Exploiting personality traits in social engineering attacks

Irina CRISTESCU, Ella Magdalena CIUPERCĂ, Carmen Elena CÎRNU

National Institute for Research and Development in Informatics – ICI Bucharest

irina.cristescu@ici.ro, ella.ciuperca@ici.ro, carmen.cirnu@ici.ro

Abstract: Phishing attacks have become more sophisticated over time, more than any other forms of social engineering attacks, exploiting the end users' vulnerabilities and weaknesses. This article reviews the literature regarding the connection between three personality models – Five Factor Model, Myers-Briggs Type Indicator and Dark Triad – and how they can be linked with the susceptibility of individuals to become targets of social engineering attacks. Thus, the focus on evaluating human vulnerabilities in the context of cyber security by identifying both the factors that influence the susceptibility to cyber-attacks, and the human characteristics/traits that can be exploited as a vulnerability in the context of cyber security attacks.

Cuvinte cheie: Social engineering, cyber security, Five Factor Model, Myers-Briggs Type Indicator, Dark Triad Personality Model.

Rolul trăsăturilor de personalitate în atacurile de inginerie socială

Rezumat: Atacurile de tip phishing s-au sofisticat de-a lungul timpului, mai mult decât orice alte forme de atac de inginerie socială, exploatând vulnerabilitățile și punctele slabe ale utilizatorilor finali. Prezentul articol evidențiază legătura dintre trei modele de personalitate – Modelul Big Five, Modelul Myers-Briggs și Modelul Dark Triad – și susceptibilitatea indivizilor de a deveni ținte ale atacurilor de inginerie socială. Scopul acestui articol este de a sublinia importanța evaluării vulnerabilităților umane în contextul securității cibernetice prin identificarea atât a factorilor care influențează susceptibilitatea la atacuri cibernetice, cât și a caracteristicilor/trăsăturilor individuale care pot fi exploatate ca vulnerabilitate în contextul atacurilor cibernetice.

Cuvinte cheie: Social engineering, securitate cibernetică, modelul Big Five al personalității, modelul Myers-Briggs, modelul Dark Triad.

1. Introduction

In the context of a great diversity of goals and motivations that determine the manifestation of cyber threats, it becomes more difficult to know, prevent and counteract a cyber attack as the profile of cyber aggressors usually involves a higher technological level than the attacked systems (Vevera, 2018).

Nowadays, cyber-attacks target individuals by exploiting the weaknesses of end users. The human factor and its vulnerabilities represent a critical threat to the security of computer data. Though technologies have been developed to detect and identify social engineering attacks (such as phishing, for example), attackers find new ways of exploiting the human limitations and biases and persuade people to respond as they had intended (ex.: spear phishing).

Research has addressed these issues and explored how individual differences in personality traits could be linked to being susceptible to several strategies and end-users vulnerabilities. Thus, several scales have been developed in order to examine the human factors that influence the security behavior, to identify the degree to which a person is likely to become an accidental inside threat or how certain personality traits make the individual susceptible to different social engineering attacks.

The aim of this article is to underline the importance of evaluating the human vulnerabilities in the context of cyber security and to offer an initial review of the existing literature on:

- Factors that influence the susceptibility to cyber-attacks such as social engineering;
- Human traits that can be exploited as a vulnerability in the context of cyber security-attacks.

https://doi.org/10.33436/v32i1y202209

Therefore, we focused on analysing how three personality traits models (Five-Factor Model, Myers-Briggs Type Indicator and Dark Triad Model) may be used to better understand human factors in cyber-attacks.

2. Social engineering (SE)

Social engineering in the online environment describes a type of attack in which human vulnerabilities are exploited in order to obtain classified information, unauthorized access to restricted areas or to violate the security objectives (confidentiality, integrity, availability, controllability) of cyber elements such as infrastructure, data and resources. Therefore, social engineering is a type of cyber-attack in which the attacker exploits human vulnerability through social interaction to violate cybersecurity (Wang, Sun & Zhu, 2020).

Compared to classic attacks such as password cracking and software vulnerabilities, social engineering attacks focus on exploiting vulnerabilities from a human perspective to bypass security barriers. In some cases, social engineering attacks may be limited to making a phone call and falsely assuming the identity of a known person in order to obtain classified information. Social engineering takes place with or without the use of technical means and vulnerabilities. Human vulnerabilities refer to human factors that are exploited by attackers to carry out a social engineering attack. These human vulnerabilities can be psychological or cognitive, related to behavioral habits or neural networks.

