BI Norwegian Business School - campus Oslo

GRA 19502

Master Thesis

Component of continuous assessment: Thesis Master of Science
Final master thesis – Counts 80% of total grade

White-collar crime in cyber time: the role of opportunity in committing financial crime online

Navn:	Maria Karvonen, Alla Fedina

Start:	02.03.2018 09.00
Finish:	03.09.2018 12.00

Alla Fedina

Maria Karvonen

-White-collar crime in cyber time: the role of opportunity in committing financial crime online -

Hand-in date:

03.09.2018

Programme:

Master of Science in Leadership and Organizational Psychology

Oslo, September 1st 2018

Acknowledgements

This Master Thesis is submitted to BI Norwegian Business School in order to finalize our MSc degree in Leadership and Organizational Psychology.

These two years of intensive studying within the framework of the program have been an enriching experience, that has provided us with valuable in-depth knowledge in the field of organizational psychology and adjacent disciplines. We have had the privilege to learn from several excellent professors, who have become a great inspiration to both of us.

Working with this thesis has been a challenging but interesting learning process. As the result of this project, we have gained invaluable knowledge and competence, which will serve as an important foundation for our future careers. We would like to thank our supervisor Petter Gottschalk for his incredible availability, valuable insights and competence. We would also like to express our appreciation for all the support we have received from our family and friends.
Finally, we would like to thank each other and every single one of our experts for making this study possible.

Sincerely yours,

Alla Fedina *Maria Karvonen*

Content

List of Tables

List of Images

Summary

The advent and expansion of Internet-enabled technology made likely the accomplishment of remarkable improvements in research, expertise, and communication. Unfortunately, computers and the Internet have furthermore supplied a new natural environment for crime. As pointed out by Jaishankar (2011), with the introduction of the Internet and subsequent possibilities, various forms of crime that have long existed before computer access require altered definitions to include the new ways these crimes can be committed.

This paper provides with an overview on white-collar crime and suggests that committing financial crime online or through computer-enabled technologies becomes more attractive for the offenders from opportunity perspective of the convenience theory. The purpose of this study was to contribute to the discussion on white-collar crime by identifying several characteristics of cyberspace that increase an attractiveness of engaging in online crime and finding the specifics of committing that crime from different perspectives in cyber context, followed by providing a foundation for further research in this field.

As a result of the study, there were severalised advantageous characteristics of the Internet related to crime category, criminals, crime type, situations and convenience dimensions. The findings of this research suggest ten factors that make online crime more attractive and convenient option. Seven of these factors were obtained through analysis of secondary and primary data: disconnected nature of personal communication, anonymity, geographical and timing distance, network size effect, low cost standard, no need for violence, and weak law regulation. The remaining three factors were empirically identified by experts in the field of cybersecurity and financial crime: larger rewards and returns on investment; automatization of the crime; and the dematerialisation of the crime. The findings also suggest that factors differ in terms of their positioning status. However, the results also indicate disagreement of experts with some of the stated hypothesis.

Future research is necessary and encourages to examine the need to continue the academic discourse regarding the boundaries of white-collar crime and white-collar cybercrime.

Finally, we consider gamification methods in employee training as a prevention strategy that could help organizations to mitigate the threat of cyber-attacks. Due to high significance of the subject in the organizational context, there was provided a detailed overview of the topic.

Key words: *white-collar crime, cyber, cyber attack, cybercrime, technology, convenience theory, opportunity, financial crime, gamification, training*.

Introduction

The purpose of this thesis

White-collar crime, as a multidimensional phenomenon, receives an increased interest from researchers and media as it becomes one of the most prevalent forms of contemporary economic crime. Bernie Madoff (Ponzi scheme), Jerome Kerviel (Societe General), Bernard Ebbers (WorldCom), Kozlowski and Swartz (Tyco International) - all are examples of famous and notorious crimes. After Enron scandal where its founder Kenneth Lay and top management team through repeated frauds and lies gained for themselves millions of dollars, the term white collar crime began to appear frequently in the media. By the current moment (May 2018) the academic database Web of Science shows 434 articles with the key phrase "white collar crime" in titles and 795 articles when searching white collar crime in topics. Google offers around 50 million results when searching for "white collar crime", where around 1,6 million results are from the news articles and media pages. There is an overwhelming amount of data sources, cases, stories and studies that support the increased public and academic interest in understanding the nature, detection and prevention of white collar crime.

A related emerging concept is a cybercrime, which entails committing a crime through Internet-enabled technologies. With a rapid growth of new technologies allowing not only for communication but also for conducting business online (e.g., e-commerce), new forms of crime have also appeared. Advances in Internet-enabled technology and devices have put high-profile criminal behavior at the forefront of people's minds with a click of a button and on a global scale (Helfgott, 2013). As a part of a global trend, white-collar crime has also migrated into cyberspace. That, obviously, changes the nature of white collar crime to a certain degree. Again, Google provides more than 5,2 million results (10 times fewer than for white collar crime, though) when searching solely for "cyber crime" and 6,7 million results when using the phrase "computer crime". Web of Science proposes 224 articles containing the word "cybercrime" in their titles, and 528 hits corresponding the topics. However, there are only few responses while searching for the combination of white collar and cyber-crime notions. This indicates that there is a niche for further scientific discoveries related to the white-collar crime in cyber setting.

Assuming that there is a need for an additional insight into the nature and specifics of such a crossover topic as white-collar cyber-crime, this thesis aims to contribute to existing research (1) by suggesting an integrated taxonomy of white-collar crime which will serve as a basis for further distinguishing between different types of crime; (2) by finding the specifics of committing white-collar crime in cyber context, through answering the main question: what characteristics of Internet-enabled technologies can be identified that make online white-collar crime attractive and through a set of additional sub-questions; and (3) by providing a foundation for further research in this field.

One of the major contributions of our paper is to create a research agenda, that considers various perspectives, some of which have not yet been used in this context. While many of the issues covered in this thesis are still the subject for continuing discussion among specialists, our main goal is to contribute to the debate on these issues rather than provide conclusive answers.

Research question

According to Lagazio, Sherif and Cushman (2014), cyber-crime is driven by rational cost-benefit calculations, when the readiness for engaging in such crime depends on whether risk-adjusted expected benefits of this crime outweigh the cost of committing it. As white-collar crime is one of the contemporary types of cyber-crime, we should find the reasons behind the white-collar crime transformation from the traditional form to the cyber one.

One may assume that there are benefits of transferring to cyberspace in order to engage in dubious activity. Computer form of white-collar crime becomes more attractive and appealing for criminal minds, as recent research (e.g., PwC's 2018 Global Economic Crime and Fraud Survey) states. Why do white-collar offenders prefer using cyberspace when committing a crime? What is so special in carrying out white-collar crime online? These questions encompass the main research question of this thesis which can be formulated as the following: **What characteristics of cyberspace can be identified that make online white-collar crime attractive?**

In order to answer this question, we will go through the evolving path of our investigation on the topic of white-collar crime, which suggests **an additional set of sub-questions**:

Can we apply universal characteristics of cyberspace, used in computer forensics, to the particular field of white-collar crime? If so, what is the specific effect of these characteristics in the context of white-collar crime? Do the identified characteristics change their influence or show any variance when the settings (type, category, executor of crime) are changing, too? If so, in which way?
The logic for answering the research question is described in the following part.

The structure of the thesis

Chapter 1 of the thesis is entitled "**Literature review**", where in the Part 1 we introduce existing approaches to the topic of white-collar crime and address the issues of conceptual definition of white-collar crime as well as the need to review the subject of white-collar crime in terms of its fusion with Internet-enabled technology. We provide with an overview of available conceptualization and the debate on the subject of white-collar crime, and exhibit concern regarding its migration to cyberspace, which creates the potential for more technical skills and offense specialization. Part 2 of the "Literature review" chapter assesses motivational aspects for committing white-collar crime and revises the use of available ideas in the literature to justify the integrated approach to the topic along three dimensions: offenses, offenders and victims. The selection of the information for literature review is due to the need to comprehensively classify white-collar crime along clear dimensions to further implement this classification in the practical setting. Furthermore, we introduce the term "cybercrime" to this study and provide with the latest statistics, highlighting the major transformation in the white-collar category of crime that has taken place alongside innovations in the technology.

Chapter 2 of the study is entitled "**Theoretical framework**". Here we revise concrete theoretical approaches in more detail. We provide with an overview of the novel theoretical perspective, which serves as an umbrella framework for reviewing the white-collar crime from the perspective of convenience. It serves as an organizing concept for a number of other relevant theories in this regard, and makes distinctions between economical, organizational and behavioral convenience. In particular, we are reviewing organizational opportunity as a distinct characteristic of white-collar crime and highlight the effect of disinhibition with regard to online interactions.

Chapter 3, namely "**Hypotheses**", entails introduction to the empirical study where, based on the discussed literature, we announce and explain seven hypotheses

which could help us in providing an answer to the research question. We suggest that cyberform of white-collar crime offers to criminals a larger set of advantages compared to the traditional physical form. Thus, committing white-collar crime online or through computer-enabled technologies becomes more attractive for the offenders from the opportunity perspective of the convenience theory. We end the theory-based part of the study with the Table 8 that accumulates the factors (characteristics of cyberspace) which, according to the literature, may positively influence the attractiveness of cybercrime and thereby increase the opportunity to engage in a criminal activity.

Chapter 4 entails the **methodology** of our empirical research, where we explain the methods chosen for this study, which assume working with both primary and secondary sources of data.

Chapter 5, namely "**Research results**", consists of two parts: Part 1 relies on the secondary data analysis and seeks to find an actual case (AFGlobal Corp.) of white-collar cybercrime to serve as an illustration for the discussion. We reassess the case from the perspective of the hypotheses testing, and therefore investigate how our theoretical hypotheses may unfold in practice. Part 2 of the Chapter 5 sets the task to ask several experts in the field of white-collar and cybercrime to share their opinion on the above discussed hypotheses. We perform descriptive statistical analysis and interpret the distribution of the answers, supported by visualization of results.

Chapter 6 is the "**Discussion**", where we analyze the most interesting results of the expert answers, as well as pay attention to any deviant from the most prevalent option or other contradictory responses. The results of the empirical part of our work (characteristics of cyberspace that make white-collar crime an attractive opportunity) are summarized in the Table 10. Then we compare Table 8 and 10, in order to see whether our hypotheses formulated on the basis of existing research are supported by empirical evidence (i.e. opinion of experts in white-collar/cybersecurity/fraud) and whether there is any new data available.

Chapter 7 describes **methodological limitations** of the study, while Chapter 8 provides the list of opportunities for **further development** with a special attention to further investigating of the role of training against cyber white-collar threat.

In the Chapter 9, we introduce **gamification** as a research topic with great potential for organizations to combat white-collar crime.

Finally, the **conclusion** comprises Chapter 10.

Chapter 1. Literature review

1.1. Definitional challenge

The evolution of criminology has introduced various theories related to the behavior of the criminal and the reasons for committing a crime. One of such theories was the Rational Choice theory, which adopted a utilitarian belief that a man is able to weigh means and ends, assuming that crime is a purposive behavior carried out to meet the offender's needs and personal situations. These situation-based theories were focused more on the socio-economic determinants of crime, such as family background and level of wealth. However, this idea was criticized by the criminologist and sociologist Edwin H. Sutherland when he introduced the term "white-collar crime" in 1939.

"This paper is concerned with crime in relation to business" (Sutherland, 1940, p.1). This opening statement of Sutherland's article, first published in February 1940, commemorated the birth of the concept of "White-Collar Criminality". Yet, from the relatively simple opening line, it has quickly become, and has remained ever since, one of the most complicated and elusive areas in criminology to research, theorize and even define.

Whilst conceptualization of the phenomenon has not happened before 1940, historically, economic crime is as old as economic activity, say Berghoff and Spiekermann in their "History of white-collar crime" (2018). Already in the seventeenth and eighteenth centuries, colonial companies (e.g., the East India Company, Royal African Company, and the Levant Company) were rocked by large corruption and embezzlement scandals, triggering public debates about private and public interests and the need for a change in corporate and state governance (Berghoff & Spiekermann, 2018). Sutherland's concept introduces white-collar criminals as an opposite to "traditional" perpetrators from lower classes, so called "blue collars", and street criminals. As far as Sutherland was concerned, white-collar criminals and blue-collar lower-class street criminals differed only with respect to "the incidentals rather than the essentials of criminality" (Sutherland, 1940, p.11). These criminals have been working in office setting and had a social status that allowed them to wear white collars as part of their dress code without the fear of getting them dirty in contrast to blue collar workers. The main idea was that even wealthy and respectful persons from privileged society are able to commit a profit-driven crime. Sutherland contradicted

widespread views that criminality was caused by poverty or biological and psychological factors, claiming instead, that the total damages of white-collar crimes were several times higher than those of all other crimes combined (Berghoff & Spiekermann, 2018).

However, there are considerable debates regarding whether only individuals from upper class are capable of committing white-collar crime. Now more and more scholars argue that the term "white-collar crime" entails a larger percentage of offenders, who are the members of the middle class. As Van Slyke et al. (2016) state, most analyses confirm that managers and their subordinates and not the owners are more directly implicated in the most serious white-collar offenses. Brightman (2009, cited in Gottschalk, 2016) explains that personal computers and the Internet allow individuals from all social classes to engage in similar activities that were once the privilege of the financial elite (e.g., buying stocks).

In order to deal with this unclear categorization, researchers try to define occupational offenders as "privileged" (Van Slyke et al., 2016), highlighting their common characteristics such as membership in the middle and/or upper classes and employment in respectable organizations. Nevertheless, more detailed definitional assessment is needed. Therefore, in this work we refer to white-collar crime as all illegal behavior that takes advantage of positions of professional authority due to person's access to opportunities for personal or corporate gain. In general, white-collar crime is financial crime committed by trusted and potentially reliable persons in important business positions (Gottschalk, 2013a). According to Gottschalk (2016 a,b,c)'s research, a white-collar criminal is typically a member of the privileged socioeconomic class in society, who commits non-violent financial crime in a professional setting. The criminal has the power and influence, enjoys trust from others in privileged networks, does not consider own actions as crime and has no guilt feelings (Gottschalk, 2016a). As Berghoff & Spiekermann (2018) continue, several factors create a privileged position for white-collar criminals: their offences are especially difficult to prosecute because of the sophisticated means to conceal their actions while the best lawyers and political influence are at their disposition.

The organizational context of this type of crimes is particularly important in distinguishing white-collar crime from other incidents. As Gottschalk (2017) highlights, such illegal actions as abusing social security benefits, committing tax evasion or committing Internet fraud on a personal level are not considered as

white-collar crime, because the latter are assumed to be committed only in a professional capability and not in an organizational context.

The scale of white-collar crime has increased considerably over the recent decades and this trend is expected to continue. Although, the study of the criminal mind and the motivations and the nature of criminal behavior has puzzled scholars and criminologists for centuries, none of these pioneers would have imagined the enormity and complexity of criminal psychology at the dawn of the twenty-first century (Helfgott, 2013).

The post-Internet era and the presence of cyberspace has created new opportunities for criminal behavior. White-collar crime has evolved its dimension and the nature of cyberspace and the Internet has changed our prior understanding of the physics of criminal actions. The weakened relevance of time, distance, quantity, legislation and authority created a greater ability for motivated offenders and potential victims to utilize the cyberspace (Helfgott, 2013). The environment of cyberspace provides a novel way for these conditions which causes the fusion of white-collar crimes and cybercrimes.

This paper sets out with the aim of improving upon existing taxonomies used in categorization of white-collar crime and providing with understanding on the explicit specifics of cyber aspect in committing this type of crime.

1.2. Extended literature overview

"The challenge of analyzing the phenomenon of white-collar crime lies in the fact that the term "white-collar crime" signifies different things to different disciplines or even different things to different camps within those disciplines", say Cliff and Wall-Parker (2017, p.2). This quotation highlights the definitional challenge, mentioned above, and may be expanded in our case to the literature review of the existing research on the topic. Since there are plenty of distinct approaches and established perspectives on what and in which way a researcher may study when aiming to study such a broad phenomenon as white-collar crime, the choice of relevant literature for reviewing was heavily limited by both the main purpose and boundaries of the master thesis work. Moreover, even when the research question becomes narrowly focused on the features that only began to arise or on uncovered yet issues, the full and comprehensive literature review of the struggling with definitional and conceptual challenges field, would be almost impossible to achieve.

Nevertheless, in this review we have tried to absorb the most actual information gained from academic publications, scientific and popular articles of prominent scholars as well as from field reports and surveys performed by acknowledged public and private organizations (FBI's Internet Crime Complaint Center, PwC, etc.). The main method we used was the database search for common keywords on the subject, meanwhile the most solid authors (such as Benson, Gottschalk, Ketil Arnulf, Lagazio, Miller, and others) have been mapped according to their research interests and scanned for published works in the area. Thus, first we review some of the existing theories explaining why white-collar employees commit crimes, then we try to suggest an integrated taxonomy of different types of white-collar crime based on the works of distinguished scholars in that field, and, finally, we approach white-collar crime as a part of contemporary computer crime, which is a highly important part of the review in order to accomplish our research goal. After the research question is formulated, we dedicate a special part of the literature review to overview the theoretical framework, relevant for our research question.

1.3. Motivational aspects of white-collar crime

Although motivation for committing white-collar crimes seems to be as simple as financial gain, the reasons behind the desire for the financial gain are one of the most discussed topics in this field. Gottschalk (2017) considers two general but opposite points of view. On the one hand, since white-collar crime has been mostly studied in the USA, researchers refer to the concept of the American dream, which implies to anyone's ability to become monetary successful and has a deep root in American mentality. A high rate for white-collar crime can be explained by the person's commitment to the material success as experienced in the American dream (Gottschalk, 2017). When such overemphasis on the value of success is present, the end justifies the means, i.e., committing non-violent crime does not provoke a feeling of being a criminal. On the other hand, the fear of falling theory suggests that people in high-level positions are afraid of consequences from failure and therefore try to survive in their positions (Piquero, 2012). As Gottschalk (2017) explains this idea, white-collar managers and top executives are afraid of losing their wealth and status, working hard to remain successful and solve their problems by any means. Thus, financial gain becomes not only a matter of making even more

money: “It is an issue of survival, and it may be about rescuing a sinking ship.” (Gottschalk, 2017, p. 2).

In conformity with the managerial perspective, that highlights the role of managers as agents for deciding and leading enterprise strategies and operations, implementing corporate priorities, managers’ perceptions and interpretations determine their commitment to certain goals over the others and may lead to implementation of legal and illegal strategies (Gottschalk, 2016a).

Therefore, according to Gottschalk (2017), white-collar crime may be a response to possibilities and strengths as well as to threats and weaknesses. This leads us to consider the existing classification of white-collar crime.

1.4. Taxonomy of white-collar crime

White-collar crime is typically characterized by the ambidextrous nature, since it can be defined in terms of the offense, the offender or both. In terms of the offense white-collar crime means a crime against property for personal or organizational gain. It is a property crime committed by non-physical means and by concealment or deception (Benson & Simpson, 2009, cited in Gottschalk, 2017). In terms of the offender, white-collar crime entails crimes committed by the members of the upper class for personal or organizational gain, which possess a set of specific characteristics, related to their social position. They usually are individuals who are wealthy, highly educated, and socially connected, and they are typically employed by and in legitimate organizations (Hansen, 2009, cited in Gottschalk, 2017).

Although there are several approaches to white-collar crime as a phenomenon (see, e.g., Sutherland (1940, 1949); Geis & Jesilow (1982); Shapiro (1990); Nelken (1994); Brightman (2011); Gottschalk (2013a, 2016a,b,c); etc.), within boundaries of this work it is not realistic to perform a wholly comprehensive meta-analysis of almost 80 years of existing research on white-collar crime. Instead, our aim is to focus on the vital attributes any white-collar crime classification possesses and thereby offer an optimal taxonomy, combining several perspectives and allowing for further implementation in practical settings (which will be discussed later). Therefore, we will assume brief nonetheless clear model for assessing white-collar crime concept along three dimensions: offenses, offenders and victims.

1.4.1. Offense perspective

Since financial gain as a motive for white-collar crime may either benefit the person or the organization (Gottschalk, 2017), the first assessed dimension (offense) can be presented as the distinction between occupational and corporate crime. Occupational crime occurs when an individual's occupation enables him/her to commit white-collar crime in order to get personal benefits. The motives for illegal financial gain can vary: it can be increased personal wealth and providing for relatives and friends, avoidance of personal bankruptcy/falling from a high-status position in society, or even compensating for the lack of popularity by buying friends (Gottschalk, 2017).

Corporate crime occurs when financial gain benefits not the individual him/herself but the organization (often through founders' illegal actions). For instance, it could be motivated by a company's need in achieving a new contract and establishing a subsidiary in a corrupt country, or by avoidance of bankruptcy of the business (e.g., through tax evasion and bank fraud) (Gottschalk, 2017). In other words, corporate crime represents pro-organizational actions or voluntary tasks undertaken to benefit the organization including helping and solving problems and exploring possibilities on the wrong side of the law (Gottschalk, 2016a).

Williams (2006) suggests a third type of crime, which is a criminal activity disguised as legitimate business, and groups some of the common white-collar criminal activities into one of these three categories. However, since the crime as an organized business is beyond the scope of our work, we will consider only two crime types in our taxonomy (i.e., corporate and occupational crime).

Thus, both occupational and corporate crimes can take any of these four broadly acknowledged forms of white-collar crime: fraud, theft, manipulation, corruption. *Fraud*, according to Henning (2009)'s definition, is an intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to deprive a victim of a legal right, where a perpetrator tries to keep the property from the victim. On average, as Gottschalk (2013b)'s analysis shows, most convicted criminals are involved in fraud crime cases, typically bank fraud. *Theft* can be defined as the illegal taking of another person's, group's or organization's property without victim's consent (Hill, 2008, cited in Gottschalk, 2013b). Identity theft is one of the most common forms of this crime. *Manipulation,* in accordance with Malkawi and Haloush (2008) entails gaining illegal control or influence over others' activities, means and results.

Tax evasion as a manipulation crime most prevalent in many countries is the result of the failure to comply with national income tax laws (Gottschalk, 2013b). Finally, *corruption* is the giving or receiving of an improper advantage, linked to a person's position, office or assignment (Kayrak, 2008). "Corruption is to destroy or pervert the integrity or fidelity of a person in his discharge of duty, to induce to act dishonestly or unfaithfully, to make venal, and to bribe." (Gottschalk, 2013b, p. 21).

1.4.2. Offender perspective

Offender's perspective is the second dimension to consider in our overview. Although research identifies several common characteristics of white-collar criminals as their personal psychological and social attributes (e.g., wealthy, highly educated, employed in organization and committing crime in a professional settings, fearing to lose their status or striving for monetary success (Gottschalk, 2016c); showing greater score in psychopathic traits (Ragatz, Fremouw, Baker, 2012); risk-taking (Berghoff & Spiekermann, 2018); narcissistic (McKay, Stevens, Fratzi, 2010; Ouimet, 2009; 2010); irresponsible, low in social conscientiousness and therefore behaving in antisocial way (Collins & Schmidt, 1993)), we suggest further offender differentiation based on their official role in relation to the organization.

In general, there are two main categories of criminal types: leaders and followers. However, there are several categorizations varying within the same field due to the context used. Still, we integrate the findings from these two papers: "White-collar Criminals in Modern Management" (Gottschalk, 2013a) and "Principals, Agents and Entrepreneurs in White-Collar Crime: An Empirical Typology of White-Collar Criminals in a National Sample" (Ketil Arnulf & Gottschalk, 2012). The first research, based on a sample of 305 convicted white-collar criminals in Norway, offers four groups of offenders: criminal entrepreneurs, corporate criminals, criminal followers, and female criminals. The second paper on the basis of agency theory and a sample of 222 convicted Norwegian offenders provides a framework of six roles of white-collar criminals: principal, agent, entrepreneur, servant, public official and robber criminal. With respect to all discussed types, we distinguish offenders not by their gender (male and female criminals) neither by the main motive behind illegal financial gain (corporate and occupational criminals), but by the frequency they hold the concrete position. Therefore, the most frequent roles of white-collar crimes are principal, agent and

entrepreneur criminals, while less frequent are servants, followers, public officials, and robber criminals. Within the context of this work, we are going to refer to more general categorization of criminal types, such as leaders and followers.

