Digital Surveillance and the Private Sector

Corporate Social Responsibility and the sale of targeted surveillance technology

Universiteit Leiden
The Netherlands

Master Thesis for the Crisis and Security Management Program
Faculty of Governance and Global Affairs

Andrei Alina Gabriela
Student Number: s2680998
Supervisor: Dr. James Shires
Second Reader: Dr. Tatiana Tropina
Date of submission: 7th of June 2020

Abstract

The present Master Thesis examines the extent to which the Israeli-based tech-company NSO-Group adheres to the principles of Corporate Social Responsibility (CSR) when marketing their Pegasus software. The Framework of Corporate Social Responsibility, as put forward by Schwartz and Carroll (2003) encompasses three core domains: *economic, legal* and *ethical* which will be defined, explained and applied to the case of the NSO-Group. Furthermore, the present thesis analyses the extent to which the NSO-Group adheres to the principles of CSR by investigating the use of the companies' technology in Mexico, by means of examining eight research reports drafted by the researchers of the Citizen Lab which thoroughly discuss the manner in which the events occurred in Mexico. A content analysis of various relevant documentation has been performed in order to understand and accurately categorize the available information and come to a valuable argumentation. The findings indicate that the Israeli-based companies' adherence to the principles of CSR can be viewed as problematic and in need for a more concrete regulatory body which shall be implemented by the NSO-Group, especially when considering the *legal* and *ethical* domains.

Acknowledgments

This Master Thesis was written as part of the Crisis and Security Management Master Programme at Leiden University. I am grateful for the entire department of the FGGA (Faculty of Governance and Global Affairs) at Leiden University for the opportunity to be part of this Master Programme and such an outstanding environment.

I would like to thank my supervisor, Dr. James Shires for encouraging me throughout the entire process and giving me the opportunity to take part of his Capstone project "*Digital surveillance and the private sector".* During the process of writing the Master Thesis, Dr. Shires has constantly challenged me in learning how to ask the right questions and sparked my interest and curiosity in the field of Cyber-security even more. Moreover, taking into account that the present Thesis was written during a pandemic, Dr. Shires was very responsive and flexible with the online-communication process, fact for which I am extremely grateful.

Likewise, I would like to thank my second reader, Dr. Tatiana Tropina for her valuable feedback in the early stages of the research which were of great help in my writing process.

Table of Contents

1.Introduction

1.1 Research Statement

Although perceived as one of the greatest achievements of all times, the continuous, ever-growing development of today's technology is simultaneously one of the biggest factors in the numerous emerging issues. The internet, which is deeply embedded in the day-to-day life of a significantly large percent of the world's population is already a 'space' whose governance is highly questioned by many institutions and organization. Due to its transboundary nature, the feasibility of a global implementation of an internet governance is highly unlikely to be realized. Not only is an issue the fact that the internet is rooted in everyday activities such as searching for information, sending e-mails and other social activities such as simply staying in touch with people, it also plays a significant role in today's global, social, economic and political realms as many businesses, organizations (and not limited to) depend on certain internet infrastructures for their proper functionality (Kurbalija & MacLean, 2007). The internet thus become a prevalent issue in global politics especially due to the high importance the digital technologies display in the social and economic developments (Flyverbom, Deibert & Matten, 2017). The growing shift in focus towards the ethical issues regarding data collection and the underlying privacy concerns that come along have pushed policy makers to reconsider the regulations that are in place with regards to data protection and the existing cyber-regulatory laws. One of the main issues with regard to the ethical spectrum of data collection, which will also serve as the core of the present thesis is to be seen in the case of the Israeli based company that goes under the name of NSO-Group which "*developed a hacking tool that can break into just about any smartphone on Earth"* (Stahl, 2019). The reason more and more emphasis is put on the issues and challenges of *ethical*, and more generally speaking data collection is because many cases of (targeted) digital surveillance have been exposed (Flyverbom et al., 2017).

As stated already, businesses like many other actors make use of digital features to keep their industry running. Research shows that a lot of attention was shifted towards this aspect, mainly because it becomes clearer that "*the current approach of governments and corporations to the governance of the Internet and the adjacent technological spaces raise a host of ethical, political, legal and rights-related issues"* (Flyverbom et al., 2017, pp. 2). This further implies that a growing concern is the fact that states, governments and corporations make use of the digital technologies for rather questionable purposes such as "*various sorts of tracking and*

profiling of citizens and users" (Flyverbom et al., 2017, pp. 2). The main concept around the framing of this issue would break down to that of 'big data' which would indeed be highly relevant for the explanation of the mass-surveillance phenomenon, but for the purpose of the current thesis the focus is shifted towards the issue of *targeted digital surveillance,* thus conceptualizing the term of big data would be beyond the present scope.