With the development of new technologies and new cyber environments, the incidence of social engineering increases. Social networks, mobile communications, Internet of Things (IoT) generate not only large amounts of information, but also many channels of attack.

Specific targets are carefully selected to create credible and targeted social engineering attacks. Technologies such as machine learning and artificial intelligence can make social engineering attacks more effective and aggressive and targeted, large-scale, automated and advanced social engineering attacks become possible (Wang, Sun & Zhu, 2020) as a large group of victims can be contacted at the same time and some open source tools can be used to launch semi-automatic attacks.

Communication or joint activity involving two or more human roles are used to attain the goals of social engineering. According to different criteria, the types of social interaction can be: direct (real-world interaction) or indirect (online interaction), real-time (talking on the phone) or non-real-time (e-mail), active or passive (e.g., reverse social engineering) (Wang, Sun & Zhu, 2020).

Some of the reasons why people tend to be more susceptible to social engineering attacks are related to the natural biases of any individual: false memories, a difficulty in concentrating for a long time or in a different stimulus environment, the natural tendency to trust and help others (Conteh & Royer, 2016).

Recent research has shown that credentials' theft and social engineering attacks are responsible for 70%, respectively 22% of data breaches, while the social engineering attacks launched via email (phishing) ranked first in line among other 16 more common attacks related to data breaches (Nathan & Scobell, 2020). The results of social engineering attacks may be disastrous not only at organizational level, but also for personal reputation or the finances of regular individuals and all these implications are reasons to address these types of attacks appropriately.

3. Human factor in cyber security attacks

The psychosociological assessment of human factor plays an important role to ensure complete cyber security solutions. Starting from this premise, we approached three of the most known personality model to highlight the most susceptible traits to be used in cyber security attacks.

3.1. Theoretical background: personality traits

Personality traits are responsible for the way in which individuals think, feel and behave (Funder, 2001). Behavioral patterns are shaped by different factors such as genetics, individual life experiences, the pressure of different contexts. If you know which of them can be exploited by attackers and the way they can do this, security policy may use some very strong indicators of the involvement in malicious actions or engagement in risky activitites to prevent attacks (Zhang, 2006; Nurse et al., 2014) and identify in real time security-related behavior issues (Gratian et al., 2018).

During the 1930s, Gordon Allport and Henry S. Odbert were the first researchers to study the concept of personality trait (John & Srivastava, 1999 apud Feist & Feist, 2006). In their view, personality is an intrinsic element pertaining to any human individual. It has a dynamic manifestation and it is an organized model of mental and physical functions, of elements that interact with each other and motivate the behavior of each individual. Ten years later, the study of personality traits was continued by Raymond Cattell (ibid.). In Cattell's view, personality traits are the foundation of any personality. These are a series of trends that remain relatively unchanged throughout life determining how the human individual reacts to the events he experiences.

Another pioneer in the study of personality traits is Louis Leon Thurstone (Zlate, 2004) who identified a total of seven factors through which it would be possible to explain an individual's personality.

3.1.1. Big Five Model (FFM)

The purpose of this model was to identify the main personality traits that are valid for each individual and also to demonstrate their persistence over time considering Eisenck super-traits : introversion, extraversion and neuroticism (Mihai, 2019).

The Big Five or The Five Factor Model (FFM) includes five distinct personality traits found to be unalterable across age and culture groups, and consistent through time (Erder & Purer, 2016). The Five-Factor Model measures the following personality traits using the Big Five Inventory (BFI), which consists of 50 questions (John and Srivastava, 1999; McCrae & Costa, 2008):

- *Openness:* the willingness to try new experiences. People with higher levels of openness are more likely to appreciate art, have an increased imagination and are more eager for adventure. Those who score low levels of openness are comfortable with their routine and do not seek new experiences;
- *Conscientiousness:* people with high conscientiousness levels are more goal-oriented, set ambitious goals, are motivated to achieve them, and exhibit strong-self orientation and self-responsibility;
- *Extraversion:* people who score high on this trait are outgoing and characterised by socially confident behaviour, feel comfortable in large group of people, are enthusiastic, energetic, and talkative. Those scoring low on this trait display a contrasting behaviour, such as: shyness around people and being intimidated by large groups;
- *Agreeableness:* people scoring high on this trait are cooperative and friendly, while people scoring low on this trait are less concerned with pleasing others, being more suspicious of other people’s intentions and less charitable;
- *Neuroticism:* this trait is measured on a continuum ranging from emotional stability to emotional instability. People who score high on this trait feel anxious, while low scores on this trait indicate emotional stability.