According to the agency theory, owners of a company (principals) hire managers (agents) to perform on their behalf and for maximizing the company's value (Engelmann-Zach, 2014). In this light, high incentives are the way to align the interests of agents with the interests of principals, while relating compensation to the achievement of performance goals can have motivational effects on employees, improving firm performance (Engelmann-Zach, 2014). However, Ketil Arnulf & Gottschalk (2012) state that since principals always suspect agents of making decisions that benefit themselves, CEOs may always be suspected of cheating on the owners and appropriate measures of checks are needed. Thus, one of the prevalent offender's type is agent criminal, represented by CEOs or similar top executive positions. Nevertheless, principals (in terms of chairmen and members of board) may also commit white-collar crime. However, as Arnulf and Gottschalk (2012) recognize, when there is a mix of roles, the principal-agent distinction is not always applicable in practice. They label those offenders who themselves are the sole owners and CEOs of a company that partly or entirely engage in unlawful activities to make revenues, often using creative methods and novel ways instead of more established ways of organizing similar work, as entrepreneur criminals, highlighting the "entrepreneurship" as the nature of such crimes (Ketil Arnulf & Gottschalk, 2012). Although the CEOs are twice as likely to engage in crimes as their principals, the most typical role of a white-collar criminal is the entrepreneur one. It is also worthy to note that in the sample of Ketil Arnulf and Gottschalk (2012)'s research, a large share of the entrepreneurial criminals has established or used their companies to cover up crimes of others, making their role as a leader of crime questionable. Besides, when comparing to others, this type of offenders makes the biggest profits. When board members and top managers are making themselves criminal for profits that are only fractions of their wealth, entrepreneurs engage in crime striving for exceeding their recorded assets much more (Ketil Arnulf & Gottschalk, 2012).

The less frequent types of offenders in terms of their occupied position are servants (accomplices to entrepreneurs or CEOs due to their specific knowledge or access); followers (non-assertive persons, convinced by cause of the crime or charisma of their leaders or just following the orders expecting returns for their

obedience); public officials (third party regulators as police or municipalities with their own interests); robber criminals (private persons acting without any business relation to the victim for individual purpose).

Paying attention to specific characteristics of offenders in relation to their position (abilities, access to confidential data and leadership level) may enrich the existing research, focusing on both personality and formal role of white-collar criminals.

1.4.3. Victim perspective

The third dimension of white-collar taxonomy is the victim perspective. The criminals differ in terms of the targets for their illegal activities. Again, an integrated view will be presented below.

In general, white-collar criminals cause financial damage to four categories of victims: business owners (in terms of investors, shareholders or any employers involved), customers, society and government (in terms of tax authorities and nation prosperity), and innocents (bystander persons). According to Gottschalk (2013b)'s research, based on the national sample, employers represent the largest group of victims, while banks are the second largest group of victims with the most severe jail sentence for white-collar criminals in this category. As research states, all white-collar criminals are about equally likely to engage in crime against government (in form of tax frauds); every third white-collar criminal (in particular CEOs and board members) is convicted of cheating investors; entrepreneur criminals are also cheating investors, but they are more inclined to cheat customers through maximizing their returns by reducing the created value (Ketil Arnulf & Gottschalk, 2012). However, as Berghoff and Spiekermann (2018) note, the victims of white-collar crimes cannot be easily identified since the harm from illegal actions is spread out over many people. For instance, a bribery may lead to overcharging in public projects and result in higher taxes for all citizens of a country (Berghoff & Spiekermann, 2018). So, on the face, white-collar crime as a financial crime appears to be victimless, but in fact victimization is real though diffused.

Regarding practical implications, the crime strategy is likely to vary depending on the victim specificity, therefore, if we aim to anticipate and prevent white-collar crime, the understanding of interrelatedness of all these dimensions taken together - offense, offender and victim - can influence the effectiveness of preventing programs.

1.5. White-collar crime as a part of cybercrime

Fraud, theft, manipulation and corruption are well-known, common traditional white-collar crimes in the field of deviant behavior. However, due to rapid growth and increased availability of new technologies, which enable electronic commerce, negotiation and banking through computer-related media and Internet, traditional form of crime is being actively replaced by its cyber form.

Organizations are reporting a growing number of cyber attacks. PwC's Global State of Information Security Survey (2016) states that the number of security incidents in cyberspace across all industries rose by 38% in 2015, which is the biggest increase in the 12 years since this global survey was first published. Meanwhile, in terms of the share of cyber attacks driven by the financial gain, PwC's Global Economic Crime and Fraud Survey (2018) claims that 31% of respondents indicate that they fell a victim not to traditional crime but to cybercrime, which is ranged as second place after asset misappropriation (42%). Although it can be difficult for companies to accurately measure the financial impact of cyberattacks, 14% of survey respondents who said cybercrime was the most disruptive fraud told us they lost over $1 million as a result (PwC's Global Economic Crime and Fraud Survey, 2018). Over one third of all respondents have been targeted by cyberattacks, through both malware and phishing. Most of these attacks, which can severely disrupt business processes, also lead to substantive losses to companies: respondents who were attacked suffered asset misappropriation and were digitally extorted (PwC's Global Economic Crime and Fraud Survey, 2018). The infographics below show the types of fraud that organizations were victims to through a cyber-attack:

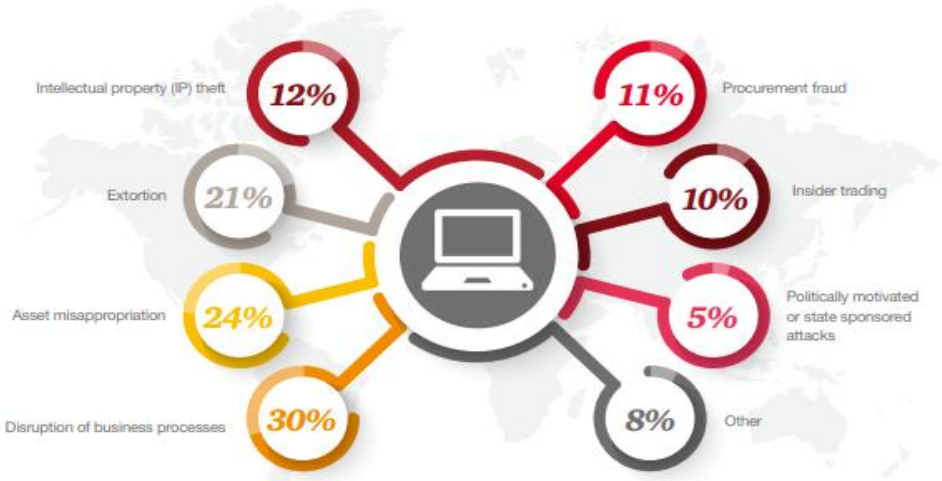

Image 1. Types of fraud and economic crime that an organization has experienced
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Another sources, such as German Gref, the CEO of Sberbank, a state-owned Russian banking and financial services company, the largest bank in Russia and Eastern Europe, and the third largest in Europe, says that the share of cybercrime in finance is even greater. According to Gref, the share of cybercrime in the financial sector in 2016 has reached 98.5%, while the remaining 1.5% of crimes were committed by traditional means (Banki.ru, 2017) [own translation].

So, first we should explain what is understood by the term "cybercrime" and then find the role of white-collar criminals in that.

In general, cybercrime (or computer enabled crime) may be divided into two big categories: crime where a computer serves as a means (instrument) or as an end (target). Similarly, Kirwan and Power (2013) divide cybercrimes into internet-enabled and internet-specific. Internet-enabled crimes can also exist offline, but the presence of internet-enabled devices allows for easier and faster execution of such offences. Internet-specific crimes are those cybercrimes that do not exist without an Internet-enabled environment. However, due to its relative novelty, the concept of cybercrime is open to a variety of social, political, criminological and academic interpretations and explanations. As Lagazio et al. (2014) summarize, most of the definitions of cybercrime take into consideration "the utilization and mediation of cyberspace in the perpetration of cyber criminal activities, while distinguishing those criminal activities that are heavily dependent on cyberspace from those that are not" (p.64). In few words, cybercrimes are criminal activities transformed or mediated by the Internet (Wall, 2007, cited in Lagazio et al., 2014). In our work, we will adhere this definition in order to focus on essential characteristics of cybercrime rather than on the specific technological attributes.

Lagazio et al. (2014), when assessing the impact of cybercrime on the financial sector, divide the former into four categories: (1) *traditional crimes* conducted online and exploiting cyberspace as providing more opportunity for crime (e.g., traditional fraud, piracy, espionage, stalking, trading sexual material); (2) *hybrid cybercrimes* which are traditional crimes whose effectiveness, nature and modus operandi have significantly changed as a result of new opportunities provided by the Internet (e.g., ID theft, hacking, hacktivism, illegal online sex trade); (3) *true cybercrimes* consisting of opportunities created purely by the Internet and carried out only within cyberspace (e.g., spam, denial of service, phishing, illicit cyber sex); (4) *cyber platform crimes* such as the use of botnets to facilitate other crimes (Lagazio et al., 2014, p. 65).

On the whole, from organizational perspective, any organization may face two distinct types crime: external and internal. Each year the Software Engineering Institute (SEI), a federally funded research and development center sponsored by the U.S. Department of Defense, develops a U.S. State of Cybercrime report, where more than 500 organizations self-report on information security issues that have impacted their work. One of the assessed threats for organizations is the insider's attack. As SEI researchers claim, historically organizations have focused on external security mechanisms (firewalls, intrusion detection and electronic building access systems). However, the insider threat is real and substantial, since an insider possesses an advantage over external attackers. They are aware of their company's policies, procedures, routines and technologies, as well as of their vulnerabilities and security gaps. The 2016 U.S. State of Cybercrime Survey reports that 27% of computer crimes were suspected or known to be caused by insiders, while the 2017 survey states that although the amount of crime has slightly decreased, nearly half (43%) of survey respondents acknowledged that computer crimes committed by insiders were costlier than those committed by outsiders (Miller, 2018). Besides, 44% of organizations indicated that they could not identify the individuals behind an incident, and this is a 13% increase from the last year. Therefore, the seeming decrease in amount of crimes could be attributed not to the fact that there are fewer insider incidents but instead to the fact that organizations are becoming less potent to identify them.

As Miller (2016) reports, in 453 of the 726 incidents where a malicious insider's motivation was known, that motivation was financial gain (62.4%). At the same time, high-earning male insiders represent 45% of all male insiders. 29% of high-earning insiders committed fraud and 71% committed theft of intellectual property (IP). Particularly within incidents of theft of IP, these male insiders typically held developer or C-suite positions (Miller, 2016). "While those committing fraud may have done so to fund their lifestyle, others may have committed theft of IP for a competitive business advantage", - says Miller (2016, p. n\a).

Other sources, such as the most recent PwC's 2018 Global Economic Crime and Fraud Survey, claim that 52% of all frauds are perpetrated by people inside the organization, while frauds committed by senior management increased from 16% to record 24% (PwC's Global Economic Crime and Fraud Survey, 2018), that is in

line with previous research and show an important tendency for growth of both internal fraud and criminal activities of CEOs.

In general, the gained data allows for a speculation that at least a part of the mentioned crimes were committed by persons which literature identifies as white-collar criminals. Therefore, one can assume that white-collar criminals also use the facilities of cyberspace to commit their crimes. For instance, traditional fraud and theft committed by white-collar criminals become online fraud and online identity theft (in most cases), while manipulation and corruption incidents are also facilitated by computer technologies. Although there are only few specific statistical data available on the amount of white-collar crime committed through computer-enabled devices (i.e., gained from Miller (2018) or PwC's reports), the general tendency allows for speculations about the constant growth of this form of crime as a function of a total amount of cybercrime.

Chapter 2. Theoretical framework

Theory is a statement of concepts and their interrelationships that shows how and/or why a phenomenon occurs (Corley & Gioia, 2011 cited in Gottschalk, 2017).

This chapter will provide an overview of the novel theoretical perspective of convenience, which accumulates the knowledge regarding the occurrence of white-collar crime and criminals, serves as an organizing concept for a number of other relevant theories in this regard, and makes distinctions between economical, organizational and behavioral convenience. Convenience orientation is conceptualized, as well as empirically examined and validated by Gottschalk (2016c; 2017). His recent research is described as "theory testing by evidence" (Gottschalk, 2017, p. 159) and is concentrated on establishing the validity of the theory's core propositions. Gottschalk's work on convenience theory introduces the construct of convenience and defines relationships between its dimensions: economics (desire for more profit), organization (opportunity for crime) and behavior (willingness to commit crime). These three dimensions influence each other and identify a set of further relationships among them.

These aspects of the convenience theory provide accumulated knowledge, relevant for the study, and accommodate the reader with contemporary background information to understand and critically assess the findings.

2.1. Convenience theory

According to Gottschalk (2016c), convenience is the perceived savings in time and effort required to find a solution or to exploit an opportunity. Convenient action is an action which can be also characterized as easy, comfortable, advantageous or suitable. The convenience theory suggests three main dimensions to explain white-collar crime.

The first (economical) dimension is coded as motive and is concerned with economic aspects, where the illegal financial gain is a convenient option for the offenders to satisfy their needs. The second (organizational) dimension is concerned with opportunities opening to the offenders from organizational aspects, where the offender has convenient access to premises and convenient ability to hide illegal transactions among legal transactions. The third (behavioral) dimension relates to people's willingness to engage in illegal behavior and implies that the offender has convenient justification and acceptance of their own deviant behavior (Gottschalk, 2016c). All these dimensions are linked to each other. Economic dimension interacts with the behavioral one in terms of the fear of falling concept, where entrepreneurs or CEOs perceive committing a financial crime and gaining some money as the only way out of the crises they are afraid of. Consequently, behavioral dimension may interact with the organizational one, if the offenders with expressed psychopathic or narcissistic personality traits may take a risk to engage in criminal act and search for such opportunities.

However, within this thesis, we will focus only on the organizational dimension of the convenience theory (opportunity for crime), since our research question is mostly concerned about external factors, that facilitate engaging in cybercrime, rather than internal motives of criminals or their behavioral dispositions.

2.2. Opportunity perspective

Organizational opportunity is a distinct characteristic of white-collar crime. A criminal opportunity is defined by Aguilera and Vadera (2008, p.434, cited in Gottschalk, 2017, p. 40) as "the presence of a favorable combination of circumstances that renders a possible course of action relevant". Benson, Madensen and Eck (2009) assume that all forms of white-collar crime have an opportunity structure, defining opportunity as a set of conditions (varying from one type of

offense to another) that must be in place in order for the offense to be carried out. Gottschalk (2016c) defines opportunity as an opening and a possibility to commit criminal acts in order to reach an organizational or a personal goal: “When criminal opportunity is attractive as a means to fulfill one’s desires, rational actors will choose it” (Gottschalk, 2016c, p.xii).

The organizational opportunity for an offender consists of two dominating aspects: an opportunity to carry out financial crime, and an opportunity to conceal and hide financial crime, in both cases due to a prominent position of the offender in the organization based on trust and power (Gottschalk, 2016c). From routine activity theory, opportunity entails two important elements: a suitable target and a lack of capable guardianship.

Benson and Simpson (2014) highlight three opportunity properties: offender’s legitimate access to the location where the crime is committed; offender’s spatial separation from the victim; and superficial appearance of legitimacy of the offender’s actions. This is in line with Gottschalk (2017)’s opportunity characteristics: legal access to premises and resources, distance from victims, and manipulation within regular transactions.

How are criminal opportunities actually formed by environment and how are they discovered later by criminals? Benson et al. (2009) answer these questions through applying three perspectives: routine activity theory, crime pattern theory, and situational crime prevention theory.

According to routine activity theory, necessary conditions for crime (opportunities) are present if three key elements - a target, a motivated offender and a common place where the offender can gain access to the target - are also in place. If there is a lack of guardianship (i.e., the absence of an effective controller, which can be a guardian for targets or a handler for offenders), a crime will occur (Cohen & Felson 1979; Eck 1994; Benson et al., 2009). In post-modern era, a common place where offenders gain access or meet their victims is moved to cyberspace and its facilities (e.g., Internet networks). The function of such networks is to facilitate contact between the offender and the victim. Although the routine activity approach was originally written to account for direct-contact offenses, it appears that it could also be applied to crimes in which the victim and offender never come into physical proximity (Reyns, 2013).

Crime pattern theory states that offenders tend to find their victims in familiar places. As Benson et al. (2009) point out, “criminal opportunities that are

close to the areas that an offender moves through during their everyday activities are more likely to be taken advantage of by the offender than opportunities in areas less familiar to the offender" (Benson et al., 2009, p.180). In terms of white-collar crime, the offenders' awareness of opportunities arises out of their position (occupation within the organization) and work environment, where larger networks provide more opportunities for a crime.

Situational crime prevention theory explains why some criminal opportunities are more attractive to offenders than others. Based on the rational choice perspective, this theory assumes that offenders consider both the costs and benefits of engaging in such activity (Cornish & Clarke, 1986; Benson et al., 2009). Offenders base their choice on the following characteristics of criminal opportunity: the effort required to carry out the crime; the risks of detection; the gain from the crime; situational conditions that may encourage criminal action; and excuses that offenders can use to justify their actions (Cornish & Clarke, 2003; Benson et al., 2009). Consequently, white-collar crimes are more likely to occur if they are "easy to commit, have low risks of detection, provide an attractive reward, are encouraged by the immediate environment, and are easy to justify" (Benson et al., 2009, p. 183).

The opportunity perspective of the organizational dimension, which proposes convenient opportunities for white-collar crime, facilitated by the development of the Internet-enabled technologies highlights the effect of disinhibition with regard to online interactions.

2.3. The online disinhibition effect

The online environment is convenient and comprises numerous opportunities for committing a crime. Such opportunities include, among others, anonymity and invisibility, which relate to online disinhibition, generally understood as the tendency to feel less inhibited and less concerned with the consequences of one's actions in the online world (Wright, Harper & Wachs, 2018). Explanation of the disinhibition on the Internet can be traced to the concept of deindividualization or submergence, proposed by Gustave Le Bon in 1895 with relation to being in a crowd. Le Bon argued that being a member of a crowd led to submergence, a state where the normal constraints on individual behavior are removed. During the period from 19th to 20th century, deindividualization theory was subjected to a series of reformulations, variously taking into account the role of reduced internal focus.

Deindividualization has been suggested to be caused by two factors: a reduction in accountability cues (i.e., anonymity) and reduction of private self-awareness (i.e., low internal standards and self-regulation) (Joinson, 2007).

Suler (2004, 2005) explains online disinhibition as loosening of the repressive barriers against underlying fantasies, needs, and affect, and identifies six main factors that lead to an "online disinhibition effect": dissociative anonymity (i.e., you don't know me), invisibility (i.e., you can't see me), asynchronicity (i.e., see you later), solipsistic introjection (i.e., it's all in my head), dissociative imagination (i.e., it's just a game), and minimization of authority (i.e., we are equals).

Withal, considerable evidence suggests that cyberspace loosens psychological barriers and may provoke deviant behavior (Joinson, 2007). The six factors, constituting the disinhibition effect, interact with each other and supplement the three dimensions of the convenience theory, resulting in a more complex, amplified effect of cyberspace on the mindset of online users, decreasing the sense of personal accountability and altering self-boundaries, and therefore contributes to an increased tendency to commit online crime.

Chapter 3. Hypotheses

Based on the preceding discussion, in the organizational setting, opportunities faced by an offender can be transformed to advantages with an unlimited authority even before engaging in the crime. Such advantages often include access, relevant anonymity, simplicity and immediate results. As Gottschalk (2016c) summarizes, from the opportunity perspective, white-collar criminals take advantages of their position because "they have legitimate and often privileged access to physical and virtual locations in which crime is committed, are totally in charge of resource allocations and transactions, and are successful in concealment based on key resources used to hide their crime" (Gottschalk, 2016c, p.42). These advantages are general for white-collar crime as a broad concept. Coming back to the research question, we suggest that cyberform of white-collar crime offers to criminals a larger set of advantages than traditional physical form of white-collar crime does. So, committing white-collar crime online or through computer-enabled technologies becomes more attractive for the offenders from opportunity perspective of the convenience theory. Therefore, we hypothesize that white-collar

criminals choose cyberspace as the means for committing their crimes because of the broad range of opening opportunities.

In order to proceed with hypothesis, we will refer to the findings accumulated in previous chapters (Chapter 1 & 2) of this thesis. Our aim was to focus on the vital attributes of white-collar crime classification and thereby offer an optimal taxonomy, combining several perspectives and allowing for further implementation in practical settings. As a consequence, we have assumed a brief model for assessing white-collar crime concept along three dimensions: offenses, offenders and victims (partly). As per theoretical framework for the thesis, we have proposed to view our findings through the prism of the novel theoretical perspective of convenience, which accumulates the knowledge regarding the occurrence of white-collar crime and criminals and makes distinctions between economical, organizational and behavioral convenience.

In general, one could assume that 1) greater amount of computer-enabled technologies, programs and tools used at work and 2) greater access to such tools given to top management positions might lead to a greater number of opportunities for engaging in cyber activities, which could be out of law.

Gottschalk (2010) describes characteristics of Internet as a place for crime which facilitate committing such cybercrime as online child grooming. Still, the global nature of modern technologies allows us to expand these characteristics towards white-collar crime and study whether this expansion has a place to be. Based on specific characteristics described by Gottschalk, we may suggest a subset of hypotheses aimed to explain 1) how Internet-enabled characteristics (cyberspace opportunities) act as advantages when deciding whether to commit a crime and 2) how they can be applied in case of white-collar crime. However, in order to thoroughly answer the research question and present our hypothesis, we should find out what specifically addresses white-collar and make them engage in a crime by using technological means. Therefore we have decided to accrue all the above research and on the basis of the taxonomy described in previous part, and *distinguish between advantageous characteristics of the Internet related to crime category (such as fraud, corruption, theft, and manipulation), criminals (leader, follower), crime type (occupational, corporate), situations (threat and possibility) and convenience dimensions (motive, opportunity and willingness).* This will be our theoretical contribution to the existing research on white-collar crime and cybercrime. We present brief explanation of each characteristic, followed by our

detailed description of their effect in tables (Tables 1 - 7), and then we formulate a consequent hypothesis.

3.1. Disconnected nature of personal communication

First, cyberspace is characterized by a disconnected nature of personal communication, where personal communication is not perceived as interpersonal (Gottschalk, 2010). Such disconnectedness helps a criminal to avoid unpleasant emotional states (e.g., feeling of guilt), removing inhibitions related to face-to-face contact. Internet-enabled means of communication create an illusion of being invisible as well as of being unrelated to another party of communication. Usually, top managers (as an example of white-collar group) tend to perceive themselves as decent persons, who deserve their high position and privileges after years of hard and ambitious work. The disconnectedness from their victims keep their world perception in balance and helps not only avoid the mental discomfort but also protect them from living with cognitive dissonance in the future after performing actions that are expected to contradict personal beliefs and one's own perceptions.

Table 1: The effect of disconnected nature of personal communication on the engagement in a crime by using technological means.

Fraud	Corruption	Theft	Manipulation
Disconnected nature of personal communication as an inherent attribute of any impersonal activity in cyberspace does not significantly change its effect on people perception of	Disconnected nature of communication decreases the possibility of detection, making the risk-reward balance to outweigh towards committing the corrupt act.	While communication on the Internet might be personal in content, it is not perceived by criminals as interpersonal in meaning due to disconnected nature of communication. Inter net removes inhibitions associated with face-to-face contact, thus making	Marginalization of personal communication through electronic means facilitates emotional detachment from the subject, allowing to gain illegal control or influence over others' activities, means and

such a communicative act when a crime category is changing from online fraud to online theft and so on.		commitment of identity theft just a business transaction.	results. Whether this is data manipulation or tax evasion, disconnected nature of personal communication makes individuals to unconsciously change their personality while online and creates an illusion of being unrelated to the manipulated objects.