The present study aims at examining, analysing and comprehending the extent to which businesses and governments adapt to the changing developments of digital technology and simultaneously examine the extent to which they obey to the ethical rules of data processing and further usage. More specifically, the focus of the research will be on the case of the Israeli NSO-Group corporation which faces serious accusations of selling targeted digital surveillance instruments and threatens the civil society by providing advanced technological spyware tools to governments for rather questionable purposes. Therefore, the main research question at the core of the study is "*How far does responsible corporate behaviour apply in the case of the NSO-Group surveillance company?"*. Although the company claims to be portraying an ethical behaviour with respect to the products that they provide, research shows that, in some instances, the reality of the manner in which the products belonging to NSO-Group is in opposition to their own claims (Kane, 2016; Perlorth, 2016). The official statement available on the NSO website with regards to the business conduct is the following:

"*NSO Group is proud to set a model for good corporate governance in the cyber intelligence industry. Our governance framework codifies NSO's commitment to ethical business by building human rights into all aspects of our work – from the design to the licensing of our products. At NSO, we are dedicated to ensuring licensed customers use our products only for their lawful and necessary purposes of preventing and investigating terrorism and serious crime. That's why our sales approval process has always gone significantly beyond the regulatory protocol, taking every reasonable measure to ensure our technology is used as intended. NSO's commitment and alignment to the UN Guiding Principles on Business and Human Rights puts us alongside a small number of companies in the information and communication technology sector who have adopted such standards. We expect all our directors, employees and business partners to act with integrity. Our corporate governance is built on the principles of fairness, the rule of law, accountability, responsibility and transparency."* (NsoGroup).

The above-mentioned quote is relevant to portray the dissonance between what the NSO-Group is officially stating on their website as being their aim and ethical conduct and the issues regarding the targeted surveillance allegations that have been raised by numerous actors. But before going more in depth with the analysis and introducing the theoretical basis of the current research, the following section will address the academic and societal relevance of the research.

1.2 Academic and Societal Relevance of the study

It is highly relevant to investigate the extent to which a business, in this case the NSO-Group tech company, adheres to the corporate social responsibilities because of the fact that it has a clear impact on individual's lives and, in this case their privacy as well. Due to the constant transformation and development of the digital technology and the fact that the internet is deeply rooted in today's society, it is important to raise awareness with regards to which data individuals should share, and especially what could be a safe manner for them to do so. From an academic point of view, researching into the field of corporate social responsibilities of companies will enrich the academic field by means of analysing literature on the topic of business ethics and applying the evidence on a relevant case, namely that of the NSO-Group in Mexico. By means of a literature review of relevant theoretical pieces on responsible corporate behaviour and business ethics, an analysis will follow where the theoretical framework will be applied to the case study of the Israeli company and see whether their real practice is matching the theoretical findings. Moreover, continuous research in the field of targeted digital surveillance is needed because of the constant development of existing technologies. Malicious software's have become highly advanced, thus tracing such malwares can be quite problematic. The aim is to provide valuable academic insights with regards to the legal and ethical issues in the private-sector surveillance and develop a framework of analysis for businesses, such as the NSO-Group, in order for them to deliver on their obligations.

For the field of Crisis and Security Management, it is a relevant topic because it focuses on the security of the individuals. Because this study focuses on digital surveillance in the private sector, more specifically on *targeted* digital surveillance, it is important to bring to the fore the idea that the '*spyware'* tools provided by the NSO-Group are used on specific individuals by the government of the respective countries, thus is not intended as a mass-surveillance tool. The distinction between targeted surveillance and mass surveillance is important to be made because it portrays a different set of highly advanced technology made available to various actors for diverse, sometimes even *unknown* reasons. The '*victims'* of the tools, as will be discussed in the following sections when analysing the case study are journalists, human rights activists and individuals who possess classified or important information that could bring certain fraudulent and unethical information into the public eye (Scott-Railton et al., 2017).

From a societal point of view, the topic of researching the extent to which responsible corporate behaviour is to be seen in the Israeli NSO-Group is highly relevant. The company advocates for acting socially responsible and emphasize on taking into account basic human rights, facts that are not always in harmony with the actual practice of the NSO-Group. The highly advanced tools of digitalized surveillance can, in the wrong hands become powerful tools used for malicious purposes (e.g. espionage, cyber warfare and massive data breaches).

The following chapter will examine the theoretical ground of the thesis beginning with an extensive review of the Ethical and Corporate Social Responsibilities that business *shall* adhere to and present the various views available in the academic literature. Afterwards, the Methodology chapter will illustrate the means by which the present study will be conducted, the case study will be thoroughly examined as well as a list of main sources for the fore coming analysis will be provided. A short section regarding the limitations that had been encountered in the developing of the study will be present at the end of the third chapter.

2. Theoretical Framework

2.1 Social and Ethical Corporate Responsibility

The terms of social and ethical corporate responsibility have been theorized by many researchers throughout time. In the past decades, more and more attention has been given to this field due to the emergent challenges and dilemmas companies face with regards to their aim and the means these companies are willing to go in order to reach the desired end goals.

