline the term of influence (under various forms such as persuasion or manipulation), so it is relevant to mention the main functioning principles described by its most famous researcher (Cialdini, 1984/2007). Whenever we have a human interaction, there are several situations in which if positioned, we have increased chances to consolidate the change action of the individual target, as follows:

1. **Reciprocity** – returning the favors we receive;

2. **Commitment/consistency** – individuals want to be consistent with actions/choices already taken/made;

3. **Social proof** – people see an action as more appropriate when others are performing it;

4. **Authority** – or obedience to authority actions;

5. **Liking** – accepting requests of someone we know and like;

6. **Scarcity** – attraction for the limited-number items.

3. Social engineering categories and techniques

Previous studies grouped social engineering activities in two main categories: computer/technology-based deception and human-based deception (Abbas, 2018) or computer-based attack and human-based attack (Ghafir et al., 2016). These two main categories have been further detailed and explained. Other researches worked on the above categories and identified a cluster composed of four main areas: physical (e.g., accessing workspaces), technical (attacks are carried out over the Internet), social (relying on sociopsychological principles of influence), and socio-technical (combining the previous three) (Krombholz et al., 2015).

Human-based attacks have been structured in the following techniques:

1. **Impersonation** – when a hacker presents himself as a legitimate user/employee with the purpose to gain access;

2. **Posing as an important user** – e.g., when claiming the role of a high-level manager;

3. **Claiming to be a third party** – claiming to have permission from an authorized person;

4. **Desktop support** – calling technical support team and impersonating a user needing help.

Computer-based social engineering attacks were also further detailed in the following techniques (Kumar, Chaudhary & Kumar, 2015):

1. **Phishing** – usually through email that looks from a legitimate source;

2. **Baiting** – lures based on USB or programs for download that install malicious software;

3. **On-line scams** – emails with malicious code;

4. **Pop-up windows** – asking to enter network credentials;

5. **Email attachments** – emails with hidden viruses;

6. **Email scams** – e.g., fake lotteries prizes;

7. **Chain Letters and Hoaxes** – generating loss of productivity and use of resources.

Other scholars (Breda, Barbosa & Morais, 2017) preferred a different separation: the Social category (Tailgating – following an employee to an open door, Impersonating, Eavesdropping – listening to communicating channels such as emails and telephone lines, Shoulder surfing – to visually collect data, Dumpster diving – searching for improperly disposed documents, Reverse social engineering – encouraging the target to initiate communication) and the Socio-Technical category (Phishing, Baiting, Watering hole – infecting a legitimate website frequently accessed by the target). In addition, using phones to call a target or to leave messages asking for specific actions, in a perceived manner that induces a legitimate organization or person is a newer technique

called vishing. Other recent methods such as spear-phishing – attack focused on a specific individual (a clear example of the previously mentioned psychographic targeting level), QRishing (using QR codes), Smishing (using SMS), Malvertisement (fake advertisement), Wi-Fi even twin (creating a similar Wi-Fi network name to get information) were referenced and discussed in detail (Yasin et al., 2019).

A paper grouping social engineering activities not in techniques categories but in topics that frequent social engineering situations are built on (Alsufyani et al., 2020) has detailed the following: 1. Worker data; 2. Emails; 3. Directed documents; 4. Bills; 4. IDs and PINs; 5. Electronical media; 6. Handbook, Manual and Operational Actions; 7. Signs (from business leaders). I suggest that in the future defense trainings that organizations conduct for their employees it would maybe be better to describe the techniques, but to focus especially on such topics as the above, as it is easier for people with no professional experience or special skills to identify the solicited item, rather than the technique.

I argue that the social engineering activities can be structured, based on their historical roots, in two main categories:

1. **State-driven social engineering initiatives** – when attacks are synchronized with wider infrastructure hacking strategies and are perpetrated by groups affiliated to/supported by state agencies, with the main goal to capture sensitive strategic information or to produce a damage;

2. **Privately driven social engineering initiatives** – when attacks are launched by individuals or groups with the main goal to obtain financial gains, notoriety or distraction.