Leader	Follower
The benefits of disconnected nature of personal communication do not depend on the criminal types.	The benefits of disconnected nature of personal communication do not depend on the criminal types.

Occupational	Corporate
Disconnected nature of personal communication makes *attractive any type of crime regardless* whether they satisfy personal or organizational needs and whether they are committed in traditional or cyber form. For occupational crime, disconnected nature of communication is a perfect	Disconnected nature of personal communication makes *attractive any type of crime regardless* whether they satisfy personal or organizational needs and whether they are committed in traditional or cyber form. For corporate crime, it is an opportunity to "provide for the company" and remain unpunished.

maneuver to remain undiscovered by people that might recognize him otherwise.	

Threat	Possibility
As criminals try to implement any actions in order to avoid financial risks, monetary or social failure, the ability to keep their world intact may be seen as advantageous in terms of avoiding one more problem.	As long as disconnected and impersonal communication will facilitate increasing one's own wealth and gaining other benefits, it will be seen as *possibility*, especially in tight connection to anonymity and its advantages.

Motive	Opportunity	Willingness
The current research does not evidence strong and/or significant correlation between disconnectedness of communication and financial goal.	Disconnectedness of communication is closely related to online disinhibition effect and advantages of anonymity, which in turn entail a lot of opportunities and high chances to succeed and get away with the crime.	The absence of face-to-face contact may disinhibit perpetrators and increase their willingness to engage in crime. Disconnectedness in personal communication, while online, transfers a person to an intrapsychic constellation, with inhibited guilt, anxiety etc. of the "in-person self", but not as part of that online self, that has similar implications as anonymity. It encourages fraudulent behavior, since it allows for remote "hit and run"

		and dehumanized interaction.

Thus, we hypothesize that:

H1: The more disconnected nature of personal communication the greater opportunity to engage in white-collar cybercrime.

3.2. Anonymity

The online environment involves anonymity and invisibility, which relate to online disinhibition, discussed before, and generally understood as the tendency to feel less inhibited and less concerned with the consequences of one's actions in the online world. A related concept is the electronic double. A person acting within cyberspace perceives oneself as a distinct person, a kind of digital personality instead of who he/she is in a real life, getting away from the unpleasant feelings about oneself acting as criminal (Gottschalk, 2010). The person in the physical space may be not the same as in cyberspace (Tosun & Lajunen, 2010). Consequently, the causation of crimes in cyberspace can be also explained by the nature of the behavior in the physical space versus cyber space, amplified by the online disinhibition effect. According to the space transition theory, developed by Jaishankar (2007), an individual behaves differently when he or she moves from one space to another. Some of the postulates of the theory are persons with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.

Cybercrime means no direct contact with victims and hence poses no physical danger or risk to be caught to its perpetrators (Sjouwerman, 2016). The most important and universal feature of cyberspace in that case is that such personality separation provides the opportunity to be anonymous, while anonymity gives an illusion of control and ability to hide one's personality from others (e.g., public, police, law). As a construct, anonymity is commonly thought of as the state of an individual who is unknown or lacks visible identifiable information that others can pick up on to determine an identity (Zimmerman, 2017). In terms of specific advantage for a white-collar criminal, it is not just an opportunity to stay unpunished, but it is ability to save his/her reputation, public respect (including

warm and respectful relation with family), high social status and all other privileges that define the position of white-collar persons.

Table 2: The effect of anonymity on the engagement in a crime by using technological means.

Fraud	Corruption	Theft	Manipulation
Most cases of cyber fraud (as CEO fraud and business email compromise schemes) entails not anonymity solely but identity flexibility and taking other's identity in order to pretend CEOs or other persons authorized for financial requests (i.e., requests to transfer the money).	In case of corruption anonymity is not supposed to play a significant role due to the nature of this criminal activity. The giving or receiving of an improper advantage is linked to a concrete person's position, office or assignment, which contradicts to concept of being anonymous (invisible and unknown).	The most frequent type of online theft is the identity theft, which in turn is a powerful cloak of anonymity for criminals and danger for national security (FBI, 2018). Some of the more prevalent schemes to steal identities include suspicious e-mail and/or phishing attempts to trick victims into revealing personally identifiable information. As in case of fraud, this entails fake identity of the email sender, which is more	In case of online manipulation (e.g., tax evasions) the role of anonymity has not been studied sufficiently, but an overall picture of the cybercrime allows to suggest that in that case offenders use anonymity benefits as much as they can.

		than just anonymous sender and a consequence of a developed ability to switch identities in cyberspace.	

Leader	Follower
Anonymity is equally beneficial for both roles of leader and followers, while the importance of being uncovered may be higher for leaders due to the higher risks involved for them.	Anonymity is equally beneficial for both roles of leader and followers, while the importance of being uncovered may be lower for followers due to the lower risks involved for them in case they are caught and are subjects to legal proceeding.

Occupational	Corporate
Anonymity of cyberspace is an attractive factor that almost guarantees to an individual that nobody will uncover his identity and therefore his position, reputation and personal relationships will be safe.	In terms of corporate crime, the value of anonymity is much higher, because it allows saving the reputation of a firm in a corporate world and the loyalty of customers to its corporate brand. On the other hand, as research states, criminals committing corporate crime often identify themselves with the company they represent, thereby changing the idea of anonymity to idea of identity flexibility in white-collar crime.

Threat	Possibility

Anonymity serves as a way to avoid a threat of financial and/or reputational failure and loss of high social status through avoiding risk to be caught and uncovered. Moreover, anonymity itself is an instrument that helps to avoid any failure through successful commitment of crime for rescuing white-collar's status qvo.	Anonymity is seen as possibility when it facilitates increasing personal or corporate wealth, although it simultaneously entails committing a crime.

Motive	Opportunity	Willingness
Anonymity is related to economic motivation of a criminal only indirectly. Since the main goal is to satisfy financial desires, anonymity is not the factor that makes motivation stronger but the factor that encourages engaging in a crime.	Maintaining anonymity or bogus identities during the commission of crimes is easier in virtual spaces than in real physical space. Apps, avatars, disposable devices, and the deep web - where search engines cannot detect websites due to an added layer of security - facilitate a concealment of criminal transactions, socialization into subcultures, and networking of those involved in illicit or nonconventional behavior (Stalans & Finn, 2016). Anonymity in more narrow sense provides opportunity to	Anonymity increases deviant behavior otherwise not expressed by white-collar criminals. The anonymity of the Internet and the possibility of adopting flexible identities can be incentives for criminal behavior (UN, 2015). Anonymous individuals will behave more aggressively than individuals who are not anonymous (Zimmerman, 2017). The increased level of aggression in cyberspace can be also explained by the online disinhibition effect (Suler, 2004). Moreover, some managers

	maintain occupational role of a white-collar criminal and continue using its privileges.	demonstrate narcissistic identification with the organization, that can in itself lead to a higher level of white-collar crime where criminals claim they are entitled to enrichment at the expense of the organization (Gottschalk, 2017).

Thus, we hypothesize that:

H2: The greater anonymity the greater opportunity to engage in white-collar cybercrime.

3.3. Geographical and timing distance

Universality of Internet provides an access across both distance and time in such a way that an offender has the potential to contact anyone, anywhere, anytime with no need to be at the same place and the moment of time with his/her victim (Gottschalk, 2010). This also saves the offender's efforts and resources, including psychological efforts of getting rid of guilty feelings. Due to ubiquity of Internet as a phenomenon, crime place extended beyond traditional boundaries and removed from temporal and geographical location. The universal advantage there is that committing crimes through the Internet lets criminals interact with potential victims from anywhere in the world, with no real-world contact needed, in a way that virtually guarantees preserving their anonymity (Sjouwerman, 2016). When applied for the white-collar offenders, spatial and timing separation plays as an extra opportunity to provide an alibi, get away from suspicions being physically absent at the moment when a crime occurs (e.g., an offender gets a chance to commit the crime while taking sunbathes on Bali as an innocent and reputable person). Moreover, this is an opportunity to defraud not only his own company, but also reach a wide pool of other organizations (e.g., suppliers, counteragents, etc.) located in other places/countries.

Table 3: The effect of geographical and timing distance on the engagement in a crime by using technological means.

Fraud	Corruption	Theft	Manipulation
In case of fraud (like in CEO fraud scheme) the absence of boundaries in terms of place and time is very convenient for criminals since allows them to manage the fraud process (sending e-mails, transferring money to foreign bank accounts) regardless their physical location, converting such well-known type of crime as fraud into totally cyber-oriented crime.	Ability to overcome geographical (and probably timing) distance may increase the range of potential corrupted relationships between both givers and receivers since they may be located in different regions and do not need to meet face to face in order to make a deal (or bribe); they can transfer funds or exploit money laundering through computer technologies, thereby expanding the corrupted network all around the world.	With regards to theft, the impact of geographical and timing distance may be described in general terms as facilitating crime through opportunity to steal identities while being located overseas, in comparison with traditional form of the same identity theft that involved physical theft of papers, ID cards, etc., and therefore entailed physical proximity to the objects of theft.	Manipulation as an ability to influence others' or one's own data (e.g., tax evasion) is indirectly influenced by geographical and timing distance between offender and his target, because it allows to have an access to the manipulated objects regardless the physical location of the attackers. It facilitates committing a crime but does not significantly change its nature.

Leader	Follower

The ability to overcome geographical distance is equally beneficial for criminals regardless their role	The ability to overcome geographical distance is equally beneficial for criminals regardless their role

Occupational	Corporate
For both types of crime, the opportunity to commit it beyond the physical boundaries of countries or regions is seen as attractive. In both cases physical separation of the offender from the victim creates an additional alibi when comparing with traditional crimes.	For both types of crime, the opportunity to commit it beyond the physical boundaries of countries or regions is seen as attractive.

Threat	Possibility
Geographical and timing separation serves as *a way to avoid a threat* of financial and/or reputational failure and loss of high social status through providing an additional alibi of being far from the place of crime. The geographical indeterminacy of the cyberspace will be eventually addressed and regulated by the authorities, making it more difficult to stay unnoticed.	Possibility to commit a crime across geographical boundaries is an opportunity to increase one's personal wealth through facilitating crimes towards victims which have been unreachable before due to their geographical location.

Motive	Opportunity	Willingness
Geographical and timing distance does not affect the	Physical separation from the victim is an extra opportunity to get away from suspicions being physically	The physical separation from the victim may have

financial motivation of an attacker.	absent at the moment when a crime occurs (commit the crime while taking sunbathes on Bali as an innocent and reputable person). Moreover, this is an opportunity to defraud not only his own company, but also to reach a wide pool of other organizations (e.g., suppliers, counteragents, etc.) located in other places/countries.	effects similar to the effects of the disconnected nature of communication (i.e. psychological separation). The absence of face-to-face contacts and the illusion that a crime takes place "somewhere far away" keeps the offenders' world perception intact, protecting from mental discomfort and a feeling of guilt. In fact, it is hard to assume that the above-mentioned benefits will reduce the readiness to engage in crime. However, there is no established evidence that these benefits directly influence their willingness. So, we assume, that the physical separation does not supposed

		to *change that willingness to commit a crime.*

Thus, we hypothesize that:

H3: The larger spatial and timing separation from victim and the less is the proximity, the greater opportunity to engage in white-collar cybercrime.

3.4. Network size effect

Cyberspace possesses characteristics of a network value chain and therefore creates a value for criminals. The sheer size of the Internet user community allows criminals to experiment with the types and methods of their scams (Sjouwerman, 2016). As the effect of network externalities involves (Stabell & Fjeldstad, 1998), the more people are connected to a network within the Internet, the more valuable the network is to each user. Therefore, the more victims are connected through computer or keep their data in computer, the more valuable the network is for offenders, since the number of their victims increases with every new user (Gottschalk, 2010). The specific advantage for white-collar criminals there is that for them it is not usual network of all computer users or companies, but it is access to a plenty of valuable assets, a specific network of the most promising (in terms of expected profit) victims. High occupational role of white-collar criminals is often a guarantee of having this special network and such accesses, and an offender may successfully exploit them.

Table 4: The effect of network size on the engagement in a crime by using technological means.

Fraud	Corruption	Theft	Manipulation
In case of cyber fraud, the more people are connected to a network within the Internet, the more potential	Since in most cases the act of corruption is oriented towards a unique, concrete person or object,	The ability to reach a large scale of objects for theft (such as others' identities),	In case of manipulation over some data or objects, the network size effect may make

victims of fraud there are. Using the same scheme (e.g., CEO fraud) several times on different victims, an offender due to the network size effect may easily amplify his future returns from his crime.	the ability to reach a wider range of similar persons almost does not make a difference in the case of a particular corruption act.	connected to the same network, increases the convenience (easiness) of committing the crime and therefore may positively affect the attacker's decision to engage in crime.	the online crime more attractive for a criminal but only in case the criminal may be interested in additional expansion of his illegal scheme over other subjects of interest.

Leader	Follower
Since in most cases the powerful occupational role of a criminal (CEO, top manager, director, etc.) coincides with his role in a crime as a head, mastermind or main executor of illegal activities, *the effect of network size will be more beneficial for leaders*. Leaders have greater access to specific data, networks, persons and other valuable assets, therefore may exploit the network size effect in the most profitable way.	Since in most cases the occupational role of a follower is not so high in terms of corporate hierarchy as the role of leader, *followers usually get fewer benefits from the network size effect* due to their limited accesses to networks as the range of important data, programs, persons and other valuable assets.

Occupational	Corporate
The personal network and accesses a criminal has may be less significant than the overall corporate accesses to specific and highly valuable business networks. Thus, in occupational crime the network size effect may be applied less efficiently than in corporate crime.	In case a person solely commits a crime aiming to satisfy his company's needs (e.g., avoid bankruptcy), the network size effects as attributed to the assets of this particular person will no differ with a case of occupational crime. However, if the company covers and/or facilitates committing such a crime, the network size effect may be greater due to the additional accesses and facilities the organization provides to a criminal who is "in charge" to commit this crime for the company's wealth.

Threat	Possibility
The network size effect may be seen as an additional instrument to avoid financial or social failure through amplifying the pool of future victims and gains of committing a crime.	Similarly, the network size effect indirectly influences the view to a crime as to a possibility to improve one's own wealth through amplifying the pool of potentially reachable victims and therefore gains of committing a crime.

Motive	Opportunity	Willingness

Making use of the network size effect enables offenders to make large profits from a number of small acts. Since their main motive is satisfy financial desires, the possibility to apply the same method for a large sample in a less costly and potentially highly profitable way, we assume that the network size effect may straighten the motivation to engage in cyber crime.	The ability to possess and utilize new network technologies is not restricted by education or income level. As a logical consequence of the widespread adoption of these technologies among increasing online population is the proportional increase in the number of opportunities to engage in a white-collar crime (Cliff & Wall-Parker, 2017).	The network size effect is not supposed to influence the criminal's predisposition for deviant behavior or their willingness to take socially unacceptable actions.

Thus, we hypothesize that:

H4: The larger the network size, the greater opportunity to engage in white-collar cybercrime.

3.5. Low cost standard

Internet and web tools are standards open to everyone, easy to use at a lower cost than earlier media. First, as Sjouwerman (2016) points out, until the Internet came along, committing such crime as scamming required significant effort and finesse to generate earnings while involving physical risk and close proximity to victims. In contrast, modern criminals need invest only small amounts of time and effort to run Internet scams, but they can easily gain thousands of dollars in return (Sjouwerman, 2016). Second, given the low-cost standard, access to Internet-enabled technologies is not limited to rich or well-educated people; universal technical standards of Internet connection give an opportunity to everyone regardless their social status and job position to have access to cyberspace (Gottschalk, 2010). This is reflected in organizational settings in a way that latest computer technology and facilitated access give equal opportunities in terms of allowing almost anyone in organization to engage in cybercrime (in contrast to top

managers with highest level of access and trust). Today an ordinary manager also may hack the system, take a privileged (in terms of access) position through deception and, e.g., steal the money. However, this implies a further discussion regarding the boundaries of social status of white-collar criminal and its tendency for democratization. In terms of white-collar specifics, two additional advantages could be identified there. First, low cost standard provides no need to attract additional funds for a crime, that means no suspicion in illegal use of funds from auditors, society or family in the future. Second, it also entails no need to acquire specific technical skills (that is an advantage in settings where top managers are extremely busy and do not have time for learning computer coding, programming, etc.) as well as no need to hire any external assistants. Today a manager can commit a crime by himself.

Table 5: The effect of low cost standard on the engagement in a crime by using technological means.

Fraud	Corruption	Theft	Manipulation
For online fraudsters low cost standard is very convenient characteristic of committing online crime since the distribution of the fraud scheme does not require additional instruments or resources.	In particular cases when the act of corruption takes place in cyberspace as a means of giver-receiver relationships, the low cost standard of maintaining such means may increase convenience of corruption but it is not its principal characteristic neither advantage.	Due to low cost standard online thefts become convenient crimes that does not require specific resources or knowledge. For example, in case of identity theft, the crime may be committed through available malware that will do all work for the criminal (e.g., key loggers, installed through a	Manipulation as an influence over certain assets or data requires specific competencies and skills by itself. The cyberspace costs of committing a manipulation (e.g., tax evasion) do not significantly affect the final costs of this crime, which

		malicious link, record the entered passwords from the victim's accounts).	may be considered as indirectly beneficial characteristics in terms of potential economy.

Leader	Follower
For both leader and follower type of criminal the low-cost standard is beneficial since it does not require specific skills and learning which are not always available for a white-collar criminal due to his busy work schedule. Neither it requires hiring external assistants which may uncover the criminal's intentions.	For both leader and follower type of criminal the low-cost standard is beneficial since it does not require specific skills and learning which are not always available for a white-collar criminal due to his busy work schedule. Neither it requires hiring external assistants which may uncover the criminal's intentions.

Occupational	Corporate
Regardless whether the main purpose of a crime is to satisfy personal or organizational needs, the benefit of economy of resources will be important for both occupational and corporate crime and true for cyber crime as well as for its traditional form.	However, in case a company is covering the illegal actions of its managers, low cost means less need to attract additional corporate funds for committing a crime, that in turn assumes lower risks during future financial audit.

Threat	Possibility

When a person engages in a crime in order to avoid financial failure or other risks, it usually entails certain financial or business problems. In that case the ability to reduce the costs involved by a crime is an attractive characteristic of cyberspace.	Low cost standard indirectly influences the attractiveness of engaging in a crime since it promises a possibility to increase one's own wealth or solve problems without additional costs and limitations involved.

Motive	Opportunity	Willingness
Low cost standard may only indirectly strengthen the criminal's motivation. Since the main goal is financial, the ability to reach it without additional costs may be considered as potentially attractive for cost-benefit calculations of the criminal.	Some time ago only a very few individuals had access to the means to commit many crimes. The number of workers employed in the service sector, including management, is increasing year by year. Almost a half of the total workforce is now in a position to sell trade secrets, embezzle funds, or commit other traditional white-collar crimes (Bureau of Labor Statistics, 2013; Cliff & Wall-Parker, 2017). This means two things: first, the network of persons which have manager and other influential position with consequent accesses and privileges for	Internet and web application are standards open to everyone, easy to use and inexpensive. Universal technical features of Internet and given the low-cost standard, might facilitate the willingness to engage in financial crime.

	committing a crime is increasing and expanding itself. Second, this network becomes more and more attractive in the eyes of an external criminal who is interested in gaining access and influence over this potentially profitable pool of victims.	

Therefore, based on what we already know we may hypothesize that:

H5: The lower costs the greater opportunity to engage in white-collar cybercrime.

3.6. No need for violence

Very different from the traditional form of theft (e.g. burglary), there is no need for physician violence involved in criminal actions performed by white-collar criminals over the Internet. Although psychological violence may be present in some of the white-collar criminal cases, typical cases of such criminals can be characterized as charming and charismatic. Violence is usually associated with criminality, while the absence of violence makes an illusion that committed offense is not a crime or at least is not a serious crime. When applied for white-collar criminals, the specific advantage there is that in public perception any type of violence is not associated with a perfect black suit of a top manager. The image of white-collar criminal as well as his/her behavior does not involve any violence, i.e. a perfect gentleman or lady cannot commit any cruel crime. Therefore, the fact that cyberspace reduces physical violence to zero is convenient for psychological state of the criminal, because it decreases chances of ending with a cognitive dissonance in his/her mind in case any cruelty took place.

Table 6: The effect of no need for violence on the engagement in a crime by using technological means.

Fraud	Corruption	Theft	Manipulation
Both traditional and cyber forms of fraud do not involve any physical aggression or violence towards their victims, since the main goal of a fraud is to deceive others in an invisible way.	The mechanism of corruption is often based on offering and receiving additional services in order to convince another party or to enrich oneself by providing not allowed officially services. The scheme almost always assumes mutual desire to interchange services and bribes with no need for violence. *Cyberspace does not affect the degree of violence in that case*.	Traditional forms of theft (e.g. burglary) involve physical and psychological violence to a certain degree, while *in case of cyber theft (e.g., identity theft) there is no need for any physician actions* associated with aggression.	Manipulation entails some extent of influence over others' activities, means and results, which in turn in some cases makes a room for some degree of violence (including physical aggression in face-to-face communication) in process of acquiring others' results and establishing control over them (e.g, over auditors books or taxes). *Cyberspace reduces to zero any need for violence* in that case. Still, the *psychological type of violence* towards the victims may remain.

Leader	Follower
Existing research *does not distinguish* between the importance of zero violence for both leader and follower types of criminals in both traditional and cyber forms of white-collar crime.	Existing research *does not distinguish* between the importance of zero violence for both leader and follower types of criminals in both traditional and cyber forms of white-collar crime.

Occupational	Corporate
Zero need for violence makes *attractive any type of crime regardless* whether they satisfy personal or organizational needs and whether they are committed in traditional or cyber form, because non-violent crime will always be convenient in terms of lower risks of potential reputation damage and severe punishment.	Zero need for violence makes *attractive any type of crime regardless* whether they satisfy personal or organizational needs and whether they are committed in traditional or cyber form, because apart of being non-violent, white-collar crime appears to be victimless, too, and this appearance is not considered as dangerous for or destroying the image of a company or its corporate values and reputation.

Threat	Possibility
Zero need for violence only *indirectly* relates to the avoidance of financial failure through justification of the means of this avoidance as non-violent and/or victimless (denial of the victims, (Sykes & Matza, 1957)).	No need for violence *indirectly* influences the attractiveness of possibility to enrich oneself or to improve personal wealth through promising (although delusionally) no victims, no punishment and no cognitive dissonance between proclaimed values and actual actions.

Motive	Opportunity	Willingness

Non-violent nature of cybercrime is related to economic motivation of a criminal *only indirectly*. Since the main goal is to satisfy financial desires, zero need of violence is not the factor that makes financial motivation stronger but the factor that encourages engaging in a crime promising no economic consequences (in terms of losses of punishment) for desire satisfaction.	Opportunities in the organizational dimension revolve on how crime can be committed conveniently (Gottschalk, 2017). This observation may be interpreted as the absence of any aggressive actions that can attract the attention of undesirable witnesses and disturb the convenient conditions for committing a crime. However, one should remember that *both forms of white-collar crime* (traditional and cyber form) suggest non-violent context, so in fact there is *no specific influence of zero violence to cyber crimes.*	In criminology, psychology and world culture there is an axiom that violence (begets) breeds violence. The nature of cybercrime suggests there is no violence in contrast to some traditional forms of crime. People may *more willingly engage into the crime* when they are convinced that committed offense is not a crime or at least is not a serious crime due to the absence of visible damage or victims. This neutralization technique is called *denial of victims* (Sykes & Matza, 1957). Moreover, it keeps white-collar respectable persons from cognitive dissonance issues and bad conscience.

Thus, we hypothesize that:

H6: The less need for violence the greater opportunity to engage in white-collar cybercrime.