According to Archie Carroll (1999) the evolution of the notion of Corporate Social Responsibility (CSR) has been mainly a product of the 20th century whose understanding and definition was greatly changed over time. Carroll himself changed his definition of CSR numerous times, until he formulated in 1983 the following: "*In my view, CSR involves the conduct of a business so that it is economically profitable, law abiding, ethical and socially supportive. To be socially responsible, … then means that profitability and obedience to the law are foremost conditions to discussing the firm's ethics and the extent to which it supports the society in which it exists with contributions of money, time and talent"* (Carroll, 1983, pp. 604 as cited in Carroll, 1999, pp. 286). His work is still cited in more current work with regard to CSR and business ethics, whereby the above-mentioned definition is referred to as the pyramid of corporate social responsibility. Researchers Davidson and Griffin (2000) define social responsibility as "*the set of obligations an organization has to protect and enhance the society in which it functions"* whereas they define ethics as "*an individuals' personal beliefs regarding what is right and wrong or, good or bad"* (Fisher, 2004, pp. 392). What the two authors are further trying to imply is that there should be a difference when discussing social responsibility and ethics in a business scenario. According to them organizations themselves do not have ethics but the individuals in the organization do. This means that no matter how ethical (or not) the individuals within the organization are, the end goals of the organization per se will, most of the time, rule over personal beliefs. By applying these theoretical ideas to the case of the NSO-Group, it could be argued that the employees of the NSO Group are expected to portray an ethical approach to conducting their business as compared to the business itself. Furthermore, in an organizational setting it could be also argued that hierarchy is highly important, therefore the employees themselves are basically doing their job, thus the ethical initiative shall be taken from the top-down, issue that will be further discussed in the fifth chapter, when discussing how the NSO-Group is officially responding to the spyware allegations. From their official statement on their website, the company claims at acting.

ethically responsible and that the developed products are only sold to parties (i.e. governments) who will further make use of these technological systems for the greater good (i.e. combating crime). These facts will be challenged in the analysis section of this paper, whereby evidence of misuse of the company's software will be presented and analysed and will help in determining the extent to which the NSO-Group adheres to the principles of CSR.

Another interesting aspect of the relationship between the Corporate Social Responsibility and ethics was illustrated by Shaw and Barry (2001) when they stated that "*the ethical responsibility of business managers is to maximise profits while complying with the 'rules of the game'"* (Fisher, 2004, pp. 394). The notion of 'the rules of the game' was described by Friedman (2000) by saying that business have only one social responsibility which is to "*use its resources and engage in activities designed to increase its profits so long as it stays within the ruled of the fame, which is to say, engages in open and free competition without deception or fraud"* (cited in Fisher, 2004, pp. 394). Thus, because the end goal of any business is profit maximization, which hardly ever comes without any type of constraints, it has been hypothesized that businesses should be able to meet the *moral minimum* which means basically to comply with those 'rules of the game' that have been determined by the society the business exists in. This theory, which portrays a different perspective as from the above-mentioned ones, therefore demonstrates that there is indeed a relationship between corporate social responsibility and ethical norms because businesses do have to comply with society's ethical norms nonetheless (Fisher, 2004).

Similarly, ethics has various definitions as well whereby it is important to note that the general term of ethics is different from that of *business ethics*. But before illustrating the general views on business ethics, literature stresses that firstly, there is a distinction to be made between *ethics* and *morality.* One of the differences lies in the fact that it is believed that morality denotes the rules of moral conduct as society has defined them and ethics on the other hand is more of a reflective attitude with regards to the justifications of what is good and what is wrong (Fisher, 2004). Other authors (Boatright, De George and Ferrell et al. as cited in Fisher, 2004) support the idea that "*morality is the subject of ethical enquiry"* (Fisher, 2004, pp. 397). The two general views with regards to this idea is that the majority of authors, especially in the public debate use the terms of ethics and morality interchangeably whereas some emphasise on the idea that "*morality refers to human conducts and values while ethics is the study of morality"* (pp. 397). The general view with regards to business ethics, as portrayed by Trevino and Nelson

(1999) is that the portraying of an ethical business behaviour implies for the businesses to conform to the specific principles, norms and regulations that society accepts as valid business conduct. More specifically, Epstein (1987) states that "*business ethics concerns the systematic, value-based reflection on the moral significance of personal and organization business action and its consequences for societal stakeholders"* (Epstein, 1987, pp. 104; Fisher, 2004).