An example of the first category is the campaign run by the Iranian hacking group Tortoiseshell, that used social engineering methods to target US military personnel. Through a combination of a fake site and a downloadable malware containing malicious spying tools, the attack retrieved various information about the user and the system, with the potential of further exploitations (Mercer, Rascagneres & An, 2019). Recently, the same group continued the initial plan of targeting US military members, by developing social engineering tactics based on fake accounts on Facebook and phishing sites that were planned to collect credentials (Greenberg, 2021). Such groups are connected to or gravitating around state agencies and execute offensive commands against foreign adversaries.

Previously, Russian state affiliated groups executed social engineering campaigns in US presidential elections, Brexit (2016), French presidential elections (2017) and other key events. It should be understood that highly skilled social engineering campaigns are not a result of private individuals with a native set of abilities, but are the product of trained groups in close relation to state agencies from countries aiming to interfere abroad in the internal politics of those perceived as adversaries. Either we call it cyber influence, disinformation, foreign intervention, cyber warfare or active measures, the process of engaging in hybrid attacks against other countries is designed by and implemented by intelligence entities and it encapsulates creative social engineering techniques (Erbschloe, 2020).

As studies find, pretexting (or impersonation) is maybe one of the most frequent applied techniques in social engineering, when the attacker uses a scenario to persuade a target, that under the influence of the perceived relationship with the attacker (subordination, familiarity, professional support) divulges sensitive information about an organization or personal, individual, details (Luo et al., 2011). For others, pretexting is a type of attack that appears when the attackers construct an entire scenario in which the victim is playing a central role, thus the possibility to reveal valuable information is subsequently increased (Lohani, 2019). Authors developed the framework containing the main stages of a social engineering cycle as follows: 1. Information gathering; 2. Elicitation; 3. Pretexting; 4. Mind tricks; 5. Persuasion; 6. Targeting; 7. Recon. Pretexting is a critical phase in this chain, and the skill is considered mandatory for a social engineer in order to ensure the success of its operations, to such an extent that it should eventually "become" the role he is impersonating (Ozkaya, 2018). In order for the pretexting activity to succeed, two components must by achieved: 1. A plausible situation, defined as a sequence of events designed to be believed; and 2. A character, defined as the role that a social engineer is

playing, in an actor/fictious approach (Watson, Mason & Ackroyd, 2014). Pretexting has been naturally connected to the commercial sector in case studies or examples destined to explain the functioning of the process – e.g., when a "pretending" senior member of an organization calls a junior representative and influences him to divulge customer data, internal details or credentials for systems access.

4. Framing, deception and disinformation – social engineering roots

If we attempt summarizing the concept of social engineering, the most expressive definition is the one stating that social engineering is actually lying, but its name just sounds better than calling someone a liar (Cole & Ring, 2006). Because many of the social engineering examples frequently exposed in the media focus on extorting financial resources from the victims, we tend to assume that this is the field the term stemmed from. In fact, the intelligence field is the territory where the skills of crafting lies, deception and disinformation were organizationally studied and applied, attaining over time a mastery level. In the past, disinformation was designed to target mass audiences, national and international public opinion, as opposed to operations influencing an individual or a small group. This was the reason that such a strategic activity was entrusted to the state agencies that had the strategy, the capabilities and the resources to work complex disinformation scenarios targeting adversary's audience.