3.7. Weak legal regulation

Current legal system provides an example of a stimuli for a white-collar criminal to commit the crime. There are many differences between cybercrime and the conventional crime both in committing the crime and prosecuting it. Tracking,

catching and prosecuting cyber criminals within the current legal system is very difficult. The speed at which new technologies are developed requires a choreographed nimbleness that legislative deliberation may not be able to deliver on a global scale: national laws may utilize different standards for conviction and impose different punishment; computer crime in more industrialized nation will have greater ramification than in a less industrialized nation; laws amendments done by developing countries may still lack the clarity that the industrialized nations desire. Moreover, in confronting the rising phenomenon of computer crime, strategies that focus solely on increasing the effectiveness of prosecution will inevitably fail (Lewis, 2004). In terms of *specific advantages for white-collar crime* weak legal regulation can be viewed from two perspectives, where each of them increases effects of another. First, when addressing financial (economic) crimes in comparison with robbery or murder, the position of law is often considered as very indulgent or even forgiving (detailed cases and exceptions will be discussed in the empirical part of this study). Privileged position of white-collar criminals often allows them to get away with the crime. Second, cyberspace provides many opportunities to stay uncaught, thereby increasing their chances to stay unpunished. The legal regulation of cybercrime is unclear and weak. Moreover, even compared with other cybercrime (state espionage, "pure" hacking), financial crime gets less attention and sometimes does not involve severe punishment even when the attackers have been identified.

Table 7: The effect of the weak legal regulation on the engagement in a crime by using technological means

Fraud	Corruption	Theft	Manipulation
When addressing any category of financial (economic) crimes in comparison with robbery or murder, the position of law is often considered	Crimes that are viewed as benefiting the company at the expense of external parties, or are seen as victimless, usually *get less severe*	The most prevalent type of online theft is identity theft. Although the overall state of cyberspace regulation is unclear and	As for manipulation, only the average assumption of legal weaknesses in cyberspace may be applied due to the *limited data of online*

as very indulgent or even forgiving. Given the difficulty to track the perpetrator online, *cyberspace increases the chances to get away with the crime*. Cyber fraudsters use fake identities and advanced money laundering schemes launched by criminals as soon as the funds have been transferred to the fake account (e.g., as in CEO fraud scheme), when even banks themselves cannot track the whole path of money transfer.	*punishment*. Corruption is often seen as helping companies to compete and generate sales in countries where laws are unenforced, at the expense of taxpayers or customers (Healy & Serafeim, 2016). Since it is a quite difficult to establish a fact of committing corruption online, the general implication of law interpretation in case of corruption may be expanded on the online corruption cases, too, combined with advantageous difficulty for prosecutors to track illegal activity in cyberspace.	varying in different regions, theft as a crime usually occurs as a part of a more serious crime where theft is only beginning or foundation for further illegal actions with property stolen (e.g., with person's identity). Therefore the average *punishment for crimes containing theft as part of them is considered to be more severe.* However, the *difficulty to trace back the criminals due to their anonymity compensates the rigor of the law*.	*manipulation cases*.

Leader	Follower
The privileged position of a white-collar crime assumes that in case he/she has an place in top team management, his/her *chances to get away with the crime will be greater.* Similarly, it is logically to assume that when a white-collar holds a top position, he/she often plays the role of criminal leader in illegal activities. Thus, one can suggest that *leaders have greater chances to escape the punishment mostly due to its privileges and not to the current gaps in cyberspace regulation.* An additional insight concerns the gender of a criminal. As a study shows, *senior male executives receive lighter punishments* than female peers. Moreover, senior executives receive even lighter punishments when the firm has detected multiple crimes during the past year instead of only one case (Healy & Serafeim, 2016).	Followers are less frequently used and/or described in research types of criminals than leaders. As Ketil Arnulf & Gottschalk (2012) state, followers are non-assertive persons, convinced by cause of the crime or charisma of their leaders or just following the orders. This means that while weak law regulation of cybercrimes provides equal advantage for leaders and followers, the social status and position of the latest may be not so high as position of their leaders. They have lower chances to get away with the crime due to fewer privileges in eyes of both company owners and society. Thus, the *weaknesses of law in cyberspace does not significantly change the degree of follower's punishment* but their lower hierarchy position does change their chances in an unfavorable direction.

Occupational	Corporate
In terms of corporate regulation of employees misconduct, executives may be concerned about the risk of regulator and the public overreaction if the incident becomes public. As a result, they may decide that it would be more harmful for shareholders to pursue legal redress against senior perpetrators	Withall mentioned regarding occupational crime, when the investigation is initiated by the owners of a company, punishments are even *less severe if the perpetrators' crimes could be rationalized as being for the benefit of the firm*, rather than where he/she has directly stolen money from

given the risks of public disclosure. Moreover, since senior executives are typically more costly to replace than other employees, companies understand the costs of lost productivity and replacement and therefore may be *less likely to dismiss high-performing senior perpetrators even after their crimes* (Healy & Serafeim, 2016).	the company itself (Healy & Serafeim, 2016).

Threat	Possibility
Weak law regulation serves only as an *indirect means* to avoid a threat of financial and/or reputational failure and loss of high social status through reducing or even avoiding risks to be severely punished.	Weak regulation may be seen as *possibility* when it facilitates increasing personal or corporate wealth without any punishment for illegal actions.

Motive	Opportunity	Willingness
Weak law regulation is related to economic motivation of a criminal *only indirectly*. Since the main goal is to satisfy financial desires, cyberspace laws is not the factor that makes motivation stronger but the factor that encourages engaging in a crime promising no punishment for desire satisfaction.	*Privileged position of white-collar criminals often allows them to get away with the crime*. They are reputed, well-known persons with a significant weight in the society. Compared with other crimes and even cybercrimes (state espionage, "pure" hacking), financial crime in both forms (traditional	The Internet facilitates deviance and crime through providing visibility and accessibility to alternative justifications and normative viewpoints on forms of cybercrime. The fragmented and layered nature of the Internet further stimulates deviant and criminal activity as

	and cyber) gets less attention and sometimes does not involve severe punishment for offenders due to their privileged position even when the attackers have been identified. *The opportunity to get away with the white-collar crime vary depending on the national laws and development of the legal system*, while in less developed and more corrupted states this opportunity is greater (e.g., the case of Evgeniya Vasilieva in Russia).	there is *no centralized government body to establish the norms for appropriate conduct* and to enforce criminal laws in specific countries. Unlawful behavior in some countries is tolerated and legal behavior in other countries, allowing offenders to choose jurisdictions for their websites that have the least harsh legal consequences (Stalans & Finn, (2016). Moreover, offenders may use *neutralization techniques* (denial of injury, denial of victims) in order to convince themselves they are behaving within socially accepted norms (Sykes & Matza, 1957).

Based on all these factors, we hypothesize that:

H7: The weaker the law regulation in cyberspace the greater opportunity to engage in white-collar cybercrime.

Thus, on the basis of the literature review, we have identified seven characteristics, that according to our hypothesis, make online white-collar crime more attractive. Later, we will also interchangeably refer to these characteristics as

seven factors that influence engaging in cybercrime. Below Table 8 summarizes these characteristics (factors).

Table 8: Factors influencing the opportunity to engage in cybercrime

disconnected nature of communication
anonymity
geographical and timing distance
network size effect
low cost standard
no need for violence
weak law regulation in cyberspace

In continuation of formulation of the hypotheses, we perform an empirical study where through analyzing both primary and secondary data i.e. practical evidence and expert opinion, we conclude whether they are supported or rejected.

Chapter 4. Methodology

4.1. Introduction to the chosen method

As Bethune (2015) states, researchers in the field of white-collar crime have an arsenal of research methods including: surveys; interviews; case-study, media and statistical analyses; historical, victim and offender accounts; experiments and participant observation. However, any method always has its own strengths and weaknesses, and addresses very specific aspects of the topic. Moreover, it is very difficult for researchers to obtain empirical evidence from convicted white-collar criminals or get an access to white-collar crime environments due to the necessity to keep confidentiality of the data while any method of research in white-collar crime will inevitably involve compromise (Bethune, 2015; Gottschalk, 2017).

Even more, there is often a sampling problem. The issue is that the offenders "available" for research (i.e. incarcerated) represent a very small subset of white-collar criminals, because most of the offenders still being unpunished. Since gaining

access to these subjects remains problematic, researchers may expand the offence based of their study aiming to generate a sufficient sample size meanwhile raising questions regarding its representativeness (Bethune, 2015).

In this study, we will consider three research methods: secondary data, surveys and interviews. Secondary data research aims to produce new results by analyzing the primary data collected by other researcher in a new way (Bethune, 2015). However, it also means relying upon the quality of this primary data that may affect the interpretation of the results. Therefore, in the first part of this paper we apply secondary data analysis when we refer to crime statistics, companies' reports and the scope of academic articles. Next, we collect the available information about CEO fraud cases published in journals and online and analyze them in order to find common patterns in the behavior of cyber offender's aiming to support or reject the hypotheses mentioned above. Nevertheless, we use secondary data only as an illustration of how the hypothesized advantages of committing cybercrime unfold in practice (e.g., in the real case of crime). The CEO fraud cases and in particular the AFGlobal Corp. case, discussed below, serve as an illustration and an important source of secondary data. However, the primary data remains more valuable source of information for this thesis, and in the coming part of the paper we look after direct confirmation or rejection of our hypotheses.

In contrast to secondary data, obtaining primary data from offenders themselves through interviewing them is one of the most popular and useful research methods in the field of criminology and in particular white-collar crime. The typical scheme of work entails conducting in-depth interviews with incarcerated offenders asking them about the circumstances of their offending, their motivations at the time, and their reflections upon the case (Bethune, 2015). However, the interpretation of the results should be carefully reviewed. There is an opinion that offenders are likely to portray themselves as decent moral people despite their wrongdoing, and that this is more the case with white-collar crime (Klenowski et al., 2011, cited in Bethune, 2015). Moreover, keeping in mind the sampling and access problems, face-to-face interview with criminals becomes a substantial challenge for researchers.

According to Bethune (2015), another common research method, both in the field of white-collar crime and in criminology in general, is a survey. Survey resembles the same interview only in its standardized form with structured questions with no room for change of question, usually performed via telephone or

email. However, in adopting survey-based approach to research, scholars once again should make sure that the survey questions are appropriately formulated and addressed to the right sample of population.

Therefore, we have decided to leave interviewing of the incarcerated offenders to further and more elaborated research and focus on interviewing from other perspective of white-collar crime, namely from the perspective of the experts in the field of financial crime, cybercrime and cybersecurity. We created and distributed a survey among the selected experts on the field of interest in order to find out their opinion regarding what is so special in committing white-collar crime in cyberspace. Therefore, we used an interview as a method of data collection. In general, the design of our work corresponds survey research, which comprises "a cross-sectional design in relation to which data are collected predominantly by questionnaire or structured interview on a sample of cases drawn from a wider population and at a single point in time in order to collect a body of quantitative or qualitative data in connection with a number of variables, which are then examined to detect patterns of associations" (Bryman, 2016, p.54). Since the results have been analyzed and interpreted via displaying the distribution of answers in the bar charts, we understand the research design of this thesis in terms of qualitative cross-sectional interview study.

Cross-sectional data can be conducted using any mode of data collection, including surveys, questionnaires and interviews (Bryman, 2016). Therefore, throughout the text of the paper, and addressing the methods of data collection, we will also refer to the design of this work as expert survey or structured interview.

4.2. Secondary data analysis

By secondary data analysis we refer to crime statistics, relevant companies' reports and the scope of academic articles. We address this data through the analysis of available information via printed material (books and newspapers), online databases (BI library portal) and other Internet platforms (Google and Google Scholar). We aim at finding common patterns in the context of committing cybercrime and offenders' behavior in order to support or reject the hypotheses.

A major advantage of using this type of data is the breadth of available information. Another advantage of using secondary data corresponding our subject is that the data collection process and research presented in scholar articles possesses a high level of expertise. For example, data collection for statistical data

is often performed by staff members who specialize in certain tasks and have many years of experience in that particular area. Moreover, many of these data sets are longitudinal, which allows us to review the changes of phenomena of white-collar crime and white-collar crime in cyberspace over time.

However, there are several disadvantages of using secondary data sources in our research that we would like to acknowledge. For example, despite the fact that a lot of information is readily available on the Internet, as in the case with crime statistic and company reports, still a lot of criminal justice data is hard to come by. It can be difficult to understand, unavailable due to identity protection issues or currently unavailable. A related problem is that the keywords for searching for the information on the Internet may have been defined or categorized differently by different researchers. Moreover, in the absence of the common language and having many definitions in use related to the white-collar crime phenomena, makes it difficult to compare data gathered by different white-collar crime stakeholders.

Withal, we would like to note, that we use secondary data as a foundation for our research and as an illustration of how the hypothesized advantages of committing cybercrime unfold in practice. For instance, the CEO fraud cases and in particular the AFGlobal Corp. case, discussed below, serve as an important source of secondary data and an elucidation, demonstrating common traits for succeeding in such type of crime.

4.3. Primary data analysis

The primary data for this research has been obtained through interviewing a group of independent and acknowledged experts in the field. We have implemented an extensive search and have found (via academic publications, university and business school webpages, LinkedIn and personal recommendations) several experts in such topics as white-collar crime, financial crime, cybercrime, cybersecurity, corporate security.

The expert interview as a "streamlined" method of qualitative empirical research, designed to explore expert knowledge, has long been popular in social research (Meuser & Nagel, 2009). Experts are defined as "people, who possesses special knowledge of a social phenomenon which interviewer is interested in, and expert interviews as a specific method for collecting data about this social phenomenon" (Bogner, Littig & Menz, 2009, p.117). The advantages of applying this method are undeniable: it is more efficient and concentrated method of

gathering data and they are useful in situations in which it might prove difficult to gain access to a particular field (as in the case with white-collar crime). Furthermore, it is evident that expert interviews offer sufficient means in quickly obtaining reliable results. Finally, a shared understanding of the social relevance of the research coupled with professional curiosity about the subject make it comparatively easy to motivate the experts to participate in such interview. (Bogner et al., 2009)

However, as far as the expertise is concerned, recent social science research is currently rethinking what really constitutes an expert, as a source of objective information; and what kind of ethical dilemmas might underline the method. In order to avoid the bias, this confirms a need for an increased transparency and simplicity in application of the method; and reflection on the interview itself.

In our context, the success of interview-based research considerably depends on the quality of the interviewees, i.e. on the extent to which they meet our selection criteria. We expect respondents to "speak the common language" and understand what kind of information we need. We also hope the interviewees to be able to provide additional information and own opinion on the subject. Withal, we have created and distributed a survey among 65 pre-selected experts on the field of white-collar crime, financial crime, cybercrime, cybersecurity and corporate security in order to find out their opinion regarding what is so special in committing white-collar crime in cyberspace. In our case, the interview type was the structured interview with an identical set of questions for each participant. Since some experts were located overseas (e.g., in U.S. or Russia), we used electronic means for interviewing (the Qualtrics survey product) in order to overcome geographical distance and time separation. The design of answers entailed evaluation on the degree of experts' agreement with seven suggested statements on the Likert scale. Likert scale is a popular evaluation method used in cross-sectional research design (often referred to as social survey), which measures participant's opinion on 7-point scale from "strongly disagree" to "strongly agree" options. The nature of Likert scale instruments is quantitative; however, they can be analyzed both quantitatively (through inferential and robust statistical tools such as ANOVA, MANOVA, and COVAS, regressions, path analysis, SEM, etc.) and qualitatively (through frequencies and percentage analyses).

The objective of the following chapter is to present the results of secondary and primary data analysis in detail. First, we will use the CEO fraud scheme in order

to exemplify how do the Internet characteristics enact on a concrete example. However, this illustration is not enough to make valid conclusions. Therefore, we have performed an expert interview and asked their opinion regarding the vitality of the above stated hypothesis.

Chapter 5. Research results

5.1. Sketch for the chosen crime type

According to the FBI's Internet Crime Complaint Center (IC3, a partnership between the National White Collar Crime Center and the FBI), online extortion, tech support scams and business email compromise (BEC) were among the most costly cyber scams in 2016. As FBI (2017a) reports, in 2017 the top three crime types with the highest reported loss were BEC, confidence/romance fraud, and non-payment/non-delivery. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses from BEC. The scam has been reported in all 50 states and in 150 countries (IC3, 2018). The IC3 states that they received more than 12 000 complaints about so called CEO fraud attacks, a form of BEC fraud, which resulted in total loss of more than $360 million in 2016. At the same time, the IC3 points out that victims hardly report such crimes to police or make them publicly known, and one may assume that only 15% of the victims actually inform about their losses. Theoretically, after applying 15% as a percentage of potentially 100% cases, the amount of losses arises from $360 million to potential $2.4 billion, consequently highlighting the extent of the damaged caused. As FBI (2017b) claims, business email compromise has affected organizations from non-profit associations to large corporations as well as religious and educational systems. While the information security world focuses on technical vulnerabilities and exploits (e.g., malware and hacking), there is one kind of attack that is rapidly increasing, defrauds organizations out of millions of dollars every year and requires often no more than a tool with which we are all familiar – email (Mansfield-Devine, 2016). Due to vast geographical distribution and significant economic loss as an estimated consequence, we will choose business e-mail compromise scheme, and more specifically CEO fraud, as an example of financial cybercrime.

5.2. Introduction to the CEO fraud scheme

In line with FBI's definition, business email compromise is a form of a sophisticated financial scam, targeting businesses working with wire transfer payments (usually to foreign suppliers). In the typical CEO fraud scheme, an offender sends an email to a victim inside a target organization, where he pretends to appear as the organization's CEO, CFO or any other top manager and asks to transfer immediately some money to an outside (e.g., foreign bank account) recipient. In order to make the victim believe that this is CEO who is asking, the offenders use deception techniques. Usually, they gain access to an organization's network through social engineering or the use of malware, where they study the target's contacts, billing systems, CEO's style of communication, his/her hours of work and other HR and finance-related practices within the organization. Often when the CEO is away from the office, the criminals send a request to a targeted employee in the finance department for an immediate wire transfer to a known and trusted vendor or supplier. The account seems to be familiar, but the account numbers are slightly different. The criminals usually spoof email accounts, adding slight variations on legitimate corporate addresses (e.g., an.example@bi.no vs an.exampl@bi.no) in order to fool the victims and make them believe that they are corresponding with the genuine managers.

The main problem with CEO fraud is that if the scam is not discovered in time, the money is hard to trace and recover due to the advanced money laundering schemes launched by criminals as soon as the funds have been transferred to the fake account. For example, Pomeroy Investment Corp (US) has lost $495 000 with the error being unnoticed for the whole 8 (!) days (KrebsOnSecurity, 2016). Moreover, FBI (2016) notes that the goal of business email compromise scams may not always be the transfer of funds. Sometimes the scam includes the compromise of legitimate business email accounts and requests for personal identity information or is designed to obtain wage and tax information from an HR manager. For instance, in 2017 Campbell County Health (US) has lost almost 1500 employees' social security numbers due to this scam scheme. Even further, as an article in Trustwave (an international security services company based in US) warns, CEO fraud may point to infect a target's computer network with a malware, pretending to be an image or document with bank account description or other relevant financial information, which in practice is a command to download a malicious data stealing program executable from an external link (Trustwave.com, 2016).

According to Mansfield-Devine's (2016) categorization, based on FBI's typology, BEC can be divided into five main fraud schemes: bogus invoice scam targeting business working with a foreign supplier; request for a wire transfer from a fake CEO; fraudulent payment requests through compromised employees' email; executive and attorney impersonation handling confidential issues and asking for secret funds transfers; data theft (sensitive information requested from HR or finance departments).

There are many cases where criminals have succeeded and the requested funds have been transferred to their accounts. The table below is based on open-source information and presents some of such cases and also contains estimated loss of fraudsters' actions:

Organization	Loss	Description
Ubiquiti Networks	$46.7 million	Employee emails impersonated, and money transferred to overseas accounts held by third parties. The company recouped about $15 million
SS&C Technologies Holdings	$5.9 million	A spoofed email, claiming to come from the CEO, requested that accounting transfer money to a foreign account for a fake acquisition. The scam emails added an extra "L" to Tillage as in Tilllage and contained unusual syntax and grammatical errors. Although the company recovered some of the funds, the CEO lost his job.
Xoom	$30.8 million	Employee impersonation and fraudulent requests to the finance department. The CFO resigned.
Mattel	$3 million	A transfer to an account in China after receiving a spoofed email from the CEO. Thanks to little time elapsed after the incident, the bank in China still had the funds and returned them to Mattel.

Pomeroy Investment Corp	$500 000	The email account of a CEO has been hacked. The error was noticed eight days after it took place, and the money was long gone.
Leoni, AG	$44 million	Emails like legitimate payment requests from the head office in Germany, asking for the money to be sent from a subsidiary in Romania. The offenders had extensive knowledge about the internal procedures for approving and processing transfers at Leoni.
Etna Industrie	$542 000	A series of spoofed emails and phone calls from CEO's address and a fake lawyer consultant requesting several wire transfers. Later three transfers were recovered.
FACC Operations GMbH	$54 million	The offenders targeted financial department and under CEO's name requested several wire transfers. No malware has been found. CEO and CFO were fired. FACC's share price had fallen 38% since the incident. Some funds were recovered.
Medidata Solutions Inc.	$4.8 million	A company employee under instruction of fake CEO and attorney wired money to a Chinese bank.
AFGlobal Corp.	$480 000	A series of spoofed CEO's emails with phone calls from a fake lawyer made the director of accounting in 30 minutes send money to a Chinese bank. When a new request for $18 million has appeared, the director alerted the officers. Still, due to long time, money was gone.

Table 9: Brief overview of several criminal cases including estimated loss
Sources: CEO fraud manual, KnowBe4 Inc. (2016); BBC, (2016); FACC, (2016); KrebsOnSecurity, (2015, 2016)

These ten episodes are just the latest and the most known cases of CEO fraud made available to the public. The problem with this type of crime as well as other financial crimes against a corporate property is that most of the victims prefer

to hide such incidents in order to avoid rumors potentially damaging their reputation and affecting the stock price.

Although crafted to trick distinct companies, business email compromise crimes demonstrate some common traits or prerequisites for succeeding in such type of crime. As an exemplification with regard to the CEO fraud, we decided to chose the AFGlobal Corp. case in order to assess the specifics of CEO fraud and apply the hypotheses in order to see whether our theoretical assumptions fit the practical evidence.

5.3. The AFGlobal Corp case

The available information indicates that May 21, 2014 AFGlobal's director of accounting Glen Wurm received a series of emails from someone pretending to be Gean Stalcup, the AFGlobal's CEO. The text of his message is cited here as it has been published by KrebsOnSecurity (2016): "Glen, I have assigned you to manage file T521. This is a strictly confidential financial operation, to which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)? This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do not speak with anyone by email or phone regarding this. Regards, Gean Stalcup." Roughly 30 minutes later, Glen Wurm was contacted via phone and email by Steven Shapiro stating that due diligence fees associated with the China acquisition in the amount of $480 000 were needed. Glen Wurm wired the funds as requested to an account at the Agricultural Bank of China. In one week, the faked CEO acknowledged receipt of the money and asked Wurm to wire an additional $18 million. However, Wurm became suspicious after that request and called for an officer. After realizing what has happened, the company attempted to recover the funds, but by that moment the money was already gone. Moreover, the insurance firm has also denied to recover the losses, arguing that the CEO fraud does not involve the forgery of a financial instrument as required by the policy (KrebsOnSecurity, 2016).

The case described above is a typical scheme of the well-known business email compromise. Still, this is the case where the offender won. What makes victims to fall into the trap? As Mansfield-Devine (2017) notes, most people only need a few convincing details to believe that an email is legitimate. Thus, we will assess the impact of several factors which affected the human behavior in AFGlobal Corp case through the opportunity perspective used as theoretical framework for

this thesis. These factors fall into two categories: universal features and cyber-specific features.

5.3.1 The impact of universal features

First of all, attackers perform a sophisticated work in terms of using power and persuasion techniques. They often imply one of the Cialdini's principles - the principle of scarcity, which in these settings is a sense of urgency and limited time given for an action. Scammers manipulate reliable staff to act rapidly by using such phrases as "code to admin expenses," "urgent wire transfer," "urgent invoice payment" and "new account information" (KnowBe4, 2016). They pressure a victim to act quickly and without thinking whether something is unusual, falling them back on earlier learned responses to crucial situations. Such regression under stress to first learned behavior is a known phenomenon in organizational and psychological research (e.g., Barthol & Ku, 1959; Weick, 1990). In case of AFGlobal attack, the criminals gave to Glen Wurm no more than 30 minutes between the first email and a phone call from a false attorney with transfer instructions. Fraudsters combine urgency with the sense of secrecy, asking their targets to be silent and keep communicating only with them, as they have requested from the AFGlobal's director of accounting. Many business processes are based on the implicit trust, and this is something that is successfully exploited by criminals (Mansfield-Devine, 2016).