Each personality trait can be understand as an indicator of cyber-security-related behavior intentions of users regarding their computer devices. For exemple, Frauenstein & Flowerday (2020) have shown that certain personality traits, like agreeableness, can be statistically linked to victimization. The same study shows that neuroticism is associated with computer anxiety, thus people with this personality trait may be more concerned about their security and privacy (security worries), which may decrease susceptibility to social engineering attacks, like phishing.

3.1.2. Myers-Briggs Type Indicator (MBTI)

The Myers-Briggs Type Indicator (MBTI) model of personality (Myers, McCaulley, Quenk & Hammer, 2018) has the advantage of being a widely used instrument (Furnham, 2017) due to its insightful information regarding the personality-based guidelines as it is focused on four areas of personality type and their dynamic combination: Extraversion / Introversion, Sensing / Intuition, Thinking / Feeling and Judging / Perceiving.

Thus, people differ in the way they prefer to focus their attention (extroverts/introverts), the way they gather information (sensing/intuition), the way they come to decisions or make judgments (thinking/feeling), and the way they choose to live their lives (judging/perceiving) (Cullen & Armitage, 2018).

According to Isabel Briggs Myers in Papatsaroucha et al. (2021), extroverts focus on the external environment, while introverts are more concerned with the inner world. Sensing people tend to gather information through their senses and focus on what is real, whereas people driven by intuition in information gathering prefer to trust their instincts (Cullen &Armitage, 2018).

Regarding decision making and judgment, people who rely on thinking are more objective and use logic for drawing conclusions, while people who rely on feeling judge under the guidance of their emotions, but also they show an increased level of empathy. In the same line, their lifestyle can either be well planned and organized if the person is a rational one, or it can be more open to possibilities like the perceiving trait dictates (Cullen & Armitage, 2018).

3.1.3. Dark Triad

The "Dark Triad" model of personality traits includs machiavellianism, narcissism, and psychopathy (Paulhus & Williams, 2002), and has been researched with regard to interpersonal manipulation and deception taking into consideration different contexts (Jonason & Webster, 2012).

Machiavellianism is associated with manipulative behavior that targets personal gain through strategic deception and flexible moral tactics (Bereczkei, 2015).

Narcissism is linked to interpersonal dominance, entitlement, and the willingness to exploit others (McHoskey, 1995).

Psychopathy mainly denotes the lack of empathy and tendencies for uncontrolled behaviour and emotions (Book et al., 2015; Azizli et al., 2016; Williams, Paulhus & Hare, 2007).

The traits included in the Dark triad model of personality can be assessed using the Dirty Dozen inventary (Jonason & Webster, 2010) and the Short Dark Triad inventory (SD3; Jones & Paulhus, 2014).

While the previous two models are able to give hints regarding either the victim of an cyberattack and an attacker, the Dark Triad is more appropriate for the assessment of the hacker's personality. All three characteristics are indicators of behaviors that can be successful in social engineering. Social engineering attackers need a high manipulation ability, the willingness to exploit others and lack of empathy.

To be cautious, organizations may apply the tests that reveal such personality traits of employees in order to guard themselves against individuals that may be exhibit such behaviors.

3.2. Personality traits and social engeneering attacks

Investigating the user's weaknesses and vulnerabilities that facilitate the success of social engineering attacks is critical when preventing and protecting against these kind of threats.

Alseadoon et al. (2015) and Halevi et al. (2013) were interested in sociopsychological characteristics such as demographics, trust, and email experience in order to predict the individual detection ability for email phising. Other studies (Imaji, 2019, Salahdine & Kaabouch, 2019, Tandon & Nayyar, 2019) have focused on increasing the awareness of the success of these type of attacks by studying the taxonomy of social engineering attacks.

3.2.1. The Five-Factor Model of Personality and social engineering

An important part of the subject of cyber security tackles the relationship between the personality traits and cyber-attacks. In this context, social engineering plays a special role. For example, Alseadoon et al. (2015) and Halevi et al. (2013) investigated the impact of personality traits on email phising responses.