Using radio, TV, newspapers, influential leaders or political representatives, complex strategies were applied to hit the enemies in such a way that they could never understand who was behind it. Most mentions about disinformation go back almost 100 years ago, to the moment when Russia created its first disinformation office – in 1923. Decade after decade, this office grew to a Department (D) level, a Service (A) within the KGB and, after the collapse of the Soviet Union, it continued as a new Department (for Support Measures), delivering their specialized work while relying on newer and better supports to reach the objectives. In its highest points during the Cold War (the 70's and 80's), the disinformation activity in the Soviet Union was counting on 15,000 operatives trained and engaged in psychological warfare, while billions of USD were spent each year to support this army (Nance, 2018). Delivering activities currently known to the public as active measures, the above-mentioned department/service creatively imagined dirty schemes, crafted machinations, disinformation campaigns, document forgeries, movie-like scenarios and black propaganda with the aim of manipulating selected individuals, important decision makers, political and religious leaders. But maybe the most strategic goal was to deliver high quality deceptions to their counterparts from the intelligence and military field, in such a manner that they would neither realize the lie, nor identify its creator.

But the true meaning of the disinformation/active measure is in the term "framing" (subversive framing operations), described by Gen. Ion-Mihai Pacepa (highest-ranking Soviet Bloc defector to the West) as the rewriting of history through manipulation of records and documents (Pacepa & Rychlak, 2013). Kremlin and its satellites specialized in two types of framings: negative – demotion of people and positive – that had a promotion goal. Individual behaviors and rapports with the ideology and the Party defined the way people's future and past were written. For those who betrayed the cause, their past itself could easily be readjusted by KGB and its satellites to correspond to the current status – you could become in documents that enemy the state said you were, if necessary. When Andrey Sakharov became ill in the 80's, the KGB 5th Directorate instructed its members to provide the Western media with disinformation that he himself caused this health deterioration by not following the physician's advice (Rubenstein & Gribanov, 2005). For the Soviet Union establishment, the enemies could be found outside, but they could also act (subversively) inside.

As Pacepa detailed, framing was a complex technique that for the elite of the intelligence was almost an art. The black art of framing, the art of deception, the art of forgery, the dark art of disinformation or even the "science" of disinformation – this is the image the masters and strategists projected over their work. During communism, it was based on portrayed people, false stories and fake news, fabricated documents and support organizations/persons. These days, the

power resides in social networking sites, messaging platforms and fake websites. But the link exists between the old operations and the current ones, the tradition has been continued from subversive activities to modern cyber-attacks (Barber, 2016). I argue this is also the case for skilled social engineering, having its roots in the framing operations. In the 60's, subversive/false messages and stories were sent to targeted individuals through direct letters, personal relations or newspapers. These days, an email, SMS or a message in VoIP platform is fast, secure and has a minimal cost for the social engineering planners. This also applies at a larger level, in the cyber influence campaigns. When the Soviet Union wanted to influence the perception of the Western public opinion, it used a chain mechanism by planting an idea in a peripheral Indian newspaper, that was then taken over by a European newspaper with socialist sympathies, and heavily cited by a Russian journal explaining what a strong argument the Western media had published. This chain is easily replicable today with the creation of fake websites and presentation of fabricated stories, that are further mentioned in community groups and rolled out on social network platforms until they reach the planned audience.

One particular point Pacepa described in its work is the "kernel of truth" that was mandatory for a strong framing operation. The social engineering attempts are also built on truth-based pillars, so the victim could perceive the framework as real, but misses the false part when taking a decision. The attacker would still have to know real people names from the organization, the website domain, locations, minimal procedures or flows, in order to successfully deliver the attack. Another tactic Pacepa learned from his KGB advisors to successfully deliver a deception was to let the target see part of the story with his or her own eyes, like documents or specific things. This would naturally strengthen the target's opinion and ease the influence process.

In social engineering, there are frequent attacks based on calls, but there are numerous emails where victims notice their bank logo, standard company messages or websites that look similar to the ones they usually visit – this part is a trigger to perform intended actions. It's like being influenced by TV stories that people are seeing with their own eyes: "I believe it, because I have seen it on television". This time it's "I believe it, because I received it on my work/personal email". Strong forgeries rely on the appearance of authentic documents and records; the better the imitation, the greater the results. Sometimes even specialists face issues in detecting skilled imitations.