There are also cultural and personality factors affecting the result of CEO fraud. According to Hofstede's power distance dimension of national culture, people in societies with high level of power distance accept a hierarchical order, where less powerful members of a community do not need further justification accepting the obedient position (Hofstede, 2011). High power distance is likely to have a place in Russia and China (93 and 80 points out of 100), is also present in such European countries as Belgium and France (65 and 68 points) while in Norway, UK and US this dimension shows significantly lower scores (31, 35, and 40 points, according to Hofstede Insights (2018)). In a country with a higher power distance an employee is more likely to blindly obey the demands of his/her boss than in a country with more equal power distribution.

Next, an individual's readiness to obey may depend on personal traits. Offenders are taking an advantage of human nature and gullibility, claims Sjouwerman in his book *Cyberheist* (2016). They exploit human emotional

vulnerabilities in order to pull off all types of scams. Even smart professionals and savvy investors can be fooled by complex math, exaggerated returns, and manipulative pitches (Sjouwerman, 2016, p.40). Moreover, such personal characteristics and attitudes as extroversion, gullibility, high risk tolerance and blind trust (naivety) increase a person's susceptibility to fraud (Greenspan, 2008).

Nevertheless, urgency, secrecy, exploitation of emotional vulnerabilities and break of trust are features associated with persuasive tactics of criminals regardless the space of crime commitment (physical or cyberspace). Therefore, now we ask what are the advantages of committing CEO fraud online which are unreachable otherwise?

5.3.2 The impact of cyberspace opportunities

The key to CEO fraud is the ability to fake one's identity while hiding his/her own. This ability is rooted in the separation of personality and creation of the electronic double of a person which is distinct from his physical personality. Cyberspace, in contrast to physical space, provides an opportunity to achieve it through simple means (e.g., using similar email address or gaining access to corporate communication network). The offender(s) in AFGlobal case could both create a fake yet realistic identity of CEO and simultaneously hide their own personality. In case of this type of fraud the creation of electronic double is essential requirement for success. This is in line with our hypothesis (*H2*) claiming that greater anonymity (e.g., gained through taking other's identity) provides greater opportunities to engage in cybercrime, making committing a crime an attractive and convenient option for potential criminals.

A related concept is the disconnected nature of interpersonal communication within cyberspace. When an offender communicates to his victim through sending emails, he may perceive this act not as a conversation with other person, but only as a technical means to achieve his goal (steal the money). The interaction with victims in cyberspace is not the same as interaction with a human in real-life settings, where face-to-face form of communication and physical actions towards a victim may rise undesirable psychological states for the offender (e.g., feeling of guilty when robbing another person). In cyber form of such an interaction the guilty feeling may be reduced as victim is not perceived as a real person. Experts argue that individuals who make unethical use of computer networks do not really perceive the ethical implications of their actions (Kallman & Grillo, 1996; Kshetri,

2010). However, as cyber offenders are seldom identified and consequently caught, researches have a very limited ability to interview them about their psychological states. Thus, the correlation and causal relationships between the disconnectedness of interpersonal communication and the willingness to engage in a crime are still on the level of hypothesis (*H1*) with a need for further assessment.

Cyberspace connects different physical locations all over the world. The most popular targets for BEC-based frauds are US companies while the accounts for wire transfers are usually open overseas - in Asian banks (Chinese bank in the AFGlobal case). Regarding potential geographical location of the criminals, Mansfield-Devine (2016) notes that although cyber attacks tend to be perpetrated by known hackers' groups from Russia, China or Brazil, CEO frauds can come from almost anywhere. If someone is about to commit a CEO fraud there is no need for geographical proximity to his victims due to stable Internet connection which is present in most of countries. So, cybercrime becomes a convenient option. However, in terms of timing there is an important requirement. The offenders' pressure the victims to respond quickly and therefore they should be ready to send further instructions as the victims begin to respond or react to the victim's behavior in another way. Thus, the time is limited and for victims it takes no more than 1-2 hours to fulfill the requirements of a fake CEO. Moreover, a CEO's email sent during unusual time period or without adjusting appropriate time zone (e.g., at 3 a.m.) may engender suspicions and undermine offenders' attempts. Therefore, in case of CEO fraud, our hypothesis (*H3*) stating that greater geographical and time separation facilitate committing a cybercrime is supported only in terms of a broader geographical location as a cyberspace advantage for criminals.

Another key advantage given by cyberspace is the low cost of committing a crime, in particular in case of business email compromise. The level of technical expertise required to conduct an attack is low comparing with hacking or espionage, because all an offender needs is to demonstrate a reasonable level of competence at reconnaissance and social engineering and have an ability to manipulate email address (Mansfield-Devine, 2016). The offenders learn information from social networks (e.g., LinkedIn, Facebook) and corporate pages, examining comments and studying the manner of interpersonal communication of their victims. Sometimes they deploy malware (e.g., keyloggers) to steal login credentials or buy this data in the dark web. Too often, employees use their company login details to register on sites which then become breached and their databases are sold online (Mansfield-

Devine, 2016). As a consequence, low cost standard for entry into criminal activity widens out the pool of people from technically advanced criminals to more traditional fraudsters who may not have that technical expertise. In case of AFGlobal fraud, the offenders have used only email communication and made a phone call from a false attorney. Universal technical standards of Internet connection provide an opportunity to everyone regardless their social status and job position to have access to cyberspace, which makes cybercrime a convenient option for criminal minds. This supports our hypothesis (*H5*) that lower costs increase the opportunity to engage in crime. However, at the same moment the definitional challenge of white-collar crime arises again.

White-collar crime as a phenomenon assumes that offenders occupy a significant position within organizational hierarchy and take an advantage of their positions in order to satisfy their need through committing financial crime. The key distinction there is their profession/position which is considered to be the main differentiating factor from blue collar criminals from lower social classes. However, the personality of offenders in case of CEO fraud is rarely known. On the one hand, there are suggestions they are internal offenders or at least have an insider within the organization attacked. As Mansfield-Devine (2016) says, the more the attacker knows about the target company, the more the CEO fraud is likely to succeed, and an inside offender is not beyond the bounds of possibility. For instance, in case of AFGlobal Corp., the criminal seemed to know the normal procedures of the company and also that Gean Stalcup had a long-standing, very personal and familiar relationship with Glen Wurm, sufficient enough that Wurm would not question a request from the CEO (KrebsOnSecurity, 2016). This data may indirectly indicate that an internal accomplice might have been involved. On the other hand, due to a rapid growth of new technologies, low cost standards and little technical knowledge required for this type of crime, it is possible that the offenders are external attackers which may have no relation to higher social classes. In other words, a typical indigent scammer with a solid preparatory work could have committed CEO fraud as well as a sophisticated white-collar manager. The CEO fraud offenders have seldom been caught least but not last thanks to all cyberspace advantages they had used, thus, their belongingness to a privileged class is an underdeveloped topic which needs more research and statistical data (e.g., as it has been done in Harel (2015)'s work). Still, it makes sense to point out once again that this ambiguity gives a new round of development for the old academic debate

regarding the boundaries of white-collar crime. Since we assume the relevance of both options (an external and an internal offender), we will continue to look at CEO fraud as at a crime that can be committed by white-collar criminals with equal (or even greater) chances as (than) by others.

Due to relative technical simplicity of committing CEO fraud, the offenders may exploit the network size and its opportunities, adjusting the same scheme (e.g., email content and data collection process) to a broad range of targeted organizations. According to network value chain, the more connected users are in the common network, the greater value is for each user. Since any modern company is actively employing and using computer technologies, in particular e-commerce (wire transfer in case of CEO fraud) and internal communication (email) systems, the list of potential victims is almost unlimited and therefore very attractive for criminals. This is in line with our hypothesis (*H4*) stating that the larger the network size, the greater opportunity to engage in white-collar cybercrime and the more convenient this option is for the offenders.

On the one hand, CEO fraudsters are difficult to be identified and caught. On the other hand, financial crime is often seen as a contradictive topic in terms of law regulations and potential sentence for this crime. There is a view that white-collar offenders are treated more favorably than other criminals when is comes to sentencing (The New York Times, 2013). As Schoepfer, Carmichael and Piquero (2007) study claims, public perceptions of sanction certainty and severity suggested that street criminals were more likely to be caught and be sentenced to more severe sanctions than white-collar criminals, while the perceptions of which type of crime should be more severely punished indicated that both blue-collar robbery and white-collar fraud were equally likely to be perceived "on par". Similarly, the majority of respondents in Holtfreter, Van Slyke, Bratton & Gertz (2008) study reported that violent criminals should be punished more severely than white-collar criminals, while one-third expressed the opposite opinion. This is in line with an assumption that white-collars are perceived as persons who present no real threat of physical harm to society and continue to lead productive lives after committing a crime. Moreover, long prison sentence for such criminals imposes significant costs on the public. This reflect the class bias towards white-collar criminals, as long as it is considered that senior executive is somehow not as bad as an "ordinary" criminal, and perhaps more valuable to society living outside prison (The New York Times, 2013). At the same moment, there are cases where offenders get severe punishments

(e.g., Bernard Madoff and Robert Stanford who employed Ponzi scheme and money laundering got more than 100 years of prison sentence) meanwhile FBI enforces white-collar criminal laws and imposes large sanctions and long prison terms (Forbes, 2014). Frank A. Rubino, Esq., a criminal defense firm, says that the belief that white-collar criminals get to do "easy time" in comfortable minimum-security institutions is a myth, because in recent years sentencing for white-collar crimes has increased dramatically and some securities fraud offenses can carry a twenty-year sentence (Frank A. Rubino, Esq., 2018).

This is a brief overview of current legislation and sentence ambiguity in the field of white-collar crime regardless its form (traditional or cyber). When it comes to cyberspace legislation, there are even more undercovered issues. Livingstone (2015) highlights that the speed and agility of the cybercrime industry anticipate the glacial pace of regulatory and legislative evolution. Cybercrime has no borders, but national laws separated by state boundaries may utilize different standards for conviction and impose different punishment. As it has been mentioned in case of CEO crime, offenders from Eastern Europe, Asia or South America target organizations from highly developed countries (US, UK, Western Europe). However, computer crime in more industrialized nation will have greater ramification than in a less industrialized nation, and laws amendments done by developing countries may still lack the clarity that the industrialized nations desire. When challenges of sentencing financial crime are combined with difficulties when tracking, catching and prosecuting criminals in boundaryless cyberspace within the current legal systems, it multiplies challenges for policy makers and law enforcement, but increases opportunities for perpetrators. Such weak and unclear legal systems provide a stimulus for white-collar criminals to engage in cybercrime. AFGlobal Corp case demonstrated additional aspect where the regulation gap is calling for our attention. As in many other cases, the company insurance firm (Chubb Group) denied recovering the stolen funds, arguing that the existing policy covers only hacking, not voluntary yet fraudulent transfers of money. It was the human who has been hacked instead hardware or software. This inefficiency reflects a need for a change in corporate legislation as well as in current legal systems. Summarizing all discussed above, the actual legal situation regarding white-collar cybercrime prosecution provides an attractive opportunity to engage in illegal behavior at a low risk of being caught and sentenced to a severe term in

prison. Thus, it supports our hypothesis (*H7*) that the weaker the law regulation in cyberspace the more convenient white-collar cybercrime is for the attackers.

CEO fraud is a type of cybercrime that does not involve any kind of physical or psychological violence (excluding persuasion techniques). If a victim does not respond to spoofed emails, most probably the offenders will switch their attention to another companies. The harm of most of the white-collar crimes is evaluated in financial, economic, reputational losses, which makes white-collar crimes appear to be harmless. The illusion of zero harm gives among other things a feeling that everything is ok. Although we lack details (in particular, information about psychological state of the fraudsters) in AFGlobal Corp case, we have some empirical evidence that no need for violence is associated with criminals' acceptance of their own behavior. Olejarz (2016) when reviewing the book *Why they do it* written by Eugene Soltes, a professor at Harvard Business School, notes that white-collar criminals rarely pause to think about the outcomes or potential victims of their decisions. He illustrate this tendency with quotations from interviews with white-collar perpetrators who have been caught: "I never once thought about the costs versus the rewards" (insider trading); "I know this is going to sound bizarre, but when I was signing the documents, I didn't think of that as lying" (fraud); and "I never thought about the consequences…because I didn't think I was doing anything blatantly wrong" (insider trading) (Olejarz, 2016, p.111). Thus, if we generalize this assumption on a broader range of crimes including its cyber forms, no need for violence and any physical harm makes committing a crime a convenient option for white-collar offenders, increasing probability that they will do it, which is reflected in our hypothesis (*H6*) stating that the less violence the greater opportunity to engage in cybercrime.

After looking at CEO fraud through applying seven hypothetical assumptions we may conclude that almost all of them are supported by empirical evidence gained from AFGlobal case. In the next part of this thesis we are going to ask several experts in field of white-collar and cybercrime to share their opinion on the above discussed hypotheses.

5.2. Interviewing experts: descriptive analysis and interpretation of the results

The primary data for this research has been obtained through interviewing a group of independent and acknowledged experts in the field. We have implemented an extensive search and have found (via academic publications, university and

business school webpages, LinkedIn and personal recommendations) several experts in such topics as white-collar crime, financial crime, cybercrime, cybersecurity, corporate security. After establishing the first contact and explaining our purpose (i.e., presenting brief overview of the work and in particular hypotheses part), we have asked them to answer to a predefined set of identical questions. Since some experts were located overseas (e.g., in U.S. or Russia), we used electronic means for interviewing (the Qualtrics survey product) in order to overcome geographical distance and time separation. In the survey page we also provided them with a brief explanation of our research question and the hypotheses and offered to fulfill the form where they could evaluate the extent to which they agree with each of our seven statements (see Appendix 1 for a complete description). Although the survey has been sent to more than 60 experts, only 16 of them have answered to our request. Moreover, some of them preferred to stay anonymous when answering. Nevertheless, since our sampling was highly specific, we consider it to remain representative within the boundaries of this study. Further, we perform descriptive statistical analysis, and interpret the distribution of their answers, supported by visualization of results in pie charts.

The first statement suggested that the disconnected nature of communication between offender and victim provided by cyberspace gives greater advantage to the offender in terms of psychological separation from the victim and thereby increases the opportunity to engage in white-collar cybercrime. According to the results, half of the experts choose “agree” (31%) and “strongly agree” (19%) when evaluating this hypothesis (H1). If we add option “somewhat agree” as also supporting option, then we get in the sum 69% of experts finding the disconnected nature of communication as an influencing factor on committing cybercrime. In the following we will refer to this sum as an overall percentage of gained support for a statement. The chart below demonstrates the distribution of the answers:

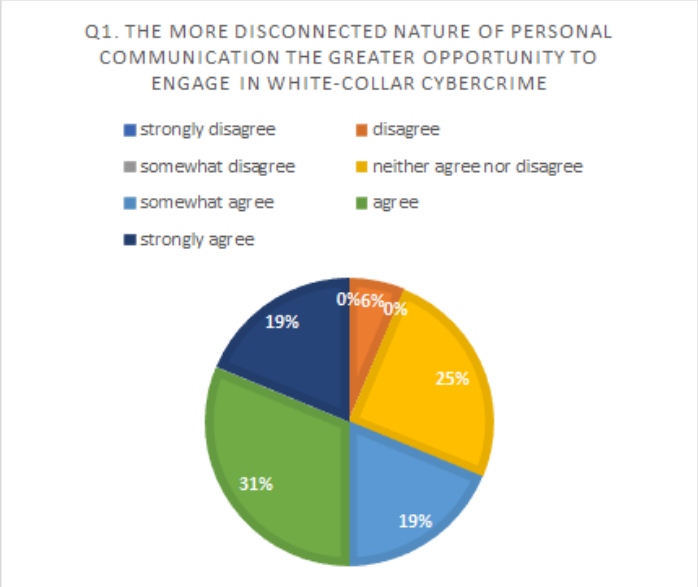

Image 2: Disconnected nature of personal communication - distribution of answers

The second statement claims that greater anonymity provided by Internet also makes committing crime a convenient option for potential offenders. As experts' opinion shows, they mostly agree that the ability to stay anonymous plays an advantageous role: 38% choose "strongly agree", 31% choose "agree" and 13% choose "somewhat agree" option, which altogether gives 82% of support for the second hypothesis (H2). The chart bar below demonstrates the distribution of the answers:

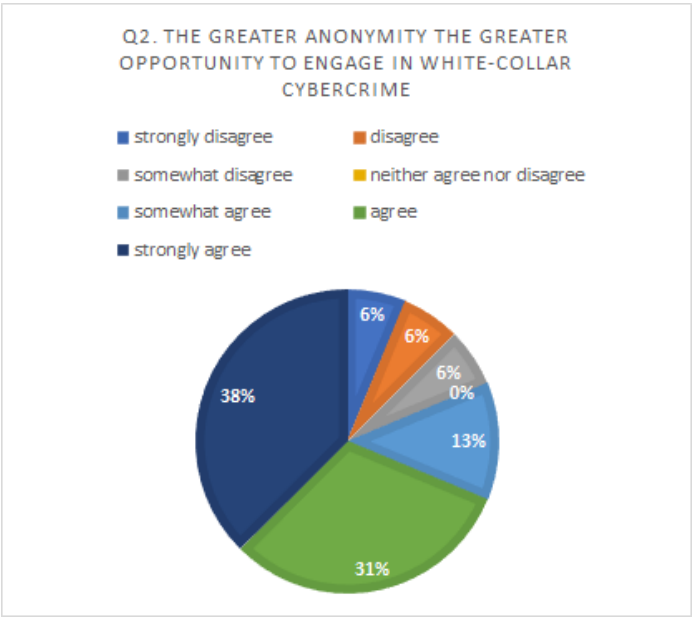

Image 3: Anonymity - distribution of answers

The third statement considers spatial and timing separation from the victim as another advantage when deciding to engage in cybercrime. This hypothesis (H3)

found the support of 69% of experts, voting for "agree" (38%), "strongly agree" (25%) and "somewhat agree" (6%) respectively. However, there is also a significant percentage of disagreement (12% of "disagree" and 6% of "strongly disagree") that should be taken into account when discussing the results. The chart below demonstrates the distribution of the answers:

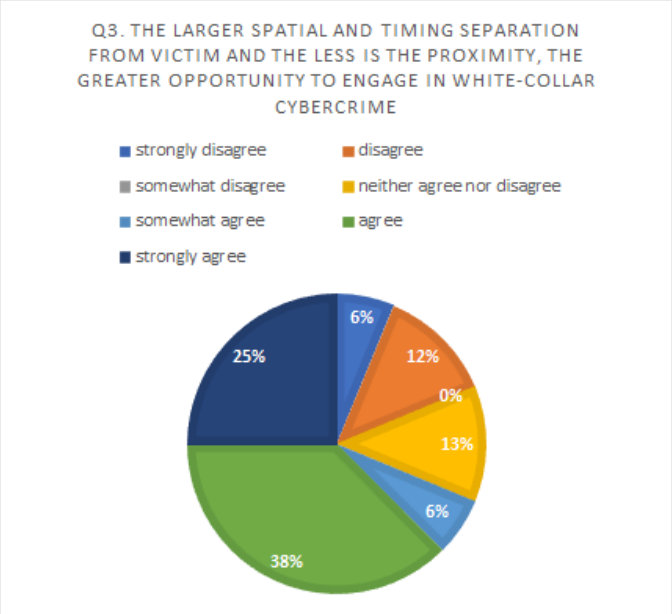

Image 4: Geographical and timing separation - distribution of answers

The fourth question was about the network size effect, where the ability to reach the greater number of possible targets provided by the very nature of Internet (e.g., network value chain) increases opportunities to engage in crime in eyes of potential offenders. Most of the experts (44%) agreed with the hypothesis (H4), which with "strongly agree" (7%) and "somewhat agree" (19%) results in 70% of support for the network size advantage. However, 25% of participants preferred to choose a neutral option rating their attitude as "neither agree nor disagree". The potential explanations of this result will be discussed later. The chart below demonstrates the distribution of the answers:

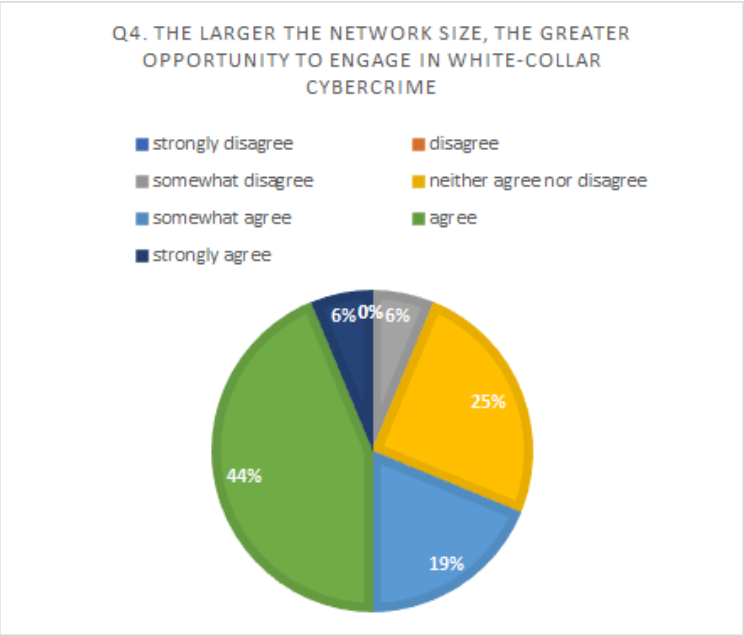

Image 5: Network size - distribution of answers

The low costs of committing such a crime online got the greatest support from experts with 50% of "agree", 19% of "strongly agree" and 12% of "somewhat agree", which in sum results in 81% of overall agreement with suggestion that low cost standard of cybercrime makes engaging in crime an attractive option for the offenders (H5). Moreover, the rest of the answers represent neutral option, and no one have chosen any form of disagreement with this hypothesis. The chart below demonstrates the distribution of the answers:

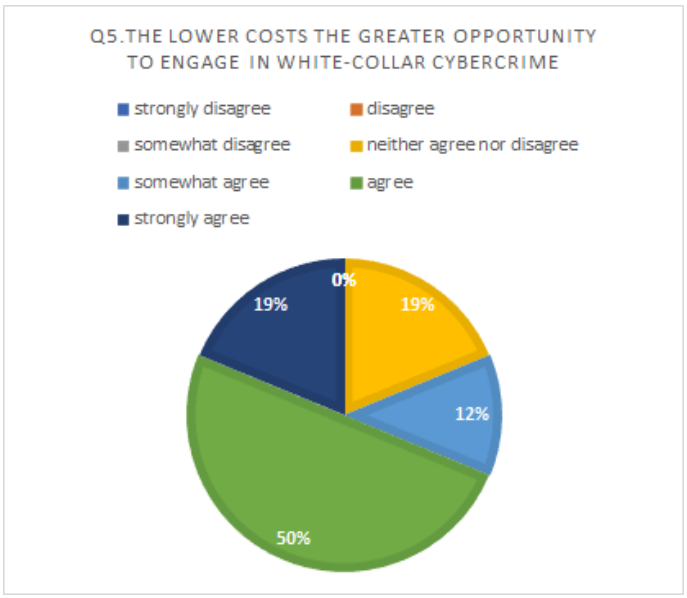

Image 6: Low costs - distribution of answers

The penultimate statement concerns the relation between violence and convenience of the crime, namely that the less need for violence provokes greater opportunity to engage in such "non-violent" type of crime. In general, this hypothesis (H6) got a significant support from the expert side. However, the extent of confidence in agreement with this particular statement was lower than with previous ones, because the most frequently chosen option was "somewhat agree" (31%). The possible explanation of this effect will be provided in the discussion part of this paper. Still, with 25% of "agree" and 19% of "strongly agree" the absence of violence as an advantage of cyberspace for engaging in crime got 75% of expert support. The chart below demonstrates the distribution of the answers:

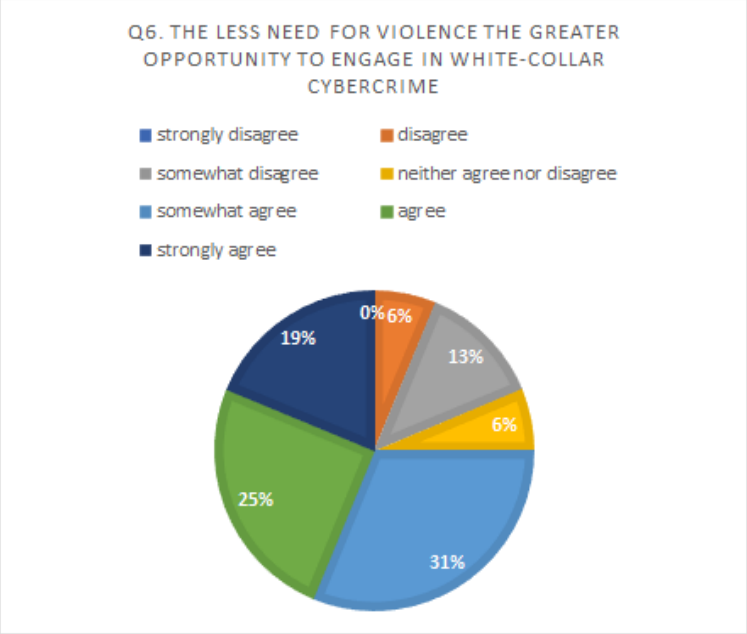

Image 7: No need for violence - distribution of answers

Finally, the last statement claims that weak law regulation in the field of cyberspace may increase the attractiveness of committing cybercrime for the offenders. In contrast to the previous hypothesis, this statement got "strongly agree" as the most popular answer among experts (50%), which demonstrates their high level of confidence. In sum with "agree" (25%) and "somewhat agree" (13%), the overall degree of agreement amounts to 88%. However, one should also point out that despite of such certainty, the residual percentage (12%) show confident disagreement with the hypothesis (H7). These slightly contradictory results will also be considered later. The last chart below demonstrates the distribution of the answers:

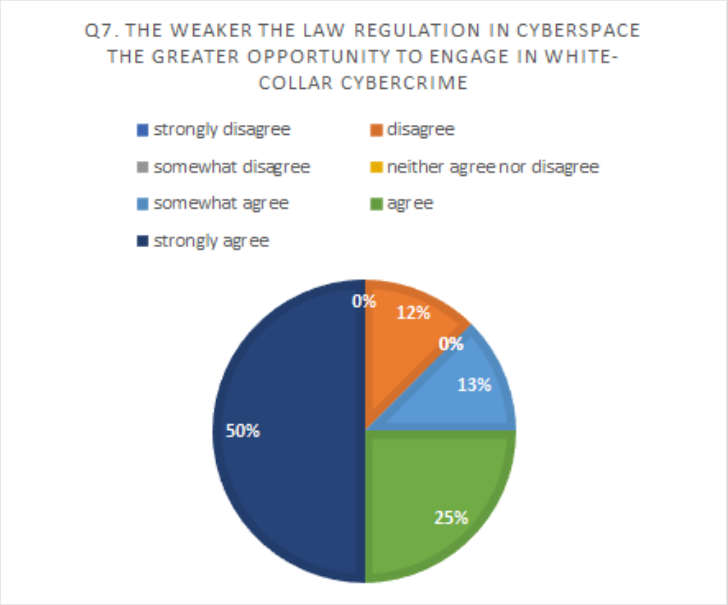

Image 8: Weak law regulation - distribution of answers

In general, results show that the most frequently chosen option was "agree" and that, calculated together as a mean of the sums of each question's overall extent of gained support, the average extent of agreement reached 76% of total expert answers.

Chapter 6. Discussion

6.1. The most interesting differences in expert opinion regarding seven factors

Our research objective was to figure out why white-collar criminals would go into cyberspace instead of committing a traditional form of crime and how Internet-enabled characteristics make online crime an attractive opportunity for them. The significant and continuous growth of financial crimes in cyberspace and persisting high amount of insider threats which organizations face on the daily basis served as the background for this question, the answer to which lies in the opportunity perspective of the convenience theory.

Opportunity perspective predicts that opportunities to physically commit a crime are an important cause of a (in our case white-collar) crime. We suggested that cyberspace provides a broad range of opportunities due to its inherit specific Internet-enabled characteristics (disconnected nature of communication, spatial and timing separation, network size effect), as well as due to its potential for facilitating crimes (ability to stay anonymous, low cost, no need for violence, weak law regulation and investigation difficulties). Whether either of these opportunities is

viewed separately or all of them are taken together, they represent an advantage (or a set of the advantages) in the eyes of a criminal, thereby making a crime activity a convenient option, which does not require any particular technical skills to implement the conceived plan. Keeping in mind that white-collar criminals by definition have a privileged access to an organization's assets, specific knowledge and are, in overall, distinguished by their privileged occupational role, these additional cyberspace opportunities can increase the convenience of engaging in a crime even further. We have formulated seven hypotheses for each of the cyberspace advantages, respectively, and then asked reputable experts in the associated field to evaluate them.

As the research results evidence, most of the experts have agreed that each of the seven factors may increase opportunity to engage in cybercrime. However, there are differences in the percentage of the gained support (from 69% to 88% of overall agreement with a statement) as well as variance in the prevalent level of their agreement upon a concrete hypothesis (from "somewhat agree" to "strongly agree"), which also makes a difference. Moreover, within the boundaries of this study, some items got a significant degree of disagreement or showed any other distinct results, which also should be carefully reviewed. Therefore, in the following part we will reflect upon the most interesting observations.

Opportunity to remain anonymous has gained greater overall support from experts (total 82% of "strongly agree", "agree" and "somewhat agree" options) than the disconnected nature of communication (69%). This result may be linked to the difference in perception of these two factors. Although, as it has been explained in hypotheses part of this work, these opportunities are interconnected and the second comes from the first, the disconnected nature of communication is more about one's own feelings and psychological states (disconnectedness helps a criminal to avoid unpleasant emotional states, e.g., feeling of guilty, remove inhibitions related to face-to-face contact, creates unrelatedness to another party of communication, avoids cognitive dissonance, etc.), while anonymity is a safety in terms of very low risks to be physically caught and uncovered in the eyes of society. As an explanation of the difference in percentage of agreement, we may suggest that when an external person evaluates what is more important for a criminal mind, it is quite expected that ability to stay anonymous and thereby safe will have greater weight in eyes of both criminals and raters than more personal, psychological aspect of their communication perceptions (such as the online disinhibition effect which decreases

the sense of personal accountability and alters self-boundaries), because the latter can vary depending on the personality of communicators and the context.

Spatial and timing separation as a facilitating factor for increasing convenience of committing a cybercrime has 69% of expert support, but also is remarked with 18% of disagreement with this statement. The question here is why, according to some part of our experts, the ability to overcome geographical distance and time zones does not increase the attractiveness of the opportunity? Disagreed experts all belong to the same Norwegian company and do not support most of other hypotheses, so their point of view to this issue will be discussed later in this part.

Regarding the network size effect (ability to reach almost unlimited market of victims), one quarter (25%) of experts preferred to choose a neutral option ("neither agree nor disagree") when evaluating this factor. One possible explanation here is that some experts do not relate the market size to the criminal's willingness to commit a crime, because, as most cases show, the attackers often have established a concrete target (a company or its senior management) and work carefully with selected victims. This style of criminal work is well-adopted in traditional form of crime and is tightly associated with the term "white-collar crime". However, the most recent crime schemes (as CEO fraud and business email compromise in general) actively use the advantages of cyberspace in order to repeat their scheme on the other targets and amplify the gains with almost no additional costs. As prevalent number of experts (70%) support this hypothesis, we may attribute the neutrality of others to unclear formulation of the question or impression that the case to evaluate is a conventional, rather than a cyber, type of crime.

Low costs of committing cybercrime viewed as a factor increasing attractiveness and convenience of engaging in a crime is the most supported hypothesis. No one has chosen any form of disagreement with this economic perspective of modern crimes. Everyone is trying to reduce the costs and increase the gains, and such behaviors are in line with rational economic theory. When new technologies, availability of knowledge and savings of effort are offered to criminals as advantages of using cyberspace, their choice seems to be predetermined. So, low cost standard of cybercrime may be interpreted as one of the main factors facilitating crime in our case.

Regarding the need for violence, in general, most experts agree (75%) that the less need to be violent towards the victims, the greater opportunity of engaging in a crime. However, the point of interest here is the "confidence level" of their

agreement. The most popular option was “somewhat agree”, that suggests they are not completely sure about the influence of violence. Why? A possible explanation is similar to network size effect: zero need for violence has been associated with traditional form of white-collar crime (fraud, money laundering, asset misappropriation, etc.) for years, and changing its form to the cyber version one does not actually change the degree of violence when committing such crimes. White-collar criminals do not torture people or blow open bank vaults; they are not inclined to decrease or increase their level of cruelty when going online (although some deviations are possible, too, as the online disinhibition theory suggests). Still, to the point that our sixth hypothesis does not contradict established opinion regarding the degree of violence in white-collar crime, it will be supported by crime and cybersecurity experts, as it has been just demonstrated.

The last advantage of cybercrime is not directly related to cyberspace but is related to external environment around cyberspace, in particular, to the ways modern society regulates its functioning. We suggest that unclear, and not completely synchronized legislation and weak law regulation in cyberspace serves as an additional opportunity to exploit when engaging in cybercrime. The 88% of experts agreed with this hypothesis and showed high level of confidence when choosing “strongly agree” (50%). However, the residual 12% of experts demonstrate quite confident (“disagree” option) disagreement. With no neutral option, the results are slightly contradictory. What may be the reasons behind the denial of law influence? There are at least two possible explanation of how legal issues may NOT affect the crime commitment. On the one hand, perpetrators may feel they are “untouchable” in cyberspace, staying unpunished because of relative anonymity, geographical distance and other benefits of cyberspace. Therefore, even being strong, legal regulation does not impact their willingness to engage in a crime, since promised punishment is compensated by weak ability to physically find the perpetrators. On the other hand, by analogy with a murder case, a killer perfectly knows the laws but decides to commit a crime regardless the severe punishment declared by justice system. So does a cyber offender: if he is psychologically ready for a crime, no law can stop him. That is why law regulation, either weak or strong, will not change the attractiveness of an opportunity to engage in cybercrime. Further explanation concerns the minimization of status and authority factor corresponding the online disinhibition effect. The traditional Internet philosophy holds that everyone is equal, with the net itself designed with no centralized control,

inclining many users to see themselves as “innovative, independent minded explorers and pioneers” (Suler, 2004, p. 4). A fear of punishment or disapproval vanishes, making an online communication more like a peer relationship, with the appearances of authority minimized (Suler, 2004).

6.2. Consistency of hypotheses with reference to experts’ opinion

In the second part of the interview the experts were invited to share their opinion on the research question, and namely to propose their own ideas regarding why criminals choose cyberspace for committing their crimes. This was made in order to see whether experts’ independent opinion would match our hypothesized statements. The answers we got entail a broad range of suggested factors which may influence the attractiveness of committing a cybercrime. Most of them overlap with the factors suggested by this thesis and can be grouped according to the core idea reflected in each answer group.

For example, such statements as “limited cost and need for funding”, “lower costs of execution”, “lower cost of entry financially, skillset (available learning resources) and physically” are all about the low costs of cybercrime, that has been reflected also in our H5. Another characteristic of cybercrime - ability to effectively use the network effect - is supported in such statements as “reaching a market of victims”, “significant number of targets”, “larger pool of targets”, which is in line with our H4. Experts marked geographical boundless of the cybercrime (“distance between victim and perpetrator”, “ability to cover different countries”) as well as disconnected nature of communication which leads to “psychological separation between criminal and victim”. Both these patterns support our H3 and H1. In expert opinion, anonymity and legal issues are tightly coupled. “Delusion of anonymity” creates a feeling of being unpunished and never caught, while “lower risk of apprehension”, “low risk to be kept” in fact are present and “police is less equipped to combat cybercrime compared to traditional crime”. Therefore, our H2 and H7 are supported by experts, too. There is only one hypothesis - H6, concerning the absence of physical violence in cybercrime - that did not get an expert attention. As it has been already mentioned, when interviewers evaluated their agreement regarding this particular hypothesis, the most popular option was “somewhat agree”, so they were not completely sure about the influence of violence.

However, there were additional insights into the field of cybercrime that make committing a crime a convenient option. First of them is expressed

simultaneously by Dr. Max Kilger (The University of Texas in San Antonio) and Gareth Grindal (Context Information Security, UK). Cybercrime provides "larger rewards" when executed successfully and gives "larger returns with a higher return on investment". It means that once a scheme of a crime is set, due to low costs, broad geographical locations and network size effect a perpetrator is able to reach more victims and thereby gain more profit (i.e., steal more money). The key there is that "the same action is repeatable which helps amplify the gains that can be made" (Gareth Grindal).

The repeatability of cybercrime leads to the second insight: automatization of the crime, suggested by Dr. Solange Ghernaouti (Swiss Cybersecurity Advisory & Research Group). Traditional schemes of crime may also be repeated and even automatized to a certain extent, but in case of cyberspace there is no need for physical presence of perpetrator for controlling such processes.

Finally, the third factor potentially affecting engaging in cybercrime activities according to Dr. Ghernaouti is the dematerialisation of the crime. This point is in line with the dissociative imagination factor of the online disinhibition effect, according to which, consciously or unconsciously people may feel that everything happening online is situated in "a make-believe dimension" (Suler, 2004, p. 3), separate and apart from the real world. Moreover, it touches upon more philosophical aspect of crime in sense of understanding the nature and the essence of crime as a phenomenon. We cannot see cyberspace but it exists "mediated" through computers, cables and other devices. Most of the times the cybercrime (as any deception) is invisible itself, we face only its consequences (damage) or even do not know that a crime has happened. This setting may create an illusion that no crime has been committed in fact, which among other things can serve as a great justification of one's criminal actions (like "it is not possible to commit something that does not exist"). All of these additional comments on the topic may be valuable for further development of this research, for example for creating a comprehensive list of reasons for committing cybercrime.

6.3. Disagreement with hypothesis and additional insight

However, there is always a room for another perspective to any question. For example, the group of experts from the Hibis Fraud Academy, expressed disagreement with the suggested hypotheses and counter argued them by stating that "white-collar criminals will commit their crime where they see the opportunity,

so cyberspace will only be one of their options. Depending on the context and the specific situation, and also the nature of the criminal, other methods might work better than cybercrime". We may be tempted to agree with this comment primarily because, according to the convenience theory, a criminal seeks for the opportunities and exploits them, and, in some context, cyberspace may provide attackers with such opportunities but in other settings all its advantages will remain unexploited. Still, our question was to find which exactly attributes of Internet and computer-enabled technologies increase the attractiveness of cybercrime in the context where these attributes may work out. If the ultimate goal of the attacker cannot be reached through cyberspace it is quite obvious that he is not going to exploit cyberspace advantages.

Another similar point of view was that "white-collar criminals recognize that people are naturally suspicious of unsolicited requests and entreatments if they are large and feel more comfortable once they KNOW someone. So the major white-collar criminals invest in more is personal relationships. Computers, the cloud and social media are all still just tools but not the PRIMARY channel of deception". Here we may turn back to the postulate that modern scammers and fraudsters often prefer to use a wide range of social engineering techniques which rely on vulnerability of human nature. In other words, the attackers hack people's minds, not the hardware/software of their computers. No computer itself (unless it is a perfect AI creature) may cheat on a human; there is always a man behind the machine trying to deceive others. Still, it remains true that sometimes white-collar criminals use personal relationship breach as a part of traditional crime scheme and at the same time as a part of new cybercrime schemes, since trust and deception remain the most important mechanisms in any fraud structure.

6.4. Comparison of the results

The table below summarizes characteristics of Internet-enabled technologies that make online cyber-crime so engaging. Withal, we identified 7 characteristics according to the relevant literature. These characteristics have been introduced to the experts, who supplemented them with 3 additional ones. Therefore, our final table comparing the data suggests that we need to further develop this topic and study the effect of additional factors.

Table 10: Comparison of the results

Characteristics according to the literature	**Characteristics according to the empirical study**
disconnected nature of personal communication	disconnected nature of communication (69% of support, agree as prevalent degree of agreement)
anonymity	anonymity (82% of support, strongly agree as prevalent degree of agreement)
spatial and timing separation from victim	spatial and timing separation from victim (69% of support, agree as prevalent degree of agreement)
the network size effect	the network size effect (70% of support, agree as prevalent degree of agreement
low cost standard	low cost standard (81% of support, agree as prevalent degree of agreement)
weak law regulation	weak law regulation (88% of support, strongly agree as prevalent degree of agreement)
Additional characteristics proposed by experts (based on the empirical study):	
	large returns
	automatization of the crime
	dematerialization of the crime

Within the framework of this thesis, we may sort out these factors or range them by the degree of expert agreement upon them.

Thus, on the basis of analysis of the empirical part, the most supported factors which may enhance engaging in an online crime are *weak law regulation, anonymity and low-cost standard* (all gained more than 80% of agreement among

the experts), and, in particular, the first two factors (i.e. weak law regulation and anonymity) gained the strongest degree of experts' support.

The findings also suggest that among these three most supported factors legal (i.e. weak law regulation) and cost (i.e. low-cost standard) characteristics of Internet-enabled technologies are external to a criminal, since they depend on the evolvement of legal environment and economic benefit for committing online crime. The only more or less "internal" factor which makes online white-collar crime attractive and applies directly to the person's willingness to engage in an online crime is "anonymity", since it is more connected to the person's ability to stay invisible in the cyberspace and, therefore, avoid the punishment. As a result, one may suggest that from the perspective of our experts, economical and legal components of white-collar crime have greater weight than so called internal factors, i.e. those related to criminal's personality, feelings or desires (disconnected nature of communication, no need for violence, physical separation from the victim, etc.). Thus, we suggest that the ratio behind the cost-benefit approach adds greater degree of attractiveness to committing online crime than other factors do, which is an expected trend in human behavior.

Chapter 7. Limitations of the study

The contributions of this research paper should be viewed in light of several limitations. The first limitation concerns shortage of available data. Cybercrime is a new concept and the amount of available research on white-collar cybercrime is insignificant in comparison to traditional crime. We find the research literature to be mostly inflexible and complex, which could be related to the multidimensionality and controversiality of the phenomenon itself. Moreover, available official statistics and records related to the subject, occasionally excludes white-collar crimes. This issue has been acknowledged by Sutherland in 1940, however, recent situation is as worse. The most significant problem that arises in the contemporary society is that organizations underreport white-collar crime and white-collar cybercrime in fear of losing credibility on the market due to vulnerability of their systems. Therefore, the cases coming to the attention of media spotlight and authorities are only a small piece of the whole "iceberg". Research and its subsequent results are limited to the quality of the available data, which is mainly about analyzing secondary data and interpreting it. Finally, we assume that

there is a lot of confidential material not available for general public due to the guidelines that assist the prosecutorial, forensic etc. discretion. Consequently, in the absence of similar studies, we were only able to review the surface, leaving the room for further mining.

The second limitation is coupled with the previous one. Within the boundaries of this thesis, we did not have an opportunity to obtain primary data and conduct a survey of white-collar offenders regarding their opinion on the subject of identification of characteristics that made online white-collar crime attractive for them. Although convicted offenders are usually reluctant to discuss their experiences (Benson & Simpson, 2014), similar attempts to identify issues related to the nature of the crime, should be analyzed from all possible perspectives.

The third limitation concerns our empirical part. The primary data was obtained through interviewing a group of experts in the field by using electronic means and with the help of standardized questionnaire, containing seven multiple-choice questions and one open-end question. According to Benson and Simpson (2014), survey is a common method in researching white-collar crime and, although, this method has valuable advantages (e.g. low cost of conduction, possibility to survey a large number of respondents etc.), we have faced the weaknesses associated with this method. In particular, using electronic means for conducting the survey made it susceptible to misinterpretation of the questions and the underlying meaning of the introduced notions. Further, although we were able to send the questionnaire to more than 60 experts, only 16 of them have provided an answer to our request, indicating ponderable limitation of our research, such as small sampling. Finally, by using electronic means of communication, we did not have an opportunity to develop rapport with our respondents. As suggested by Suler (2004), technical means make people to self-disclose and act differently while communicating online. The online disinhibition effect makes people to either reveal or encrypt "true self" and corresponding opinions. Therefore, we would like to acknowledge that there is a possibility that our experts did not reveal important information, which they would if we have had conducted face-to-face interviews.

The fourth limitation, acknowledges the scope of the subject of white-collar cybercrime and highlights the fact, that within the boundaries of MSc thesis and its' requirements, we were unable to review every notion and theory perspective in more detail, thus providing with a limited overview on potentially important issues, for example, the impact of characteristics, related to economic and behavioral

dimensions of the convenience theory, on committing white-collar crime in cyberspace. The novelty of the concept of convenience in committing white-collar crime viewed from the perspective of its fusion with Internet-related technology has not been researched previously. Although the purpose of our paper was to contribute to the debate on the issues related to the subject and provide foundation for future research, we agree, that in order to create new knowledge or break new ground, this work should be taken further and researched in the form of doctoral dissertation.

Finally, the fifth limitation potentially calls into question the validity and reliability of our survey and will be discussed in the following subchapter.

7.1. Methodological limitations

According to the literature, the field of criminology has not yet developed consensus regarding "comprehensive measures that tap into the concepts of white-collar crime and street crime" (Holtfreter, Van Slyke, Bratton, & Gertz, 2008 cited in Benson & Simpson, 2014, p. 7), needless to mention, that white-collar cybercrime makes conceptualization even more challenging. Therefore, questions about white-collar crime on our survey could be potentially influenced by other items, as a result, reflecting methodological influences as opposed to actual pattern. Moreover, the lack of comprehensive measures makes it difficult to generalize findings to various occupational settings, making it an uneasy task to draw conclusions.

More specifically, there are usually two main questions about credibility of any research, referred to as reliability and validity. Reliability raises the question whether the researchers would get similar results if their study would be repeated once again. In quantitative research the most popular tool for measuring reliability is Cronbach's alpha (coefficient of correlation). However, in terms of qualitative research, there is no definitive understanding on how the reliability may be assessed in qualitative form. Some researchers suggest that instead of reliability and validity, we should consider trustworthiness of the research, which in turn consists of credibility, transferability, dependability and confirmability (CIRT, 2018).

Guba & Lincoln (1985) interpret reliability in qualitative research as dependability, that in turn is considered as the consistency of the results with the data collected. In our case, whether the findings are likely to apply at other times (i.e. they will be the same) will depend on whether the interviewed experts will

change their answers or give different answers to different interviewers. Since the sample of our experts has been chosen based on their level of expertise and well-known academic reputation, we hopefully suggest this significantly adds to the repeatability and overall believability of the findings.

Moreover, in the first part of the study we used the other sources (secondary data that illustrated the case of CEO fraud) and this allowed us to check the results of expert interviews with the evidence gained from newspapers and investigations in order to confirm the consistency on the topic among different sources.

The second question concerns validity of the research, i.e. whether researchers actually measure what they claim to measure. Again, in its qualitative form validity is mostly referred to as credibility (internal validity) and transferability (external validity). Credibility involves that the results should be credible from the perspective of participants in the research and therefore they are the only ones who decide whether the findings actually reflect what they were supposed to reflect. This approach is applied when the research is designed as case study. However, in our thesis we work with survey (or structured interview), and our participants are not the subjects of direct investigation (as they would be in case study) but rather they are those experts who judge the topic of main interest. Therefore, the internal validity of the research should be assessed in other way. We included an additional question in the distributed survey where we asked to share their own opinion in a free form. This was made in order to see whether experts' independent opinion would match our hypothesized statements, therefore we conducted a check on validity. Since most of the factors independently suggested the experts as influencing characteristics of cyberspace overlap with the factors suggested by us in the first part of the survey and evaluated by the same experts as significant (we conclude it on the basis of 76% of agreement with those statements), we assume the internal validity of the research is checked and confirmed as satisfactory to a certain degree.