Halevi et al. (2013) underlined that neuroticism is the most important trait that correlates to phishing email responses, while, Alseadoon et al. (2015) has shown that openness, extraversion, and agreeableness increase user tendency to comply with phishing email requests.

In order to identify the factors that influence people's vulnerability to Facebook phishing attacks, Vishwanath (2015) found that desire to increase friendship connections and the frequency of network usage have a high impact on user behavior. For example, this might lead to individuals automatically accepting friend requests and enacting without conscious reflection, thus exposing themselves to possible threats, or social engineering attacks.

Saridakis et al. (2016) focused on related factors and has shown that individuals with high-risk attitudes are more likely to fall victim to cyber-attacks.

Uebelacker and Quiel (2015) assumed the following associations between certain persuasion principles and personality traits:

- *Extraversion* increases susceptibility to liking, and social proof, due to its association with sociability;
- *Conscientiousness* increases susceptibility to authority, commitment/consistency and reciprocity;
- *High levels of the agreeableness* correlate with the tendency to trust others and increase vulnerability towards social engineering as they are more vulnerable to persuasion, authority and more interested in having social validation, reciprocity and liking;
- *Openness* is associated with increased vulnerability towards social engineering tactics being highly correlated with computer proficiency, which leads to an increase in susceptibility;
- *Neuroticism* is linked to computer anxiety, which in turn decreases susceptibility. Individuals scoring high on this trait may be vulnerable towards the authority principle due to their tendency to comply with instructions and commands from authorities.

3.2.2. Myers-Briggs Type Indicator Theory and social engineering

ESET and The Myers-Briggs Company (2020) partnered up to explore both the role of employees in keeping organisations safe from online threats underlining the link between the personality type and vulnerabilities to cybercrime by publishing Cyberchology: the human element. The study proved that different kinds of cyber security errors are more common among people with certain personality preferences:

- *Extroverted* individuals are more likely to be vulnerable to social engineering attacks as they are more susceptible to manipulation, persuasion and deceit.
- *Sensing* individuals are more likely to spot phishing attacks when compared to *Intuitive* people, but they are both vulnerable to cyber security risks especially when they have a tendence for *Perceiving* or *Extraversion*.
- *Feeling* individuals (centred on their personal values) and *Judging* ones (structured, systematic individuals) are more likely to be vulnerable to social engineering attacks than the *Thinking* personalities (who have tendency for reasoning).

From Myers-Briggs Type Indicator Theory perspective, most of the personality types have different strengths and blindspots that can impact the outcome of a cyber security attack, which should be investigated and considered in order to build a coherent, integrative cyber security programme.

3.2.3. The Dark Triad Model of Personality and social engineering

The Dark Triad Model of Personality refers to a combination of characteristics that lead to shaping a personality associated with a callous-manipulative interpersonal style:

- Narcissism characterized by pride, egotism, non-empathy;
- Machiavellianism characterized by the tendency to manipulate others, lack of morality and a higher level of self-interest;
- Psychopathy characterized by antisocial behavior, impulsivity, selfishness.

Even though Narcissism is also associated with overconfidence (Campbell, Goodie & Foster, 2004) and functional impulsivity (Jones & Paulhus, 2011), these individuals act quickly considering that they can manage new situations, when in fact they act because of an unrealistic sense of optimism and invulnerability (Farwell & Wohlwend-Lloyd, 1998).

Individuals that score high in Psychopathy have little attention for the details because of their impulsive nature (Curtis et al., 2018). Thus, they tend to create emails that do not imply a proactive effort and minimal changes between emails and it is improbable to invest effort in structuring a phishing email. More likely, such individuals are victims rather than hackers (Curtis et al., 2018).

In contrast, high scores in Machiavellianism are associated with carefully planing the next move (Czibor & Bereczkei, 2012) and strategy calibration based on the audience (Esperger & Bereczkei, 2012).

Therefore, the benefits of studying the Dark Triad traits in relation with cybersecurity reside in predicting the amount of effort an individual puts into crafting a phising email (Curtis et al., 2018) revealing that Dark Tryad Model portray more probable the personality of a hacker, while The Five-Factor Model and Myers-Briggs Type Indicator Theory suggest the main traits of the victim of cyber-attacks sinces the more the personality traits that were mentioned earlier are present in high levels, the more likely is a person to fall victim to social engineering attacks.