Traditionally, disinformation departments had in their portfolio the collection of hundreds of thousands of letterhead stationery and signatures from Western and non-Communist leaders and politicians, private companies, newspapers, NGO's, etc. These assets were used at the right moment and the results were either delivered to targeted people like in a spear-phishing attempt or to wider audiences, through controlled media channels. Frequently, forged documents carried security classification to incite the receiver's interest and were sent through the mail with no return address (McCauley, 2016), like you would send an email to a target, with no real indications regarding the actual sender.

Nowadays, companies' logos, management boards and organizational charts can be found in seconds and can be easily used to create messages with an appearance of validity. As a rule, the basis of real facts ensures and empowers a highly effective disinformation process (Andrew & Mitrokhin, 1999), as the insiders of these KGB techniques revealed. During the communist regimes, state disinformation acquired a national amplitude; propaganda that is normally a distinct process identified itself with and metamorphosed to such an extent that it became an actual form of disinformation, while special deceptions were applied to support the propaganda strategy (Golitsyn, 1984). This is a historical development that explains, for example, the deeply embedded disinformation philosophy in current authoritarian state policies, in a manner that it become a natural and even legitimate tactic in the relation with foreign or national audiences.

As insiders of the communist intelligence system described (Ladislav Bittman, Deputy Director of the Disinformation Department within the Czechoslovak Intelligence Service), the Soviet intelligence activities were grouped in two main categories: 1. A "passive" information gathering phase about the strengths/weaknesses/plans/intentions of the targets and 2. Active measure activities, in its offensive understanding as a combination of core elements such as

disinformation, deception, sabotage, espionage, etc. (Bittman, 1985). One comparing the social engineering life cycle with the historical roots mentioned by the above-cited specialist, would remark the similarities of the process even after almost 60 years. For Bittman, the key for obtaining mastery in disinformation is that the creator should not believe in its own message, in the same way as Jacques Ellul previously considered about propaganda. The Czechoslovak specialist defined disinformation as a false message leaked into the adversary communication system to manipulate its decision makers or public opinion and detailed the three main components of the process:

1. **The Operator** – the entity that initiates and coordinates the operation, and will be its beneficiary;
2. **The Adversary** – the opponent entity, which could be a foreign state, its leadership or even individual citizens;
3. **The Unwitting Agent** – unaware of its role, he is a gameplayer exploited by the initiator as a means for the attack process. Personalities and press agencies fill this role in the disinformation campaigns.

I find strong similarities between the pillars of the traditional planned disinformation operations and modern social engineering activities. While the operator and the adversary entities remain the same, the only change intervened at the unwitting agent level, that has been replaced by the pretexting agent/entity using a technology layer (email/SMS/VoIP), easy to set up and totally under control. The old game plan described by Bittman underlined that the goal was to convince the adversary and the unwitting agent that each of them is the operator in the relation to each other. Nowadays, the social engineering game focuses on convincing the adversary that the pretexting agent/entity is the real initiator.

5. Conclusions

In the autumn of 1970, a large number of exiled people from Czechoslovakia (70.000 people) living mostly in different Western countries (United States, Great Britain, West Germany, Australia, Canada, a.o.) received letters signed by the "Legal Advisory Center" from their home country. They were ultimately required to pay an unclear amount of money (70-100 US$) as fee for a legal defense in a trial held in their absence, caused by their "illegal" stay abroad. Not paying would result in repercussions on their Czech or Slovak relatives. The goal was not only to inject in Czechoslovakia the requested money, but also to obtain information about the ones living abroad in terms of potential plans and procedures started with the foreign authorities to prolong their stay in those countries. Those details would have been later used against them as a blackmail, because the operation was initiated and coordinated by the Czechoslovak intelligence service, with the approval from the Communist Party (Bittman, 1972).