Another important issue in qualitative-alike research is the representativeness of the sampling. Since this research does not use a probability sample, the valid sampling becomes very important, because data collected from individuals which in reality do not represent their specific segment will not lead to valid results. The experts chosen for this research have been selected on the basis of their solid knowledge of the field and closeness to the practical work with the

cases of cybercrime, therefore we assume this consideration adds significantly to the validity and credibility of the research.

Transferability (or generalizability) is often seen as the weakest part of the qualitative research, in particular single case studies, since it is not always possible to transfer the finding from one specific case to a broader set of similar cases. However, although in boundaries of qualitative research, we use survey-oriented design, that allows to generalize results with greater confidence. In order to facilitate this process for an external reader and apply the findings in a proper way, researchers should thoroughly describe the context, the central assumptions and challenges of the research. We hope the structure and logic of this work explain both possibilities and limitations for further generalization.

Finally, confirmability refers to the extent to which other researchers (or raters) confirm the results after some "data audit" of the paper. In terms of the current master project, the school educational requirement is a joint work of two authors on the same master thesis. Thus, each of us was able to check out different data sources suggested by the other partner and conduct double-interpretation of the results in order to see their match and therefore promote confirmability of this study.

In general, the presented research has a room for further methodological improvement in terms of reliability and validity of the findings. Nevertheless, we assume that in current settings we satisfy the quality requirements to the possible achievable extent.

Chapter 8. Suggestions for further research

Already in the beginning of the 21st century Grabosky et al. (2004) noted that crime in the digital environment was prone to rapid change and those, failing to anticipate the future threat, are going to be shocked when it arrives.

There is need for further research in the area, that would entail an extensive multi-method approach to data collection, designed to address the issues, such as:

- The emerging challenges that impact on cyber-security, specifically the use of new and arising technology to facilitate cybercrime.
- The extent of the shift toward white-collar cyber criminal activities and the characteristics of these activities taken in detail.

- The best practices in response to cybercrime and best prevention strategies that could help individuals and companies to mitigate the threat.
- Addressing the challenges of regulatory enactment and prosecution of white-collar criminals.
- The central role of anonymity online as inherent democracy principle opposed to threatening reality of cybercrime.

Based on our work, we would like to suggest an additional list of improvements that could be made both within and beyond the boundaries of this study.

First, from the theoretical perspective presented in the study, it is important to review all three dimensions of the concept of convenience in white-collar crime with relation to Internet-enabled technology.

Second, we need to continue the academic discurs regarding the boundaries of white-collar crime. Due to low cost standards, increase in service sector of population employment, and overall democratization trends of the leading societies (US, Europe) the complete definition of contemporary white-collar crime should be reassessed. With a rapid growth of new technologies, and little technical knowledge required for cybercrime, it is possible that the offenders may have no relation to higher social classes. As it has been noted early in the work, a typical indigent scammer with a solid preparatory work could have committed online fraud as well as a sophisticated white-collar manager. The cyber offenders have seldom been caught least but not last thanks to all cyberspace advantages they had used, thus, their belongingness to a privileged class is an underdeveloped topic which needs more research and statistical data.

Furthermore, we should study the additional characteristics of cybercrime which have been identified by our experts as potential factors influencing the attractiveness of committing that crime. Namely, large rewards (returns), automatization and dematerialization of the crime may shed light on new aspects of white-collar crime in cyber time.

Finally, we would like to address one of the possible research directions, that we consider especially promising, needless to mention effective, in confronting the white-collar cybercrime: gamification methods in employee training as a prevention strategy that could help organizations to mitigate the threat of cyber-attacks. Due to high significance of organizational risks that could be reduced

through such type of trainings, we provide a more detailed overview of the topic in the next several pages.

Chapter 9. Gamification methods in cyber training

9.1. Role of security awareness training in organizations

Cyber security as an area for response to cyber threats includes different aspects from digital software, technical firewalls to human psychology, typically divided in two sub-categories: security of IT infrastructure and security on the user side. The latter is an area of our interest, because it entails secure user behavior and people recognizing of any web-related attacks (Hendrix, Al-Sherbaz & Victoria, 2016).

From the global perspective, according to Ginni Rometty, IBM's chairman, cybercrime is the greatest threat to every company in the world (Forbes, 2015), while Warren Buffet says that cyber-attacks are even worse than nuclear weapons and become the number one problem with mankind (Business Insider, 2017). As CSO's report states, the cybersecurity community and major media predict that cybercrime damages will cost up to $6 trillion annually by 2021, representing the greatest transfer of economic wealth and exceeding the global trade of all illegal drugs combined (CSO, 2017).

From the organizational perspective, investments in IT and digitalization are expected to boost profits. This can be supported by a number of studies on a company-by-company basis, that found that companies that use more IT are more efficient and productive than their competitors (Tarafdar, Darcy, Turel & Gupta, 2015). On the other hand, according to the recent research drawn on 14 studies that were published from 2007 to 2014 and involved 3,100 organizational employees and IT users of 28 organizations in the United States, from sectors such as health care, industrial sales, manufacturing, higher education and government services - rapidly emerging "dark side" of IT hurts employees and their organizations and robs companies of some of the productivity gains they expect from their IT investments (Tarafdar et al., 2015). According to this study, one of the key negative effects of IT use in the workplace includes employee misuse of IT.

Indeed, most efforts of the businesses in the fight against cyber threat and its mitigation is concentrated on technology. Withall, antivirus, antimalware, email filters, firewalls, two-factor authentication alongside with an up-to-date backup and disaster recovery processes must be supported with the robust "human firewall",

i.e. cyber-threat educated internal staff that can spot a phishing email and won't be vulnerable to CEO fraud. Reportedly, attacks stemming from internal sources are greater in scope and can result in about 10 times as many compromised records as those from external sources (Tarafdar et al., 2015). Unfortunately, regardless of the quality of defence, employees are the weakest link in any IT system.

Cyber security is not an IT problem or just the matter of IT specialists; it concerns all humans in the organization connected through computer-mediated technologies. In practice, surprisingly many employees, business partners and third-party suppliers are unaware of cyber security issues, and are not consistently following recommended practices. By connecting personal devices to company networks, using weak passwords and allowing poor coding practices, organizations become predisposed to e.g. phishing attacks, which may result in loss of profit and other negative consequences such as costly investigations, lawsuits, loss of reputation or loss of license to operate (Sloman, 2016).

Thus, there is evidence that organizations strive to reduce the risk and the cost of cybercrimes through implementation of cyber security policies and programs. Human errors, lack of awareness and technology misuse may lead to unpredicted results. According to Lewis (2004), Tarafdar et al. (2015), Sloman (2016) and Bounfour (2015), it is important not only to have traditionally taken primarily technical approach, consisting of largely routine, mostly one-time and one-size-fits-all technical training activities where employees go through material on how and when they can use features of particular systems, but to recognize that awareness does not equal lasting behavior change. Security is typically one of such things, that does not lead to tangible outcomes. If everything is done right, nothing happens. In organizational setting, it is only a mistake that eradicates reactions, usually negative and costly.

While it is unlikely, that cybercrime can ever be eradicated, it is possible to prevent some crimes by accentuating on the importance of construction security competence by taking various approaches in order to change behavior or reinforce good security practices. For instance, Kirwan & Power (2013) suggest that providing a more complete profile of the various types of cybercriminal aids in preventing criminal behavior by intervening with at-risk groups. Other approaches suggest prevention strategies and the potential aid of psychologists in identifying methods of encouraging users to engage in safer online behaviors, and

implementing tools able to improve the engagement of learners (Zyngier, 2008; Dabbagh & Kitsantas, 2012; Pesare, Roselli, Corriero & Rossano, 2016).

Unfortunately, despite a substantial amount of research, dedicated to the relations between security awareness, training and psychology; and multiple suggestions and recommendations on how to account for various aspects of awareness and policy compliance, while building Security Awareness and Training (SAT) Programs, recent PwC's Global Economic Crime Survey (2016) reveals that most of the studied companies are still not adequately prepared for cybercrime or even underestimate the risks faced. Moreover, only 37% of organizations have a cyber incident response plan and less than half of board members request information about their organization's state of cyber-readiness (PwC, 2016). Furthermore, traditional training programs may be outdated or inconvenient for implementation in cyber settings. As Nagarajan, Allbeck, Sood and Janssen (2012) claim, disadvantages of most of the current forms of cyber skills training are that they are disengaging, they do not require participants to apply security concepts in real time, happen once a year, presented by security professionals who are bad communicators. Although theoretical knowledge of security concepts is important, defending against cyber-attacks in real time is highly stressful and, therefore, a prior hands-on experience (learned and continuously practiced competence to make right decisions in short time guided by automatic "rules of thumb" rather than by time consuming thorough analysis of situation) is needed. Thus, given the digital nature of cyber-crime and cyber security, the latter appears to be a topic that is especially well-suited to training by applying an agile, engaging learning approach and newest digital tools. For instance, a flexible, scalable and highly interactive video game could help simulate an environment for the trainees, appropriate to training goal (Nagarajan et al., 2012).

To conclude, in a world where competition is global, and technology has lowered entry barriers, organizations whose employees, communities and customers are deeply engaged will outperform those that cannot engender authentic motivation. Thousands of organizations are showing great results by implementing new technology and trying to establish a human firewall. Sadly, these measures will reduce the potential threat, but won't eliminate breaches entirely. The way to manage this problem is new-school security awareness training, which employs the dissociative imagination factor of the online disinhibition effect and human predisposition to engage in modern media-driven lifestyles, where the power of

Internet-enabled devices and video game imagination can infiltrate reality testing. Game-design simulation techniques of training programs are not only providing the means to achieve it, but pointing towards a radical transformation in business conduct (Suler, 2004; Werbach & Hunter, 2012).

9.2. Gamification as a novel approach to cyber security training

First, we discuss the principles of gamification and game design. This will provide us with theoretical foundation and understanding of how the obtained background can be leveraged to apply gamification with regards to cyber security training.

Games have been a fundamental part of human civilization for thousands of years. Games are popular in every demographic, gender and age group, but they are especially pervasive among the generation now moving into the workforce (Werbach & Hunter, 2012).

McGonigal (2011) suggests that all games share four defining traits: a goal (gives a sense of purpose), rules (foster strategic thinking and endorse creativity), a feedback system (provides motivation and indication of how much time does it take to achieving the goal), and a voluntary participation (makes the experience safe and pleasurable). To sum up, playing a game is the voluntary attempt to overcome unnecessary obstacles (Suits, 2005 cited in McGonical, 2011).

Gamification as a phenomenon is a trend in both human-computer interaction and game studies research and practice. The most widely accepted definition of gamification is the use of game elements and game-design techniques in non-game contexts (Deterding, Dixon, Khaled & Nacke, 2011; Werbach & Hunter, 2012). Kapp (2012) extends their definition of gamification as the use of game-based mechanics, aesthetics and game thinking to engage people, motivate action, promote learning, and solve problems**.** As Armstrong & Landers (2017) note, gamification has become a popular technique to enhance instructional outcomes in both education and organizational learning.

The purpose of gamification is to emphasize the attitudes of voluntariness, learning, problem-solving and exploration. Gamification is not about turning all business into a game or rewarding people with trinkets and tokens, but it is about enriching activities with "gameful" aspects and using it as a powerful toolkit to apply existing business challenges, regardless the nature of the firm. The essence of gamification of certain activities is not entertainment, but a fusion of human nature and skillful design (Dal Sasso et al., 2017). Moreover, gamification is a

research topic of increasing importance with a steadily growing base of scholars and researchers, who have been calling for a better structuring of the domain. Scholars of various disciplines (e.g. information systems, education, marketing, computer science and business administration) consider gamification to be worthy of serious study. (Treiblmaier, Putz & Lowry, 2018)

According to Werbach and Hunter (2012), gamification approach prominently works in internal, external and behavior change settings. *Internal gamification* or enterprise gamification is used by the companies to improve productivity and foster innovation. *External gamification* involves external stakeholders and is usually driven by marketing objectives. It provides with a toolkit for better understanding and stimulating customer motivation and loyalty; additionally, it produces increased identification with the product, and ultimately higher revenues. *Behavior-change gamification* aims at forming beneficial new habits and can produce not only desirable societal outcomes, but also private benefits.

The positive effects of a well-designed gamification system include the following three elements: 1) Inherent relatedness (being part of something bigger than ourselves); 2) Reward and motivation; 3) Behavior change (e.g. changing the habits, doing something previously unknown).

Hamari, Koivisto & Sarsa (2014) assessed the effects of gamification by conducting a review of 24 empirical studies. As a result of this analysis, gamification has shown positive effects in improving learning outcomes on multiple occasions. According to Hendrix et al. (2016) research, serious games (games with a purpose other than pure entertainment) may be a cost-effective solution to educate people and reduce cybercrimes. Although this field is still developing, other researchers also confirm the potential of gamified approach in education and training, for example Deterding et al. (2011); Le Compte, Elizondo & Watson (2015); Rieb et al. (2017); Landers & Callan (2011); Landers (2014); Nagarajan et al. (2012); Adams & Makramalla (2015); Dal Sasso, Mocci, Lanza and Mastrodicasa (2017); Pesare, Roselli, Corriero and Rossano (2016).

Games provide an engaging interface that enhances training, draws more trainees and simulates a variety of scenarios, yielding positive results in supporting health, education, management and other sectors (Nagarajan et al., 2012). There is also evidence that gamified methods in training and development engage millennial employees more effectively, promoting collaboration and helping to maximize

learning experiences. (Saunders, 2017) Therefore, one may assume that application of gaming concepts to training in cybersecurity and defense can also be equally fruitful: "research is advancing in modeling and simulation that seem potentially applicable to cybersecurity and defense gaming" (Nagarajan et al., 2012, p.256). Hendrix et al. (2016) suggest that in order to increase the training effectiveness, organizations and researchers should focus more on the type of scenario-based training that is already common in the security field and often includes gaming elements. Games may represent specific case studies and facilitate a case-based learning approach (Hendrix et al., 2016).

However, Kohn (1999) raises concerns about e.g. the use of reward systems and virtual economies used in game-based learning, since rewarding a certain behavior educates the users towards obtaining the specific reward and hides the actual goal of the task. He also acknowledges that the users might perceive the rewards as a controlling mechanism, thus generating rejection instead of engagement. Moreover, Dal Sasso et al. (2017) discuss legal and moral perils that endanger the process of gamification process constitute a new area of law, further complicated by its borderless nature. These include privacy issues (gamified systems and contexts can be misused to collect a vast amount of information about the players); property and ownership (players spend time and effort in building their avatars and they might consider "owning" them); threat of deceptive marketing. Finally, the use of some poorly designed gamification elements leads to counterproductive results, such as decrease in intrinsic motivation and overall satisfaction (Treiblmaier et al., 2018).

Overall, gamification is a rising phenomenon. Despite its double-edged nature, well designed gamification learning has a vast potential in enhancing training, by helping and stimulating experts and by fostering employee motivation over a longer period of time.

9.3. Gamification methods in training as prevention against white-collar-crime

Since 1) white-collar criminals, discussed in previous chapters of this paper, are currently adopting the form of cybercrime, and 2) one of the ways of cybercrime prevention is an adequate and effective training, preferably in the digital form, we suggest that use of gamification methods in organizational context would enable organizational leaders to anticipate vulnerability towards cyber-attacks and, eventually, prevent white-collar criminals' intervention.

Human vulnerabilities account for 80 percent of total vulnerabilities exploited by attackers (IBM, 2013), yet, literature analysis allow us to claim that there is dramatically little training on prevention of white-collar crime. There are some training programs dedicated to white-collar crime, but some of them are offline courses provided by university (e.g., BPP University, U.K.), some of them are online, yet short-term oriented and not contingent (e.g., 2-hours online introduction to the topic of white-collar crime provided by National White-Collar Crime Center and Bureau of Justice Assistance, U.S.). Moreover, many of these trainings are organized by governmental structures and therefore not available for companies or individuals without agency identification/accreditation. One of the recent examples of publicly known use of gamified approach is the Sberbank case, where 80% of employees have opened a phishing email coming from the name of the company's CEO. After that had happened, they have been trained to be careful when opening the suspicious emails through a training in a form of a flash game for two hours (RBK.ru, 2017) [own translation]. To conclude, based on an extensive search of existing literature, and to the best of our knowledge, there are few current applications of cyber-attacker characteristics being used in gamified cyber-security skills training for employees. Such trainings are either not available for general public or the degree of their gamification is unclear.

According to Adams and Makramalla (2015), existing gamification training solutions include few most distinct and evolved gamified approaches, which are compared according to the following aspects: awareness (providing participants with general knowledge in detecting and avoiding penetration attempts), defensive strategy (providing participants with proper tools to repel cyber-attacks), offensive strategy (provides with information and strategies helping the participants to properly understand their rival's approaches) and attacker centricity (uses known characteristics of cyber-attackers to train participants in anticipating motivation and behavior of the offender in carrying out their attacks).

According to the current state in cybersecurity training, the characteristics of attackers are seldom incorporated in training employees to understand these attackers or anticipate their attacks. Therefore, we propose that once an integrated taxonomy of white-collar crime is provided and taken into consideration for creation of different training scenarios, representing specific case studies, there should be adopted the attacker centricity perspective as the principal in the training.

Attacker centricity or attacker centric approach enhances the creation and application of both defensive and offensive strategies against cyber-attacks (Adams & Makramalla, 2015). As Rieb et al. (2017) note, offender-oriented analysis of cybercrime can help to develop strategies for intervention and prevention. For example, they continue, analysis of techniques of neutralization which criminals are used to apply in order to psychologically enable themselves to commit crimes may contribute to overall understanding of offenders' cognitive processes and consequent behavior. According to the theory of neutralization, proposed by Sykes and Matza (1957), there are five techniques that allow people to justify breaking existing social norms and laws and rationalize deviant behavior: denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, appeal to higher loyalties. If we adopt attacker centricity as a principal perspective in cybercrime training, we may achieve a better understanding of attacker's desires and actions and thereby develop a better defensive strategy against their attacks. Therefore, a serious game first played as by the attackers and then played as by managers/other victims/ enhances the creation and application of both offensive and defensive strategies against cyber-attacks (Adams & Makramalla, 2015).

Thus, we suggest that by adoption of attacker centricity approach in gamified training program the use of gamification methods may increase the effectiveness of cyber security training and therefore enable proactive rather than reactive response of organizational leaders to this threat.

To conclude, in this paper we introduced gamification as a research topic with great potential for organizations to combat white-collar crime. Because of the relative novelty of the concept and the manifold opportunities, for example use of gamified elements in the organizational context in order to prevent white-collar crime, further research in the field (e.g. PhD dissertation) is highly promising. In fact, "the steadily increasing number of publications in the discipline indicates that various research communities have already acknowledged the importance of gamification" (Treiblmaier et al., 2018, p, 39). Thus, one of the major contributions of our paper is to create a research agenda, that takes into account various perspectives, some of which have not yet been used in this context.

Chapter 10. Conclusion

The conceptualization of the occurrence of white-collar crime developed in this paper is represented by the novel theoretical perspective of convenience, which serves as an organizing concept for a number of theories from criminology and sociology. The three aspects of the convenience theory (economical, organizational and behavioral dimensions) provide relevant knowledge and accumulate contemporary background information on the subject of white-collar crime.

The role of convenience in the contemporary setting of today's digital lifestyles is relatively new. Since the mid-2000s, technology delivers what people want most - savings in time and effort, which are inherent characteristics of convenience. In fact, technology has become the driver of convenience, and technological advances have become central to the progression of convenience. However, considerable evidence suggests that the presence of the technological factor in operations, i.e. cyberspace, loosens psychological barriers. The six factors, constituting the disinhibition effect, interact with each other and supplement the three dimensions of the convenience theory, resulting in a more complex, amplified effect of cyberspace on the mindset of online users, decreasing the sense of personal accountability and altering self-boundaries, and therefore may contribute to an increased tendency to commit online crime.

Economic crime enabled by technology represents a major crisis that increasingly affects almost every aspect of our daily lives. Usually, white-collar crime takes a back seat to more sensational or violent crimes. Nevertheless, over the past 20 years, there is a steady growth of white-collar crimes thrusting into the national spotlight because of their unprecedented potential to bring a return on investment, damage the society in terms of cost and its potential for an epidemiologic repercussion.

The analysis of the existing data presents disturbing trends. As businesses and financial transactions become more and more computer and Internet dependent, the impact of economic crime can no longer be viewed as the cost of doing business. On the macro level, the global economy is increasingly threatened by cyber economic crime, e.g. 48% of 500 organizations worldwide had suffered a ransomware attack in the past 12 months (Rowan, 2017). On the micro level, nearly half of all cyber attacks are committed against small businesses (Oates, 2001).

In fact, most of the economic crimes today have a cyber version. This is mostly due to the fact that cyberspace offers the criminals more opportunities with

larger payoffs and fewer risks. Additionally, the proliferation of technology has provided the means and the opportunity for the commission of traditional crimes e.g. submission of false applications over the Internet, embezzlement of funds by wire transfer, account takeover etc. (Oates, 2001). It is the widespread use of technology and the Internet for transactions and communications and the congruence of Internet-specific characteristics that have exposed the public and private sectors to an alarming array of cyber attacks. In addition to their inability to prevent such attacks, both government and the private sector lack effective enforcement tools and remedies to bring the perpetrators to justice.

The main research question for this Master thesis - what characteristics of Internet-enabled technologies can be identified that make online white-collar crime attractive? - supplemented by a subset of additional questions, sets its agenda to find the specifics of committing white-collar crime in cyber context. The main purpose of this work was to contribute to the existing research, firstly, by suggesting an integrated taxonomy of white-collar crime and its specifics in cyberspace context, secondly, by providing an answer to the research question and, finally, by providing a foundation for further research in this field. While many of the issues covered in this thesis are still the subject for continuing discussion among specialists, the major endeavor of this paper is an attempt to contribute to the debate on white-collar cybercrime by creating a research agenda, that considers various perspectives, some of which have not yet been used in this context.

We addressed relevant secondary data which refers to crime statistics, companies' reports and the scope of academic articles, and applied it as a foundation for our research and as an illustration of how the hypothesized advantages of committing cybercrime unfold in practice. The analyses resulted in identification of the characteristics/factors (both internal and external (environmental) in relation to cyberspace) that make online crime more attractive: disconnected nature of personal communication, anonymity, geographical and timing distance, network size effect, low cost standard, no need for violence, and weak law regulation in cyberspace.

During our path to answering the main research question, we begun with the additional sub questions about further applicability and specifics of universal characteristics of cyberspace with relation to the particular field of white-collar crime by stating that, generally, universal characteristics of cyberspace can be also applied in case of white-collar crime. The specific effect of each characteristic has

been described in the corresponding part of the third chapter. The cyberspace characteristics change their influence or show variance when the settings (type, category, executor of crime) are changing, too. The differences and variances of each particular effect in relation to crime category, crime type, criminal type, triangle of convenience theory, and in terms of threats or possibilities perspective have been described in detail in tables 1-7 corresponding each cyberspace characteristic of interest in the chapter 3 in subchapters 3.1. - 3.7.

The primary data for this research has been obtained through interviewing a group of acknowledged experts in the field of white-collar crime, financial crime, cybercrime, cybersecurity and corporate security. On the basis of analysis of the empirical part, the most supported factors which may enhance engaging in an online crime are weak law regulation, anonymity and low-cost standard. Surprisingly, the least supported factor, according to the expert's opinion, is the absence of physical violence in cybercrime.

The findings also suggest that the seven factors differ in terms of their positioning status. For instance, weak law regulation (i.e. legal) and low-cost standard (i.e. cost) characteristics of Internet-enabled technologies are external to a criminal, since they depend on the evolvement of legal environment and economic benefit for committing online crime. The major internal factor which makes white-collar cyber crime attractive and applies directly to the person's promptness to engage in an online crime is "anonymity", since it is more connected to the person's ability to stay invisible in the cyberspace and, therefore, avoid the punishment.