Another relevant approach to the CSR framework, which will also be the approach used in analysing the core issue is the 'Three Domain Approach' discussed by Schwartz and Carroll (2003). The focus is shifted towards the three core domains that are related to corporate social responsibility, namely *economic, legal and ethical responsibility* (Schwartz & Carroll, 2003, pp. 503). This work is highly significant for the issue at hand because it emphasizes on the three domains of responsibility that businesses need – and shall adhere to. The economic domain is relevant when discussing the corporate social responsibility, because according to Schwartz & Carroll (2003), this domain "*captures those activities which are intended to have either a direct or indirect positive economic impact on the corporation in question"* (Schwartz & Carroll, 2003, pp. 508). This means that of course, companies have the intention to maximize the profits, but there are also non-economic activities that can be observed within companies, such as the action of not maximizing costs when a more profitable alternative occurs or engaging in activities that are not necessarily aimed at increasing profits. This issue will be further discussed by applying the case of the NSO-Group, whereby the existent scenario can be seen in matter of maximizing profits and at the same time not engaging in more profitable alternatives. Therefore, at the same time, it can be understood from Schwartz's and Carroll's economic domain that a business is economically responsible in the case where the company does not experience any kind of financial mismanagement or various forms of corruption in reaching the profit maximization and pursuing the business's goals. The second domain, the legal one, is presented based on a three-fold categorization, namely "*(1) compliance, (2) avoidance of civil litigation, and (3) anticipation of the law"* (Schwartz & Carroll, 2003, pp. 509). Therefore, in order to take account of the legal domain, companies' actions need to comply to the law, be motivated by the desire to avoid possible civil litigation for negligent conduct in the future and to anticipate possible changes in the legislation (Schwartz & Carroll, 2003, pp. 510-511). Lastly, the third domain of the framework relates to the ethical responsibility of business, which can be broadly seen as the actions that are taken by the company which are in compliance with the societal norms. Responsible ethical business activities are expected to adhere to the set of ethical or moral standards and principles

(Schwartz & Carroll, 2003). What would be seen as activities that fall outside of ethical domain of the CSR are the activities that are "*(1) amoral in nature (i.e. with an unawareness or indifference to the morality of the action), (2) take place despite an awareness that the action conflicts with certain moral principle (i.e. are unethical) or (3) are only intended to produce a net benefit for the corporation and not for the affected stakeholders (i.e. are only supported by egoism)* (Schwartz & Carroll, 2003, pp. 513).

It is important to state that summarizing from the reviewed pieces of literature, the general view regarding responsible corporate behaviour is that, although the primary focus of a business (or corporation) is to make profit, it is expected for businesses to act in an ethical manner vis-à-vis individuals, stakeholders and civil society. Even though there are various definitions with regards to the idea how a socially responsible corporation should be portrayed, or what exactly business ethics entail, the core values are to be found in majority of definitions. By looking at the three-domain approach presented by Schwartz and Carroll, it is clear that business, in order to be seen as socially responsible have to adhere to the economic, legal and ethical principles for a long-term positive outcome. In the fifth chapter of the current thesis, Schwartz & Carroll's model will be further applied on the empirical evidence in order to evaluate the extent to which the NSO-Group adheres to the three central domains of CSR, namely economic, legal and ethical.

2.2 Privacy and Security in a Digitalized Era

Both the notions of privacy and security are basic human rights that should not be questioned, no matter the circumstances. But it becomes increasingly problematic to ensure these in today's digitalized era, as the notion of privacy becomes more and more blurred out. By having the notion of *digital targeted surveillance* in mind, the present section aims at emphasizing how these sophisticated and advanced technologies are nonetheless creating tensions between an individual's privacy and security. The software (Pegasus) that the NSO-Group has developed is believed to have the ability to remotely hack into any desired mobile phone, fact that leads to the existence of the above-mentioned tensions (Marczak et al., 2018). Pegasus is one of the most advanced espionage tools that has been available on the market, due to the fact that is highly difficult to be traced and it can be installed on the targeted victim's phone by means of a click on an exploit link. Basically, the software is exploiting a number of zero-day vulnerabilities in order be enter the desired phone (Marczak et al., 2018). Zero-day

vulnerabilities can be defined as previously unknown software flaws in a computer program or a smartphone which exposes the respective program to external manipulation (Fidler, 2015). The differentiating factor between a zero-day vulnerability and a 'common' software vulnerability is that this issue is unknown to the software's producer, thus being vulnerable towards outside threats and endangering the privacy of the respective computer or even company. NSO's Pegasus could therefore remotely infect mobile phones by exploiting such zero-day vulnerabilities (via social media applications on both IOS and Android), facts which will be further discussed in the analysis.

Another main issue with regards to the marketing of the spyware software developed by NSO-Group is related to its buyers. The private company claims that they market their products only towards governmental entities for national security reasons (NsoGroup), but research shows that the a great deal of governments that have bought the spyware software are those who have poor and troubling human rights records, such as the Mexican Government and that of the UAE (Deibert et al., 2017). The main security and privacy challenge that stems from this is that specifically these (targeted) surveillance products have a degree of dual-use, whereby on the one hand both the 'manufactures' as well as the buyers, in this case governmental authorities can nonetheless claim that the purpose of the surveillance software will be fulfilled, in terms of reducing cybercrime and fighting cyber terrorism but at the same time it can be greatly misused. NSO-Group, as well as other private companies are publicly denying the liability for abuses and accusations of spyware. As stressed by Deibert et al., "*Private companies selling surveillance products have largely adopted a two-part defence to accusations regarding the abuse of their spyware products. First, companies state that their spyware products are sold to legitimate governmental authorities and law enforcement agencies only. Second, that these same products are sold in compliance with applicable laws and regulations"* (Deibert et al., 2017, pp. 12-13).