By the standards of the modern influence operations, this is maybe the most relevant example of an old-style phishing campaign, that used letters instead of emails, targeted a large number of people, and checked both goals of a current social engineering scheme: obtaining sensitive information and financial gains in the same time. It is the deceptive grandfather of today's modern attacks based on technology, creating in the minds of the victims the appearance of veracity and demand for actions that would be against their interest.

If we attempt to find an answer for the arch in time of this knowledge transfer, there is a potential explanation. There was a massive diffusion of deception and active measures know-how in the last decades, from the intelligence sector to the private sector. This happened mostly after the collapse of communism in the Soviet Union and the countries under its influence. Once the know-how was shared by specialists with other people, the second step was the "privatization of deception expertise", as people began to discover and learn new methods to quickly achieve objectives in a competitional free market. As a result, more and more individuals learned and applied tricks and tactics that once were mastered in a closed community.

With the rise of the social networking sites (SNS) the influence tactics could be easily applied to large audiences in foreign countries, the benefits surpassing clearly the minimal costs

involved. A strategy that took time and effort in the 60's to influence political elites and journalists by sending numerous personalized letters can be done in a fraction of the time needed before, under the umbrella of total anonymity. As Facebook clearly stated in a recent report on influence operations (Gleicher et al., 2021), the major trends characterizing them are:

1. Shifting from "wholesale" to "retail" IO (more targeted operations);

2. Public debates and manipulation often have blurred lines;

3. Perception hacking – inducing false perception over inexistent manipulation of strategic areas, like electoral systems;

4. IO as a service – influence operations services offered widely, commercially;

5. Increased operational security – improved capability to technically hide identity.

Social engineering has not reached its highest possible limit, because people remain the weakest link while the technology is evolving constantly. Even if organizations are more and more aware of the importance of cybersecurity, attacks also become more sophisticated, more targeted and more diverse. While email remains an important channel for phishing attacks, platforms used for entertainment and social activities are targeted with an increasing number of malicious links and attachments. The impact of social media platforms (and their corresponding risk vulnerability) will grow, as studies confirm that people are socially influenced in continuing using Facebook, through direct and side effects of both normative and informational social influence (Cristescu, 2017).

In recent cases of social engineering attacks on private companies, with damages amounting to several million USD, the courts ruled that the computer fraud and funds transfer fraud do not cover a frequent social engineering tactic – vendor impersonation (Sprague, 2021). This is an important signal that things are developing very fast and organizations/institutions should not just update their cybersecurity strategies, but actively train their employees to face such complex challenges.

In addition, with the development of AI and voice technology, attackers can now use algorithms and machine learning to impersonate previously studied high-level individuals in targeted organizations. Malicious actors could even interfere with the organization chatbots or pretend they are one in order to capture access credentials and sensitive data from customers that need professional support from their suppliers. We need to understand that Artificial Intelligence is working not only for the benefit of cybersecurity, but it could also be used in order to generate false content and messages in social engineering attacks, increasing the complexity of the defense tasks that professionals in this field have to solve.

REFERENCES

1. Abass, I. A. M. (2018). *Social Engineering Threat and Defense: A Literature Survey*. Journal of Information Security, 9, 257-264. https://doi.org/10.4236/jis.2018.94018.

2. Allen, M. (2006). *Social Engineering: A Means To Violate A Computer System*. Sans Institute White Paper.

3. Alsufyani, A. A., Alhathally, L. A., Al Amri, B. O. & Alzahrani, S. M. (2020). *Social Engineering, New Era of Stealth and Fraud Common Attack Techniques and How to Prevent Against*. International Journal of Scientific & Technology Research, Volume 9, Issue 10.

4. Alyoubi, B. A. & Alyoubi, A. A. (2013). *Importance of Social Engineering in Community Knowledge*. The International Journal of Soft Computing and Software Engineering [JSCSE], San Francisco State University, CA, U.S.A., Vol. 3, No. 3, Special Issue, 295-300: https://Doi:10.7321/jscse.v3.n3.44.