Further, we summarized the personality traits pertaining to each model and the occurence for social engineering attacks to appear.

Table 1. Personality traits that lead to SE attacks

Personality traits	Personalities traits models	Victim of social engineering attacks	Hackers in social engineering attacks
High Openness	FFM	✓	
High Conscientiousness	FFM	✓	
High Extraversion	FFM, MBTI	✓	
High Agreeableness	FFM	✓	
High Neuroticism	FFM	✓	
High Sensing	MBTI	✓	
High Perceiving	MBTI	✓	
High Feeling	MBTI	✓	
High Judging	MBTI	✓	
High Narcissism	DT		✓
High Psychopathy	DT		✓

4. Conclusions

Designing a security system that is able to prevent or stop a variety of attacks before causing damage must keep pace with an increasingly complex and developed attack technology in order to immediately increase, for example, the level of confidence in online systems (Marinescu, Nicolau, Băjenaru, 2016).

The intense use of social media alongside the trusting human nature are a useful combination for social engineering attackers and, lately, when dealing with malicious actors, the focus has been changed to exploting human vulnerabilities by using different social engineering strategies. Therefore, the number of studies regarding personality factors connected to cybersecurity is growing.

Moreover, as the current pandemic context led to remote working, the monitoring process of the security conditions of the work/office environment became more complex and difficult, thus contributing to the expansion of the intrusion points that can be exploited by the cybercriminals.

The literature on information technology and cyber security has focused on phishing studies with the aim of discovering what affects susceptibility to cyber-attacks and what shapes human vulnerability. Understanding the types of vulnerabilities and the traits that make individuals more susceptible to cyber-attacks is a critical step to controlling security vulnerabilities. Thus, a clear understanding of the strategies and patterns used by social engineering attackers are essential to minimizing the risks that social engineering attacks present not only to individuals, but also in the business sector and government.

Moreover, exploring, researching and identifying the human vulnerabilities offers the posibility to implement training programs that lead to distinguishing phishing and ham emails (Curtis et al., 2018). This kind of approach not only makes people aware of their strenghts and blind spots, but also helps to improve the IT security behavior of individuals and organizations.

Thus, the importance of offering people the posibility to be educated to protect themselves in cyberspace, recognizing potential threats, and confronting them is starting from the acknowledgement of each vulnerability and strength. This kind of approach benefits both the systems and data of organizations and industries and also personal privacy.

Acknowledgment

This work was funded from the project "Cybernetic polygon for industrial control systems (ROCYRAN)" ("Poligon cibernetic pentru sisteme de control industrial (ROCYRAN)").

REFERENCES

1. Alseadoon, M. F. I., Othman & T. Chan (2015). *What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?* In Advanced Computer and Communication Engineering Technology, Springer International Publishing, 949–962.
2. Azizli, N., Atkinson, B. E., Baughman, H. M., Chin, K., Vernon, P. A., Harris, E., Veselka, L. (2016). *Lies and crimes: Dark Triad, misconduct, and high-stakes deception*. Personality and Individual Differences, 89, 34–39.
3. Bereczkei, T. (2015). *The manipulative skill: Cognitive devices and their neural correlates underlying Machiavellian's decision making*. Brain and Cognition, 99, 24–31.
4. Book, A., Methot, T., Gauthier, N., Hosker-Field, A., Forth, A., Quinsey, V., Molnar, D. (2015). *The mask of sanity revisited: Psychopathic traits and affective mimicry*. Evolutionary Psychological Science, 1(2), 91–102.
5. Campbell, W. K., Goodie, A. S. & Foster, J. D. (2004). *Narcissism, confidence, and risk attitude*. Journal of Behavioral Decision Making, 17(4), 297–311.
6. Conteh, N.Y. & Royer, M. D. (2016). *The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor*. International Journal of Computer. 20, 1 (2016), 1–12.
7. Cullen, A. & Armitage, L. (2018). *A Human Vulnerability Assessment Methodology*. In 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), IEEE, 1–2.

8. Curtis, S. R., Rajivan, P., Jones, D. N. & Gonzales, C. (2018). *Phishing attempts among the dark triad: Patterns of attack and vulnerability*. Computers in Human Behavior, 87, 174-182.