Furthermore, before moving towards the thorough presentation of the case study that will be analysed, it is important to touch upon the right for freedom of speech in this section. Because it was stressed earlier that such technology creates tensions between the privacy and security of individuals, it is important to highlight that these tensions can stem from the undermining of the fundamental right of freedom of expression as well. The section of the UN Report on the promotion and protection of the right to freedom of opinion and expression highlights in section C paragraph 30 the issue with regards to the Internet's impact in exercising the right to

freedom of expression by stating that "*... while Internet users can enjoy relative anonymity on the Internet, States and private actors also have access to new technologies to monitor and collect information about individual's communications and activities. Such technologies have the potential to violate the right to privacy, thereby undermining people's confidence and security on the Internet and impeding the free flow of information and ideas online"* (UN Doc A/HRC/23/40, 2017, pp. 9). The report further presents surveillance mechanisms as an example of this breach to privacy. Targeted surveillance can be seen as a type of personalized form of surveillance which can have chilling effects on the online activity of various individuals and could lead to self-censor and other types of avoidance to sharing controversial content for fear of not being a target of such technology (Deibert et al., 2017).

3. Methodology

3.1 Case Selection

As mentioned in the first chapter of the study, the aim is to thoroughly analyse the case of the Israeli based NSO-Group with regards to its targeted surveillance accusations and to determine the extent to which the tech-company adheres to the principles of CSR. Although there are many other cases around the world where NSO-Group's Pegasus was purchased and use in a questionable manner, one of the clearest cases with regards to the human rights abuses is in Mexico, thus the reason the case of Mexico was chosen for the current analysis. As it will be shown in the following sections, the case of Mexico is one of the clearest examples where the public statements of the NSO-Group contradict with the reality. There has been a lot of research done into the targeted surveillance allegations towards the people of Mexico and how their devices have been hacked by government authorities by means of the advanced software called 'Pegasus' developed by the Israeli company. Furthermore, another highly relevant argument why the case of Mexico was chosen for the present research is because of the existing political, social and economic environment in Mexico, which unfortunately can be seen as a facilitating factor for such issues to come to the fore. Evidence shows that Mexican politics is highly corrupt and those journalists, lawyers, anti-corruption activists that have evidence regarding the issues that the system encounters are being sanctioned for their actions (Tenz, 2019; BBC, 2017). As NY Times reporter Azam Ahmed has presented the situation in one of his articles regarding the freedom of press in Mexico, "*Running a newspaper, radio station or television outlet in Mexico usually means relying on a single, powerful client that spends exorbitant sums on advertising with a simple warning: I do not pay you to criticise me!" (*Ahmed, 2017).

The theoretical and empirical evidence for the case of Mexico is vast, thus helping in developing a fruitful analysis and challenging the available literature. As multiple media sources and research groups have stated, the main allegations against the Israeli company is that they have provided products "*to governments who are known for outrageous human rights abuses, giving them the tools to track activists and critics"* (Amnesty International, 2019). This case study is highly relevant for the present research because it gives the opportunity to challenge the literature on business ethics and CSR with a companies' actual practices. Although the NSO Group is constantly claiming that they are taking an ethical approach with their business governance, evidence states the contrary in a number of cases. There have been over twenty cases in Mexico where individuals, especially journalists have been targeted with

the Pegasus technology by governmental authorities in order to refrain them from disclosing classified information or in order to hack their mobile phones to stop that specific information from becoming public. Moreover, one of the main internet giants, namely WhatsApp has sued NSO for a cyberattack on its platform done by means of exploiting a vulnerability of the 'video-call' feature. Through this means, individual's smartphones were hacked. The manner in which the attacks occurred, as told by WhatsApp was very sophisticated but nonetheless it was possible to be traced back to NSO-Group (Cathcart, 2019). The main expectation from the analysis of the case study is to demonstrate that the NSO-Group, contrary to their official statements with regards to their ethical conduct are not always acting in the expected manner. The CSR framework will be applied in order for the main research question of the study to be answered.

3.2 Research Design

A qualitative research methodology will be employed in order to arrive at a pertinent answer to the research question at the core of the study. A single case study research will be performed on the case of the NSO-Group company and its targeted surveillance allegations in Mexico. The available reports on the allegation that occurred in Mexico will be analysed as well as various media outlets that have discussed the targeted surveillance allegations, the ethical approaches of the private company and the breach of human rights that the targets in Mexico have experienced. This will be conducted by analysing the reports available on the Citizen Lab data base. The Citizen Lab is a laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto which has a focus on "*research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights and global security"* (Citizen lab). Researchers at the Citizen Lab have been very involved with the case of the NSO-Group, not only with respect to Mexico but also to other countries where the issues occurred (i.e. Saudi Arabia and India). The reports will be compared with reliable media sources in order to test their validity and reliability, as well as other publicly available documents that can serve as evidence for the topic of interest. The reports that will be analysed from the Citizen Lab are part of an eight-reports series and investigation with the focus on Mexico and its targets:

Part 1 appeared in February 2017 by John Scott-Railton, Bill Marczak, Claudio Guarnier and Masashi Crete-Nishihata with the title "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted with NSO Exploit links".