As an additional insight comprising the experts' opinion, there have been identified three additional characteristics, that make committing a crime a convenient option: larger rewards and returns on investment referring to potential replicability of cybercrimes and consequent amplification of the gains; automatization of the crime referring to no need for physical presence of perpetrator for controlling criminal processes; the dematerialisation of the crime which touches upon dissociative ability of our mind to presume cyberspace as something unreal or nonexistent.

New technologies are typically met with an initial burst of enthusiasm. Today people still learn how to live with technology. The process of adjustment and accommodation through trial and error is normal and necessary. For that, people do not want to give up convenience they now enjoy. It would be nearly impossible to completely eliminate cybercrime, however there are ways to mitigate the threat. In

particular, this paper has introduced gamification as a research topic with a great potential for organizations to combat white-collar crime and which has not yet been used in this particular context. The latest research defines gamification as “the use of game-design elements in any non-game system context to achieve one or more of the following: intrinsic and extrinsic user motivation, facilitated information processing, better goal achievement, and behavioral changes” (Treiblmaier et al., 2018, p. 39). Although the concept itself is relatively novel, it has been already acknowledged by various research communities as it offers manifold opportunities in the organizational context that could prevent white-collar crime. Withal, gamification learning has a vast potential in enhancing training, by helping and stimulating experts and by fostering employee motivation over a longer period of time.

To conclude, we were able to provide an answer to our main research question in a way, that we have empirically identified seven characteristics of cyberspace, advantageous for committing online crime. The distinguished characteristics were determined on the basis of the existing theoretical foundation and further confirmed by experts' evaluation. Moreover, the experts in cybercrime and financial crime suggested three additional factors that may influence engaging in cybercrime.

In any research project, there will be inevitably unanswered questions, which we have addressed in the chapter corresponding suggestions for further research and a room for further methodological improvement in terms of reliability and validity of the findings. Our main goal was to contribute to the debate on the issues rather than provide conclusive answers. We believe we were able to review the subject and answer the research question from various perspectives and by using several methods for primary and secondary data analysis.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, 5(1), 5.

Armstrong, M. B., & Landers, R. N. (2017). An Evaluation of Gamified Training: Using Narrative to Improve Reactions and Learning. *Simulation & Gaming*, 1046878117703749.

Banki.ru (2017). Gref: The share of cybercrime in financial sector has reached 98,5%. Retrieved from: http://www.banki.ru/news/lenta/?id=9504350 [own translation]

Barthol, R.P., & Ku, N.D. (1959). Regression under stress to first learned behavior. Journal of Abnormal and Social Psychology, 59: 134-136.

BBC, (2016). The 'bogus boss' email scam costing firms millions. Retrieved from http://www.bbc.com/news/business-35250678

Benson, M. L., Madensen, T. D., & Eck, J. E. (2009). White-collar crime from an opportunity perspective. In *The criminology of white-collar crime* (pp. 175-193). Springer, New York, NY.

Benson, M., Simpson, S. (2009). *White Collar Crime: An Opportunity Perspective. Criminology and Justice Studies*. Taylor & Francis.

Benson, M. L., & Simpson, S. S. (2014). *Understanding white-collar crime: An opportunity perspective*. Routledge.

Berghoff, H., & Spiekermann, U. (2018). *Shady business: On the history of white-collar crime.*

Bethune, R. A. (2015). *Profiling white-collar criminals: what is white-collar crime, who perpetrates it and why?* (Doctoral dissertation, University of Edinburgh).

Bogner, A., Littig, B., & Menz, W. (2009). *Interviewing experts (Research Methods Series)*. Palgrave Macmillan Limited.

Bounfour, A. (2015). Digital Futures, Digital Transformation: From Lean Production to Acceluction (1st ed. 2016. ed., Progress in IS).

Brightman, H. J. (2011). Today's White Collar Crime: Legal, Investigative, and Theoretical Perspectives. *Routledge.*

Bryman, A. (2016). *Social research methods*. Oxford university press.

Bureau of Labor Statistics. (2013, December). Occupational employment projections to 2022. Retrieved from http://www.bls.gov/opub/mlr/2013/article/occupational-employment-projections-to-2022.htm.

Business Insider, (2017). Buffet: This is the number one problem with mankind. Retrieved from: http://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

CIRT (2018). Establishing validity in qualitative research. Research ready: certification program. Retrieved from: https://cirt.gcu.edu/research/developmentresources/research_ready/qualitative/validity

Cliff, G., & Wall-Parker, A. (2017). Statistical analysis of white-collar crime. Oxford Research Encyclopedia of Criminology. Retrieved from: http://criminology.oxfordre.com/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-267?print=pdf

Cohen, L. E., and Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review 44, 588–608.

Collins, J. M., & Schmidt, F. L. (1993). Personality, integrity, and white collar crime: A construct validity study. *Personnel Psychology*, 46(2), 295-311.

Cornish, D., and Clarke, R. V. (1986). Introduction. In D. Cornish and R. V. Clarke (Eds.), The Reasoning Criminal, (pp. 1–16). New York: Springer-Verlag.

Cornish, D. B., and Clarke, R. V. (2003). Opportunities, Precipitators, and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. Crime Prevention Studies 16, 41–96.

CSO, (2017). Top 5 cybersecurity facts, figures and statistics for 2017. Retrieved from: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Dabbagh, N., & Kitsantas, A. (2012). Personal Learning Environments, social media, and self-regulated learning: A natural formula for connecting formal and informal learning. *The Internet and higher education*, *15*(1), 3-8.

Dal Sasso, T., Mocci, A., Lanza, M., & Mastrodicasa, E. (2017, February). How to gamify software engineering. In *Software Analysis, Evolution and Reengineering (SANER), 2017 IEEE 24th International Conference on* (pp. 261-271). IEEE.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011, September). From game design elements to gamefulness: defining gamification. *In Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments* (pp. 9-15). ACM.

Deterding, S., Sicart, M., Nacke, L., O'Hara, K., & Dixon, D. (2011, May). Gamification. using game-design elements in non-gaming contexts. *In CHI'11 extended abstracts on human factors in computing systems* (pp. 2425-2428). ACM.

Engelmann-Zach, H. (2014). Executive Board Compensation of Publicly Traded Companies in Switzerland: The Influence of Compensation Gaps Between CEOs and Their Direct Reports on Firm Performance (Doctoral dissertation).

FACC (2016). Official note on the cyber attack. EANS-Adhoc: FACC AG/ UPDATE: FACC AG - Cyber-Fraud. Retrieved from: http://www.facc.com/en/News/News-Press/EANS-Adhoc-FACC-AG-UPDATE-FACC-AG-Cyber-Fraud

FBI (2016). Internet Crime Report. Retrieved from: https://pdf.ic3.gov/2016_IC3Report.pdf

FBI (2018). Public Service Announcement. INCREASE IN W-2 PHISHING CAMPAIGNS. Retrieved from https://www.ic3.gov/media/2018/180221.aspx

FBI (2017a). Internet Crime Report. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

FBI (2017b). Business E-Mail Compromise. Cyber-Enabled Financial Fraud on the Rise Globally. Retrieved from: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Forbes (2014). An MBA's thoughts on white collar crime punishment. Retrieved from: https://www.forbes.com/sites/walterpavlo/2014/01/15/an-mbas-thoughts-on-white-collar-crime-punishment/#457870f35049

Forbes, (2015). IBM's CEO On Hackers: Cyber Crime Is The Greatest Threat To Every Company In The World. Retrieved from: http://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world

Frank A. Rubino Esq., (2018). White collar crime: an overview. Retrieved from: https://www.frankrubino.com/White-Collar-Crime/White-Collar-Crime-An-Overview.shtml

Geis, G. (1982). On white-collar crime (p. 53). P. Jesilow (Ed.). *Lexington Books*.

Gottschalk, P. (2010). *Policing Cyber Crime.* Bookboon.

Gottschalk, P. (2013a). White-Collar criminals in modern management. *Modern Management Science & Engineering*, 1(1), 1.

Gottschalk, P. (2013b). Empirical differences in crime categories by white-collar criminals. *International Letters of Social and Humanistic Sciences*, 5, 17-26.

Gottschalk, P. (2016a). Investigating fraud and corruption: Characteristics of white-collar criminals. *Journal of Forensic Sciences & Criminal Investigation*; Volume 1.(2) p. 1-7

Gottschalk, P. (2016b). Investigation and prevention of financial crime: Knowledge management, intelligence strategy and executive leadership. *CRC Press.*

Gottschalk, P. (2016c). *Understanding white-collar crime: A convenience perspective*. CRC Press.

Gottschalk, P. (2017). White-Collar Crime Triangle: Finance, Organization and Behavior. *Journal of Forensic Sciences & Criminal Investigation*;Volume 4.(1) p. 1-7.

Grabosky, P., Russell G., Smith, & Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge University Press.

Greenspan, S. (2008), Dr. Annals of Gullibility: Why We Get Duped and How to Avoid It. Westport, CT: Praeger

Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work? -a literature review of empirical studies on gamification. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (pp. 3025-3034). IEEE.

Healy, P., & Serafeim, G. (2016). Who Pays for White-Collar Crime? *HBS*

Helfgott, J. B. (Ed.). (2013). *Criminal Psychology [4 volumes]*. ABC-CLIO.

Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, 3(1), 53-61.

Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. Online readings in psychology and culture, 2(1), 8.

Hofstede Insights (2018). Country comparison. Retrieved from: https://www.hofstede-insights.com/country-comparison/

Holtfreter, K., Van Slyke, S., Bratton, J., & Gertz, M. (2008). Public perceptions of white-collar crime and punishment. *Journal of Criminal Justice*, 36(1), 50-60.

IBM (2013). The 2013 IBM Cyber Security Intelligence Index. IBM security services.

IC3 (2018). Public Service Announcement. BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM. Retrieved from: https://www.ic3.gov/media/2018/180712.aspx

Joinson, A. (2007). Disinhibition and the Internet-Chapter 4. In *Psychology and the Internet* (pp. 75-92).

Kallman, E. A., & Grillo, J. P. (1996). Ethical decision making and information technology. Boston, Massachusetts.

Ketil Arnulf, J., & Gottschalk, P. (2012). Principals, Agents and Entrepreneurs in White-Collar Crime: An Empirical Typology of White-Collar Criminals in a National Sample. *Journal of Strategic Management Education*, 8(3).

Kirwan, G., & Power, A. (2013). Cybercrime: The psychology of online offenders. *Cambridge University Press.*

KnowBe4, (2016). CEO Fraud: prevention manual. Retrieved from http://www.venturebankonline.com/documents/CEO-Fraud-Manual

KnowBe4 (2018). What is CEO fraud? Retrieved from https://www.knowbe4.com/ceo-fraud

Kohn, A. (1999). *Punished by rewards: The trouble with gold stars, incentive plans, A's, praise, and other bribes*. Houghton Mifflin Harcourt.

KrebsOnSecurity (2015). Tech Firm Ubiquiti Suffers $46M Cyberheist. Retrieved from: https://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

KrebsOnSecurity, (2016). Firm Sues Cyber Insurer Over $480K Loss. Retrieved from: https://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, *45*, 58-74.

Landers, R. N., & Callan, R. C. (2011). Casual social games as serious games: The psychology of gamification in undergraduate education and employee

training. In *Serious games and edutainment applications* (pp. 399-423). Springer London.

Le Compte, A., Elizondo, D., & Watson, T. (2015, May). A renewed approach to serious games for cyber security. In *Cyber conflict: Architectures in cyberspace* (CyCon), 2015 7th international conference on (pp. 203-216). IEEE.

Lewis, B. C. (2004). Prevention of computer crime amidst international anarchy. *Am. Crim. L. Rev.*, 41, 1353.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry (Vol. 75). Sage.

Livingstone, R. (2015). Cybercrime regulation, legislation struggling to keep up. Retrieved from: https://www.brinknews.com/cybercrime-regulation-legislation-struggling-to-keep-up/

Mansfield-Devine, S. (2016). The imitation game: how business email compromise scams are robbing organisations. Computer Fraud & Security, 2016(11), 5-10.

Mansfield-Devine, S. (2017). Bad behaviour: exploiting human weaknesses. Computer Fraud & Security, 2017(1), 17-20.

McGonigal, J. (2011). *Reality is broken: Why games make us better and how they can change the world*. Penguin.

McKay, R., Stevens, C., Fratzi, J. (2010) A 12-step process of white-collar crime. *International Journal of Business Governance and Ethics* 5(1): 14-25.

Meuser, M., & Nagel, U. (2009). The expert interview and changes in knowledge production. In *Interviewing experts* (pp. 17-42). Palgrave Macmillan, London.

Miller, S. (2018). The 2017 U.S. State of Cybercrime highlights. Insider Threat. Retrieved from CEI insights https://insights.sei.cmu.edu/insider-threat/2018/01/2017-us-state-of-cybercrime-highlights.html

Miller, S. (2016). Malicious Insiders in the Workplace Series: What Do Malicious Insiders Get Paid? Insider Threat. Retrieved from CEI insights https://insights.sei.cmu.edu/insider-threat/2016/08/what-do-malicious-insiders-get-paid.html

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on* (pp. 256-262). IEEE.

Nelken, D. (Ed.). (1994). White-collar crime (pp. 355-392). Aldershot,, England: Dartmouth.

Oates, B. (2001). Cyber Crime: How Technology Makes it Easy and What to do About it. *Information Systems Management*, *18*(3), 92-96.

Olejarz, J. M. (2016). Understanding White-Collar Crime. *Harvard business review*, *94*(11), 110-111.

Ouimet, G. (2009) Psychology of white-collar criminal: In search of personality. *Psychologie Du Travail Et Des Organisations* 15(3): 297- 320.

Ouimet, G. (2010) Dynamics of narcissistic leadership in organizations. *Journal of Managerial Psychology* 25(7): 713-726.

Pesare, E., Roselli, T., Corriero, N., & Rossano, V. (2016). Game-based learning and Gamification to promote engagement and motivation in medical learning contexts. *Smart Learning Environments*, *3*(1), 5.

Piquero, N.L. (2012). The only thing we have to fear is fear itself: Investigating the relationship between fear of falling and white collar crime. *Crime and Delinquency* 58 (3): 362-379.

PwC's 2016 Global State of Information Security Survey http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

PwC, (2016). Global Economic Crime Survey 2016. Retrieved from: https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

PwC's 2018 Global Economic Crime and Fraud Survey https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

PwC's 2018 Global Economic Crime and Fraud Survey https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018-summary-infographic.pdf

Ragatz, LL.; Fremouw W.; Baker, E. (2012) The Psychological Profile of White-Collar Offenders: Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology. *Criminal Justice and Behavior* 39 (7): 978-997.

RBK (2017). Sberbank has created a flash game after phishing mails from its CEO. Retrieved from: https://www.rbc.ru/technology_and_media/15/02/2017/58a430e69a79472ba6d0aaad

Reyns, B. W. (2013), 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses', Journal of Research in Crime and Delinquency, 50: 216–38

Rieb, A., Gurschler, T., & Lechner, U. (2017). A Gamified Approach to Explore Techniques of Neutralization of Threat Actors in Cybercrime. In *Annual Privacy Forum* (pp. 87-103). Springer, Cham.

Rowan, T. (2017). Why are organizations failing to report cybercrime? *Infosecurity magazine*, 2 (2) retrieved from https://www.infosecurity-magazine.com/opinions/organizations-failing-report/

Saunders, M. E. (2017). *Gamification in Employee Training and Development: Millennial Perspectives* (Doctoral dissertation, The University of the Rockies).

Schoepfer, A., Carmichael, S., & Piquero, N. L. (2007). Do perceptions of punishment vary between white-collar and street crimes?. *Journal of Criminal Justice*, *35*(2), 151-163.

Shapiro, S. P. (1990). Collaring the crime, not the criminal: Reconsidering the concept of white-collar crime. *American Sociological Review*, 346-365.

Sjouwerman, S. (2016). CYBERHEIST: The biggest financial threat facing American businesses since the meltdown of 2008. KnowBe4.

Sloman, C. (2016). What impact does human behavior have on cyber security? *Accenture.*

Stabell, C. B., & Fjeldstad, Ø. D. (1998). Configuring value for competitive advantage: on chains, shops, and networks. *Strategic management journal*, 413-437.

Stalans, L. J., & Finn, M. A. (2016). Understanding how the internet facilitates crime and deviance.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & behavior*, *7*(3), 321-326.

Suler, J. (2005). The online disinhibition effect. *International Journal of Applied Psychoanalytic Studies, 2(2), 184-188.*

Sutherland, Edwin H. (1940). The White-collar criminal. *American Sociological Review* 5:1–12.

Sutherland, Edwin H. (1949). *White collar crime.* New York: Dryden.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. American sociological review, 22(6), 664-670.

Tarafdar, M., Darcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review*, 56(2), 61.

The New York Times (2013). The challenge of sentencing white collar defendants. Retrieved from https://dealbook.nytimes.com/2013/02/25/the-challenge-of-sentencing-white-collar-defendants/

Tosun, L. P., & Lajunen, T. (2010). Does Internet use reflect your personality? Relationship between Eysenck's personality dimensions and Internet use. *Computers in Human Behavior*, *26*(2), 162-167.

Treiblmaier, H., Putz, L. M., & Lowry, P. B. (2018). Setting a Definition, Context, and Research Agenda for the Gamification of Non-Gaming Systems.

Trustwave (2016). CEO fraud scams and how to deal with them at the email gateway. Retrieved from https://www.trustwave.com/Resources/SpiderLabs-Blog/CEO-Fraud-Scams-and-How-to-Deal-With-Them-at-the-Email-Gateway/

UN (2015). 13th United Nations Congress on Crime prevention and criminal justice, Doha, 12 –19 April 2015. Retrieved from http://www.un.org/en/events/crimecongress2015/pdf/Factsheet_5_Emerging_forms_of_crime_EN.pdf

Van Slyke, S. R., Van Slyke, S., Benson, M. L., & Cullen, F. T. (Eds.). (2016). *The Oxford Handbook of White-Collar Crime*. Oxford University Press.

Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of management*, *16*(3), 571-593.

Werbach, K., & Hunter, D. (2012). *For the win: How game thinking can revolutionize your business*. Wharton Digital Press.

Williams, H. E. (2006). Investigating white-collar crime: embezzlement and financial fraud. Charles C Thomas Publisher.

Wright, M. F., Harper, B. D., & Wachs, S. (2018). The associations between cyberbullying and callous-unemotional traits among adolescents: The moderating effect of online disinhibition. *Personality and Individual Differences*.

Zimmerman, A. (2017). Impact of Anonymity and Social Modeling: Online Aggression in Emerging Adults and Their Religious and Political Ideologies.

Zyngier, D. (2008). (Re) conceptualising student engagement: Doing education not doing time. *Teaching and Teacher Education*, *24*(7), 1765-1776.

Appendicies

Appendix 1. The distributed survey

Q1.

We suggest that cyberform of white-collar crime offers to criminals a larger set of advantages than traditional physical form of white-collar crime does. We hypothesize that white-collar criminals choose cyberspace as the means for committing their crimes because of the broad range of opening opportunities. There are seven characteristics of Internet which could be such opportunities.

We would like to ask you *to what extent do you agree with following statements*:

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
The more disconnected nature of personal communication the greater opportunity to engage in white-collar cybercrime.	○	○	○	○	○	○	○
The greater anonymity the greater opportunity to engage in white-collar cybercrime.	○	○	○	○	○	○	○
The larger spatial and timing separation from victim and the less is the proximity, the greater opportunity to engage in white-collar cybercrime.	○	○	○	○	○	○	○
The larger the network size, the greater opportunity to engage in white-collar cybercrime.	○	○	○	○	○	○	○
The lower costs the greater opportunity to engage in white-collar cybercrime.	○	○	○	○	○	○	○

The less need for violence the greater opportunity to engage in white-collar cybercrime.	○	○	○	○	○	○	○
The weaker the law regulation in cyberspace the greater opportunity to engage in white-collar cybercrime.	○	○	○	○	○	○	○

→

Q2. We also would like to ask you to kindly share your opinion and asnwer the following question:
What is so special in doing white-collar crime online/through computer-enabled technologies, that may explain why white-collar criminals prefer to use cyberspace when committing a crime?

Q3. Please enter your name and organization (if applicable). We will use this information only when citing your expert opinion.

← →

Appendix 2. Experts answering to the question Q2

1. Good reputation or high authority level. White-collars become under suspicion by police or law not as often as others. 2. Useful contacts, e.g. from the government-related side, which can be used to hide the offense. 3. High level of offender publicity is a nice psychological factor for society. If an offender is a public person it will have a good scoring level. Society tends to trust public figures. 4. They have an access to interesting and needful legitimate projects which can be used to mask an illegal part.

For my opinion because of delusion of anonymity and low risk to be kept.

Lower cost of entry financially, skillset (available learning resources) and physically. Larger returns with a higher return on investment, the same action is repeatable which helps amplify the gains tgat can be made.

DEMATERIALISATION OF THE CRIME AUTOMATIZATION OF THE CRIME CONTEXT OPPORTUNITIES

Unless you show numbers to support the statement, I think it is a bit of a strong assumption to make, that white-collar criminals would prefer to use cyberspace when committing a crime.

I do no think that white-collar criminal prefer to use cyberspace when committing a crime. White-collar criminals will commit their crime where they see the opportunity so cyberspace will only be one of their options. Depending on the context and the specific situation, and also the nature of the criminal, other methods might work better than cybercrime.

This is a leading question since I do not beleive that the white-collar criminals who are really serious about getting financial rewards prefer to use cyberspace. I beleive they recognise that people are naturally suspicious of unsolicited requests and entreatments if they are large and feel more comfortable once they KNOW someone. So the major white-collar criminals invest more in personal relationships. Computers, the

---

cloud and social media for example are all still just tools but not the PRIMARY channel of deception.
I'm not sure that white-collar criminals prefer to use cyberspace but if they do,one special feature is the pschological seperation between criminal and victim that helps the criminal justify thier actions.
The significant distance between victim and perpetrator reduces the dissonance of engaging in the crime.
It is all about reaching a market of victims, at scale, at ease. Note: I think your questions are good, but do not necessarily answer the key issue regarding why crime is on the rise if you contact me we can discuss. Mjakobsson@agari.com

Appendix 3. List of the experts who indicated their names in Q3.

Panov Nikita, Group-IB
Tatiana Slobodchikova, Megafon
Eric Collard
Max Kilger university of Texas at San antonio
Gareth Grindal
Prof. S. Ghernaouti, Swiss Cybersecurity Advisory & Research Group. University of Lausanne (CH)
Martina Marmai, Hibis AS
Veronica Morino (Hibis AS)
Nigel Iyer: The Hibis Fraud Academy / Hibis A/S
Ian, Hibis
Eugene Soltes, HBS
Agari

Appendix 4. Cover letter for the questionnaire

Subject: Asking for your expert opinion

Dear (NAME),

We are two Master students at BI Norwegian Business School (MSc in Leadership and Organizational Psychology) in Oslo. We are writing our MSc Thesis in the cross field of financial crime, white-collar crime, cybersecurity and training against cyber attacks. Our thesis supervisor is professor Petter Gottschalk, who is an extensive publisher on police investigation, internal investigation, fraud examination, financial crime, white-collar crime and organized crime.

Our hypothesis is that white-collar criminals choose cyber space as the means for committing their crimes, because of the larger set of advantages compared to the conventional methods for committing such crimes. They are disconnected nature of communication, anonymity, ability to overcome geographical distance, low cost standard of committing the cybercrime and so on. We focus on the CEO fraud scheme as an illustration of financial crime in cyberspace.

We would like to ask you as an expert in related topics to contribute to our research by providing an answer to a set of short questions (7 questions) about influence of certain variables to the extent of opportunity to engage in white-collar crime (in cyberspace). The link is
following https://bino.qualtrics.com/jfe/form/SV_3ZTzZbyCztUQObP

If you are interested in more details, we will be happy to provide you with the preliminary version of this work and hypotheses explanation.

We hope that this could be an interesting opportunity for you to support academic society and share the results of your work in the area.

Thank you in advance for your cooperation. We hope you will consider our request!

Kind regards,
Alla Fedina and Maria Karvonen