9. Engler, B. (2014). *Personality Theories. An Introduction.* Wadsworth: Cengage Learning.

10. Erder, M. & Pureur, P. (2016). *Role of the Architect*. Continuous Architecture, 187–213.

11. Esperger, Z. & Bereczkei, T. (2012). *Machiavellianism and spontaneous mentalization: One step ahead of others*. European Journal of Personality, 26(6), 580–587.

12. Farwell, L. & Wohlwend-Lloyd, R. (1998). *Narcissistic processes: Optimistic expectations, favorable self-evaluations, and self-enhancing attributions*. Journal of Personality, 66(1), 65–83.

13. Feist, J. & Feist, G. (2006). *Theories of Personality.* New York: The McGraw-Hill Companies, Inc.

14. Frauenstein, E. D. & Flowerday, S. (2020). *Susceptibility to phishing on social network sites: A personality information processing model.* Computers & Security, 101862.

15. Funder, D.C. (2001). *Personality*. Annual Review of Psychology, 52, 1, 197–221.

16. Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). *Correlating human traits and cyber security behavior intentions*. Computers & Security, 73, 345–358.

17. Halevi, T., Lewis, J., Memon, N. (2013). *Phishing, Personality Traits and Facebook*, arXiv:1301.7643.

18. Imaji, A. (2019). *Ransomware Attacks: Critical Analysis, Threats, and Prevention methods*, https://www.researchgate.net/publication/332551447_Ransomware_Attacks_Critical_Analysis_Threats_and_Prevention_methods.

19. John, O. P. & Srivastava, S. (1999). *The Big Five trait taxonomy: History, measurement, and theoretical perspectives*. Handbook of personality: Theory and research, 2, 102–138.

20. Jonason, P. K. & Webster, G. D. (2010). *The dirty dozen: A concise measure of the dark triad*. Psychological Assessment, 22(2), 420–432.

21. Jonason, P. K. & Webster, G. D. (2012). *A protean approach to social influence: Dark Triad personalities and social influence tactics*. Personality and Individual Differences, 52(4), 521–526.

22. Jones, D. N. & Paulhus, D. L. (2011). *The role of impulsivity in the Dark Triad of personality*. Personality and Individual Differences, 51(5), 679–682.

23. Jones, D. N. & Paulhus, D. L. (2014). *Introducing the short dark triad (SD3) a brief measure of dark personality traits*. Assessment, 21(1), 28–41.

24. Marinescu, I., Nicolau, D., Băjenaru, L. (2016). *Consideraţii asupra atacurilor cibernetice, executate în contextul comunicaţiilor prin reţea.* Revista Română de Informatică şi Automatică, 26(4), 17-28.

25. McCrae, R. R. & Costa, P. T., Jr. (2008). *The Five-Factor Theory of personality*. In O. P. John, R. W. Robins, & L. A. Pervin (Eds.), Handbook of personality: Theory and research (3rd ed., pp. 159-181). New York: Guilford.

26. McHoskey, J. (1995). *Narcissism and machiavellianism.* Psychological Reports, 77(3), 755–759.

27. Mihai, R. (2019). *Perspectiva trăsăturilor: modelul Big Five*. Retrieved from Lumen in mundo: https://lumeninmundo.com/2019/10/10/perspectiva-trasaturilor-modelul-big-five/.

28. Myers, I. B., McCaulley, M. H., Quenk, N. L. & Hammer, A. L. (2018). *MBTI Manual for the Global Step I and Step II Assessments* (4th ed.). Sunnyvale: The Myers-Briggs Company.

29. Nathan, A. J. & Scobell, A. (2020). *2020 Data Breach Investigations Report*. https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf.

30. Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T. & Whitty, M. (2014). *Understanding insider threat: A framework for characterizing attacks*. In 2014 IEEE Security and Privacy Workshops, IEEE, pp. 214–228.

31. Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., Pallis, E., Markakis, E. K. (2021). *A Survey on Human and Personality Vulnerability Assessment in Cybersecurity: Challenges, Approaches, and Open Issues*. Retrieved from: https://arxiv.org/ftp/arxiv/papers/2106/2106.09986.pdf.

32. Paulhus, D. L. & Williams, K. M. (2002). *The dark triad of personality: Narcissism, Machiavellianism, and psychopathy*. Journal of Research in Personality, 36(6), 556–563.