Part 2 appeared in June 2017 by John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata and Ron Deibert with the title "Reckless exploit: Mexican Journalists, Lawyers and a Child targeted with NSO Spyware".
Part 3 appeared in June 2017 by John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata and Ron Deibert with the title "Reckless redux: Senior Mexican Legislators and Politicians targeted with NSO Spyware".
Part 4 appeared in July 2017 (same authors as above) with the title "Reckless III: Investigation into Mexican Mass Disappearance Targeted with NSO Spyware".
Part 5 appeared in August 2017 (same authors as above) with the title "Reckless IV: Lawyers for murdered Mexican women's families targeted with NSO Spyware".
Part 6 appeared in August 2017 (same authors as above) with the title "Reckless V: Director of Mexican anti-corruption group targeted with NSO Spyware".
Part 7 appeared in November 2017 by John Scott-Railton, Bill Marczak, Siena Antis, Bahr Abdul Razzak, Masashi Crete-Nishihata and Ron Deibert with the title "Reckless VI: Mexican Journalist investigating cartels targeted with NSO Spyware following assassination of colleague".
Part 8 appeared in March 2019 (same authors as above) with the title: "Reckless VII: Wife of Journalist Slain in Cartel-linked killing targeted with NSO's-Group Spyware".

Besides the above mentioned eight reports, other media outlets will be analysed in accordance to the topic of the reports in order to see various perspective surrounding the same issue. Moreover, available interviews with the NSO-Group's company and open letters from the company will be analysed as well because of the lack of direct documentation from behalf of the NSO's-Group directors and employees. The interviews with the NSO-Group's CEO, Shalev Hulio as well as Open letters between NSO-Group and Citizen Lab as well as Novalpina Capital, which is the main financial investor in the tech-company and Citizen Lab will be analysed by means of a content analysis method. The aim of the content analysis is to categorize the justificatory statements on behalf of the NSO-Group as well as its financial backers in order to establish a pattern. The NSO-Group is very limited in terms of the information they offer the public; thus, it is highly relevant to categorize their statements based on the CSR principles.

3.3. Limitations

The main limitation of the study is acquiring direct documentation from behalf of the NSO group for a more fruitful analysis, due to the lack of transparency shown by the company. Moreover, it is clear that parts of the available content are bias due to the sensitivity of the topic, thus it is crucial for the purpose of the study to underline this. Another great limitation is the lack of available means to conduct interviews with NSO employees or representatives in order to illustrate from a business perspective how the responses to the allegations are being treated and to what extent the company is taking responsibility for the alleged missuses of their products. For this reason, conducting interviews with business experts and cyber-security experts would not necessarily enrich the analysis and serve the aim of the study.

4. NSO-Group's Activity in Mexico

In order to move forward with the illustration of the issues surrounding the NSO-Group as well as to clearly situate the companies' position with regards to the principles of Corporate Social Responsibility, it is of utmost importance to first delineate the case of interest, namely NSO-Group's Activity in Mexico. Although there are numerous other cases of misuse of NSO-Group's technology worldwide (e.g. India and Saudi Arabia), the case of Mexico has been chosen to be studied in the present research, because there are numerous investigations that reveal the identities of targets, showing again that the official statements of the NSO-Group regarding the targeting of terrorists and criminals is not always the case in Mexico. The case of Mexico is one of the clearest cases that portray the fact that what the company is stating does not, in fact, match the reality. The research reports by the Citizen Lab with the analysis of each of the infection attempt on Mexican individuals portray the instances in which the NSO-Group's technology has been used for targeted surveillances purposes in Mexico which are beyond the original scope of the company, namely that of preventing crime and terror or for national security operations. Furthermore, after the main issues that are linked to the misuse of the NSO-Group's technology in Mexico, a discussion comprising the general allegations that the company is facing, together with the application of the CSR domains will be brought to the fore.

Researchers working at The Citizen Lab have made public in a series of eight reports the extent to which the NSO-Group's spyware software, Pegasus, was used by the Mexican government targeting various individuals that were believed to have crucial information with respect to sensitive governmental issues (Scott-Railton et al., 2017). Pegasus, among some of the most sophisticated spyware tools that is being marketed to governments and official organizations aiming and combating cybercrime and terrorism is being used in questionable manners by the representants of the Mexican government, targeting individuals and sending exploit links that could potentially infect the victim's smartphones with the malware (Scott-Railton et al., 2017). There are numerous individuals that have been targeted with the Pegasus exploit links in Mexico from February 2017 until March 2019, ranging from politicians, lawyers, health activists, human rights activists, towards the most striking 'target', namely a child where the aim was to reach the attention of his mother (Scott-Railton et al., 2017). The names of the confirmed targets that have been reported by the Citizen Lab will be presented below, together with their job description and the commonalities that have been found between the targets.