5. Andrew, C. & Mitrokhin, V. (1999). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York: Basic Books.

6. Barber, T. (2016). *Russia's dark art of disinformation. Fancy Bear and Cozy Bear are examples of a rich tradition of subversion*. https://www.ft.com/content/d8495c86-7b47-11e6-b837-eb4b4333ee43.

7. Breda F., Barbosa H. & Morais T. (2017). *Social Engineering and Cyber Security*. International Technology, Education and Development Conference. March 2017. Doi: 10.21125/inted.2017.1008.

8. Bittman, L. (1972). *The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare*. Syracuse: Syracuse University Research Corporation.

9. Bittman, L. (1985). *The KGB and Soviet Disinformation: An Insider's View*. Washington: Pergamon-Brassey's.

10. Castells, M. [1996] (2009). *The Rise of the Network Society*. Information Age: Economy, Society, and Culture. Volume 1. Oxford: Wiley-Blackwell.

11. Chelcea, S. (2006). *Opinia Publică. Strategii de persuasiune si manipulare*. București: Editura Economică.

12. Cialdini, R. B. [1984] (2007). *Influence. The Psychology of Persuasion*. New York: Harper Collins Publishers.

13. Cole, E., Ring, S. (2006). *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*. Rockland: Syngress Publishing, Inc.

14. Cristescu, I. (2017*). Rolul influenţei sociale în acceptarea Facebook: testarea unui model TAM extins*. Revista Română de Informatică 46 şi Automatică, vol. 27, nr. 3, pp. 37-46. https://rria.ici.ro/art-04-vol-27-nr-3-2017/.

15. Dahl, R. A. (1957). *The Concept of Power*. Systems Research and Behavioral Science 2(3), 201–215.

16. Elinschi-Ciupercă, E. (2003). *Influența Socială*. In Chelcea, S. & Iluţ, P. (coord.). Enciclopedie de psihosociologie, pp. 185-186. Bucureşti. Editura Economică.

17. ENISA (2021). *What is "Social Engineering"?* https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering.

18. Erbschloe, M. (2020). *Social Engineering Hacking Systems, Nations, and Societies*. Boca Raton: CRC Press, Taylor & Francis Group.

19. Gleicher, N., Franklin, M., Agranovich, D., Nimmo, B., Belogolova, O. & Torrey, M. (2021). *Facebook Threat Report. The State of Influence Operations 2017-2020*. https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf .

20. Ghafir, I., Prenosil, V., Alhejailan, A. & Hammoudeh, M. (2016). *Social engineering attack strategies and defence approaches*. In: IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016), 22 August 2016 - 24 August 2016, Vienna, Austria. DOI: https://doi.org/10.1109/FiCloud.2016.28.

21. Golitsyn, A. (1984). *New Lies for Old.* The Communist Strategy of Deception and Disinformation. London: Bodley Head.

22. Greenberg, A. (2021). *Facebook Catches Iranian Spies Catfishing US Military Targets*. https://www.wired.com/story/facebook-iran-espionage-catfishing-us-military/.

23. Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Indianapolis, Indiana: Wiley Publishing, Inc.

24. Hatfield, J. M. (2017). *Social engineering in cybersecurity: the evolution of a concept*. Computers & Security, Vol. 73, 102-113. https://doi.org/doi:10.1016/j.cose.2017.10.008.

25. Krombholz, K., Hobel, H., Huber, M. & Weippl. E. (2004). *Advanced social engineering attacks*. Journal of Information Security and Applications. Volume 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

26. Kumar, A., Chaudhary, M. & Kumar, N. (2015). *Social Engineering Threats and Awareness: A Survey*. European Journal of Advances in Engineering and Technology, 2015, 2(11): 15-19.