33. Salahdine, F., Kaabouch, N. (2019). *Social Engineering Attacks: A Survey*. Future Internet, 11(4), 89.

34. Saridakis, G., Benson, V., Ezingeard, J. N. & Tennakoon, H. (2016). *Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users*, Technological Forecasting and Social Change, vol. 102, 320–330.

35. Tandon, A. & Nayyar, A. (2019). *A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat*. Springer, City.

36. Uebelacker, S. & Quiel, S. (2014). *The Social Engineering Personality Framework*. In *2014* Workshop on Socio-Technical Aspects in Security and Trust, IEEE, pp. 24–30.

37. Vevera, A. V. (2018). *De la amenințarea cibernetică la acțiunea ostilă în spațiul cibernetic.* Romanian Journal of Information Technology and Automatic Control, 28(3), 17-30.

38. Vishwanath, A. (2015). *Habitual Facebook use and its impact on getting deceived on social media*. Journal of Computer-Mediated Communication, vol. 20, no. 1, 83–98.

39. Williams, K. M., Paulhus, D. L. & Hare, R. D. (2007). *Capturing the four-factor structure of psychopathy in college students via self-report*. Journal of Personality Assessment, 88(2), 205–219.

40. Zhang, L. F. (2006). *Thinking styles and the big five personality traits revisited*. Personality and Individual Differences, 40, 6, 1177–1187.

41. Zlate, M. (2004). *Eul și personalitatea*. București: Editura Trei.

Irina CRISTESCU is a scientific researcher in the *Protection of Critical Infrastructure Department* at the National Institute for Research and Development in Informatics – ICI Bucharest. She received the PhD degree in Sociology from the University of Bucharest in 2011. She is involved in the development of research and projects in the field of cyber security, non-invasive monitoring applications for elderly (using sets of extensible technologies, smart devices), technology acceptance, and advanced statistical methods.

Irina CRISTESCU este cercetător științific în cadrul Serviciului Protecție Infrastructuri Critice din cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. A obținut titlul de doctor în Sociologie de la Universitatea din București în 2011. Este implicată în

dezvoltarea de cercetări și proiecte în domeniul securității cibernetice, aplicații de monitorizare non-invazivă pentru vârstnici (folosind seturi de tehnologii extensibile, dispozitive inteligente), acceptarea tehnologiei și metode statistice avansate.

Ella Magdalena CIUPERCĂ is the Head of Critical Infrastructure Service of ICI Bucharest being specialized in security studies, sociology and social psychology (especially the study of innovation and social change). She defended her PhD in sociology at Bucharest University in 2004. In the last 20 years, she held different management positions in higher education (as a department director, director of Doctoral School and Faculty Dean). Over the last years, she has been a project director and member of different research teams for international and national projects. Also, she published more than 50 books and articles.

Ella Magdalena CIUPERCĂ este Șefa Serviciului Protecția Infrastructurilor Critice al ICI București fiind specializată în studii de securitate, sociologie și psihologie socială. Și-a susținut doctoratul în sociologie la Universitatea București în 2004, iar in ultimii 25 de ani a ocupat diferite funcții de conducere în învățământul superior și în cercetare (ca director de departament, decan, director școală doctorală). A fost director de proiect și membru a diferitelor echipe de cercetare pentru proiecte internaționale și naționale și a publicat peste 50 de cărți și articole.

Carmen Elena CÎRNU graduated from the University of Bucharest, Faculty of Philosophy in 2003, and obtained her PhD in 2011. Currently, she is a Senior Scientific Researcher II and Scientific Director of the National Institute for Research and Development in Informatics - ICI Bucharest, where she is involved in the development of research and development projects in the field of interoperability, cybersecurity and e-government. She has collaborated with universities and central public administration institutions over the years. In 2015 she was a Guest Researcher at the Global Security Research Institute at Keio University (Japan). She is the author or co-author of numerous articles, studies, and research reports.

Carmen Elena CÎRNU este Director Științific al Institutului Național de Cercetare-Dezvoltare în Informatică - ICI București și cercetător științific II. Este implicată în derularea de proiecte de cercetare și dezvoltare în domeniul interoperabilității, securității cibernetice și guvernării electronice. De-a lungul anilor, a colaborat cu universități și instituții ale administrației publice centrale. În 2015, a fost cercetător invitat la Institutul de Cercetare în Securitate Globală de la Universitatea Keio (Japonia). Ea este autoarea sau coautoare a numeroase articole, studii și rapoarte de cercetare.