Moreover, examples of the exploit messages will be presented, in order to understand the manner in which the malware operates. The main point of this analysis is to portray that the victims of the NSO-Group's exploits sent by the Mexican Government are not to be framed in the category of terrorists or individuals affiliated with cyber-criminal organizations, but are journalists, politicians, lawyers and human rights activists that have not interfered with the Mexican Government unlawfully.

In the first report, report number 89 the name of the three targets were Dr. Simon Barquera which is a health scientist, Alejandro Calvillo which is the director of health and consumer rights organizations and Luis Encarnacion which is the director of an anti-obesity coalition. The commonalities that the three targets had is that they were all advocating for lowering the consumption of sugary drinks and sodas in Mexico (Scott-Railton et al., 2017, Report 89). The second report concerning the exploits in Mexico, report number 93 includes a longer lists of targets, among which were journalists and members of civil society groups. The targeted journalists were Carmen Aristegui and her minor child, Emillio Aristegui, Rafael Cabrera, Sebastian Barragan, Carlos Loret de Mola, Daniel Lizarraga and Salvador Camarena. Besides these journalists, the human rights activists and anti-corruption activists that were targeted where Mario Patron, Stephanie Brewer, Santiago Aguirre, Juan Pardinas and Alexandra Zapata. The main commonality and connection between these targets was that they have all been involved in investigating high level of corruption that was involving the Mexican government as well as the degree to which the government was involved in human right abuses (Scott-Railton et al., 2017, Report 93). The third report (number 94) from June 2017 presents three new targets, namely Ricardo Anaya Cortes which was the President of Mexico's National Action Party (PAN), Senator Roberto Gil Zuarth which at the time of the targeting was the President of Mexico's Senate and Fernando Rodriguez Doval which was the communication secretary for PAN. All three of the targets were Mexican politicians and legislators affiliated with the PAN party and the main factor that was common for all three of the targets was that at the time of the infection attempts, anti-corruption legislation was being discussed in the Mexican Congress (Scott-Railton et al., 2017, Report 94).

The fourth report analysed from the Citizen Lab database shows a different category of targets. As in the first three reports, the targets were either advocating for lowering the consumption of sugary drinks in Mexico and food scientist, journalists, lawyers and Mexican politicians and anti-corruption advocates, in the fourth report a new category of victims emerges, namely

"international expert investigators working on the 2014 Iguala Mass Disappearance" (Scott-Railton et al., 2017, Report 96, pp. 6). In this report it is examined how a phone belonging to a member of the group of experts who were investigating the 2014 Iguala Mass Disappearance of 43 Mexican students was targeted with the Pegasus software. The Interdisciplinary Group of Independent Experts (GIEI) has criticised the Mexican government for interfering with their investigation on the disappearance as they were preparing the final report (Scott-Railton et al., 2017, Report 96). The infection of the phone belonging to the GIEI investigator has occurred shortly after a period in which the organization has publicly criticised the Mexican government for hampering the progress of their investigation and not being cooperative. Moreover, the GIEI made public several findings that were presenting "*investigative irregularities and torture of suspects"* which included irregularities in the investigation led by Mexico's PGR (Office of the Prosecutor), which is a known NSO client (Scott-Railton et al., 2017, Report 96). The report concluded that it is "*self-evident that elements of the Mexican government would be interested in the activities of the GIEI during the time-frame in which the targeting of the NSO took place"* (Scott-Railton et al., 2017, Report 96, pp. 10).

The fifth report put together by the researchers at the Citizen Lab looked into a similar infection attempt as in the former ones, namely the case of Karla Micheel Salas and David Pena, two prominent Mexican lawyers and human rights defenders who were representing the families of three assassinated Mexican women (Scott-Railton et al., 2017, Report 98). The two targets have worked on various high-profile cases in Mexico, among which the famous case of the 'Navarte killings'. The 'Navarte killings' took place on the 31st of July 2015, when journalists Ruben Espinosa and activists Nadia Vera were shot to death in Mexico City. The two were voicing their critics for the governor of Veracruz, which at that time was Javier Duarte (Scott-Railton et al., 2017, Report 98, pp. 9). The infection attempts of the lawyer David Pena occurred on the 25th of September and on the 15th of October, whereby in both of the cases he received text messages on his smartphone which contained an infection attempt with NSO's Pegasus software. The first message Mr. Pena received was a 'service message' containing the exploit link and the second message referenced the organization the lawyer belonged to, revealing an audio conspiracy and the exploit link (Scott-Railton et al., 2017, Report 98, pp. 10-11). For the second target, Karla Micheel Salas there was only one message containing the exploit link which was sent on the 1st of October. The message was aiming to inform her of a death and inviting her to a wake, followed by the exploit link (Scott-Railton et al., 2017, Report 98, pp. 12).