27. Lohani, S. (2019). *Social Engineering: Hacking into Humans*. International Journal of Advanced Studies of Scientific Research. Vol. 4, No. 1: https://ssrn.com/abstract=3329391.

28. Luo, X., Brody, R., Seazzu, A., Burd., S. (2011). *Social Engineering: The Neglected Human Factor for Information Security Management*. Information Resources Management Journal, 24(3), 1-8. DOI: 10.4018/irmj.2011070101.

29. Mann, I. (2008). *Hacking the human: social engineering techniques and security countermeasures*. Hampshire, England: Gower Publishing, Ltd.

30. McCauley, K. N. (2016). *Russian Influence Campaigns against the West: From the Cold War to Putin*. North Charleston: CreateSpace Independent Publishing Platform.

31. Mercer, W., Rascagneres, P. & An, J. (2019). *How Tortoiseshell created a fake veteran hiring website to host malware*. https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html.

32. Mitnick, K. D. & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, Indiana: Wiley Publishing.

33. Mucchielli A. (2000). *L'art d'influencer: analyse des techniques de manipulation*. Paris: A. Colin.

34. Nance, M. (2018). *The plot to destroy democracy. How Putin and his spies are undermining America and dismantling the West*. New York: Hachette Books.

35. Ozkaya, E. (2018). *Learn Social Engineering. Learn the art of human hacking with an internationally renowned expert*. Birmingham: Packt Publishng Ltd.

36. Pacepa, I. M. & Rychlak, R. J. (2013). *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. Washington, DC: WND Books.

37. Pamment, J., Nothhaft, H., Agardh-Twetman, H. & Fjällhed, A. (2018). *Countering Information Influence Activities: The State of the Art*. Department of Strategic Communication, Lund University.

38. Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies. Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Birmingham: Packt Publishing.

39. Reynolds, V. (2015). *Social Engineering. The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception*. Createspace Independent Pub.

40. Rubenstein, J. & Gribanov, A., eds. (2015). *The KGB File of Andrei Sakharov*. New Haven & London: Yale University Press.

41. Sprague, N. (2021). *The future of social engineering*. https://www.willistowerswatson.com/en-CA/Insights/2021/04/the-future-of-social-engineering.

42. Yasin, A., Fatima, R., Liu., L, Yasin, A. & Wang., J. (2019). *Contemplating social engineering studies and attack scenarios: A review study*. Security Privacy. Volume 2, Issue 4. https://doi.org/10.1002/spy2.73.

43. Wang, Z., Zhu, H. & Sun, L. (2020). *Defining Social Engineering in Cybersecurity*. IEEE Access, vol. 8, 85094-85115, 2020. doi: 10.1109/ACCESS.2020.2992807.

44. Wang, Z., Zhu, H. & Sun, L. (2021). *Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods*. In IEEE Access, vol. 9, 11895-11910, 2021. doi: 10.1109/ACCESS.2021.3051633.

45. Watson, G., Mason, A. & Ackroyd, R. (2014). *Social engineering penetration testing: executing social engineering pen tests, assessments and defense*. Waltham, MA: Syngress.

Aurelian STOICA holds a Ph.D. in Sociology and he is a Cybersecurity Consultant with extensive experience in managing complex technology projects in different markets (Europe, North America, Middle East and North Africa). He has more than 20 years of professional experience in IT&C companies and organizations, such as Orange Romania, Huawei Technologies, S&T Romania, SIVECO Romania, MRM//Commerce, National Institute for Research and Development in Informatics.

Aurelian STOICA este doctor în sociologie și consultant în domeniul securității cibernetice, cu o vastă experiență în gestionarea de proiecte complexe de tehnologie în diferite piețe (Europa, America de Nord, Orientul Mijlociu și Africa de Nord). Are o experiență profesională de peste 20 de ani în companii și organizații IT&C, precum Orange România, Huawei Technologies, S&T România, SIVECO România, MRM // Commerce, Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București.