The sixth research report continuing the series of abuses of the NSO-Group's spyware technology in Mexico reveals the targeting of the Director of Mexican Anti-Corruption Organization (Mexicanos Contra la Corrupcion y la Impunidad [MCCI]), Claudio X. Gonzalez (Scott-Railton et al., 2017, Report 99). Mr. Gonzalez's work in the recent years was focused on founding the MCCI and with the investigation and denunciation of high-level corruption in Mexico. Prior to the infection attempts of the MCCI Director "*has conducted a number of high-profile investigations, including work with the Panama Papers to scrutinizes offshore holdings of prominent Mexicans and investigative work on corruption in areas like procurement and nepotism"* (Scott-Railton et al., 2017, Report 99, pp. 7). The infection attempts against Mr. Gonzalez occurred on the 27th of July and 2nd of August, by means of two text messages on his phone. Both messages were similar in terms of claiming that Mr. Gonzalez was the subject of negative press coverage by two major Mexican newspapers, *Proceso* and *El Universal*, each followed by an exploit link pointing to the NSO's exploit framework (pp. 10).

The seventh research report of the misuse of the NSO-Group's technology in Mexico unveils a complex case surrounding the murder of the award-winning journalist Javier Valdez Cardenas who was the founder of the Mexican newspaper known for investigating cartels and organized crime in Mexico, *Rio Doce* (Scott-Railton et al., 2018, Report 116). Several days prior to his death, Mr. Cardenas received the news that he was cancer-free, but on the 15th of May he was shot 12 times after leaving his office of Rio Doce, whereby the killers "*had pulled him from his car taking his investigative files, laptop and mobile phone"* (Scott-Railton et al., 2018, Report 116, pp. 6). Nearly two days after the killing, Mr. Cardena's colleague at Rio Doce received text messages with infection attempts linked to the NSO-Group's Pegasus software, whereby most of the infection attempts presumed to provide information about the killing of his colleague and the identity of the killers. Andres Villarreal started to receive the infection attempts on the 17th of May, followed by a message on the 19th of May and the last message was on the 26th of May. The three infection attempts were framed under the same narrative, namely they purported to disclose information regarding the killing of Mr. Cardenas. The infection attempt was unsuccessful; therefore, the investigation shows that after a week "*the operator selected a new victim: Rio Doce's Director Ismael Bojorquez"* in attempting to compromise his phone (Scott-Railton et al., 2018, Report 116, pp. 9).

The last research report relating to the case of Mexico reveals the targeting of Griselda Triana, a journalist and the wife of the murdered journalist Javier Valdez Cardena, case that was discussed in the previous research report (Scott-Railton et al., 2019, Report 117). It was reported that eleven days after her husband was murdered, namely on the 25th and 26th May, Ms. Tirana has received text messages that were meant to trick her into clicking on the exploit links. During that period, Ms. Tirana was publicly active in investigating her husband's killing and cooperating with the Mexican authorities as well as taking part in public protests demanding a serious official investigation for Mr. Cardena (Scott-Railton et al., 2019, Report 117). The two infections attempts were similar to the ones in the previous report, as the operator framed the attempts as news updates with regards to the killing. Counting the targeting of Griselda Triana, the number of Mexican individuals that have been targeted with the technology manufactured by the NSO-Group rises to 25.

As seen in the analysis of the eight reports that solely focused on the cases in Mexico, the messages with the exploit links that the victims have received were "*paired with troubling personal and sexual taunts, messages impersonating official communication by the Embassy of the United States in Mexico, fake AMBER Alerts, warnings of kidnappings and other threats. The operation also included more mundane tactics such as messages sending fake bills for phone services and sex-lines"* (Scott-Railton et al., 2017, pp 8.). Another example of exploit links that were sent to the GIEI investigator (Report 96) were emotionally loaded, whereby the messages sent were the following: on the 1st of March "*My father died at dawn today, we are devastated, I'm sending you the dates of the wake, hope you can come: [exploit link]"* and on the 4th of March: "*we will bury my father's ashes today, hope you can join us for his last goodbye. I'm sending you the dates: [exploit link]"* (Scott-Railton et al., 2017, Report 96, pp. 11) Therefore, it can be established that the exploit links are very much relying on the emotional variables regarding each victim in hopes for the target to actually click the leading to the infection of the phone. All the text messages that have been examined by the researchers of Citizen Lab and the various organizations that they were affiliated with in working on the cases of NSO-Group's misuse of the spyware software in Mexico had the same domain "*smsmensaje[.]mx",* domain which is part of the NSO's exploit framework and the exploit links were all shortened to "bit.ly", thus the possibility to trace and connect them to the Pegasus software (Scott-Railton et al., 2017).

From the eight research reports that have investigated the misuse of the NSO-Group's spyware technology in Mexico over a period of two years, it can be concluded that a pattern of infection attempts can be established. The majority of the total number of targets in Mexico (i.e. 25) were either human rights activists, lawyers, anti-corruption politicians and journalists that were criticising the Mexican government from different points of view in their work. But what can be stated for sure is the fact that these 25 victims cannot be included in the range of targets that the NSO-Group has publicly announced that the technology is meant for, such as criminals and terrorist organizations. However, when referring to the 25 victims that have been discussed in the present thesis, for accuracy purposes it is necessary to mention the fact that it is not intendent to argue that there are *only* 25 victims that have been targeted in Mexico with the NSO exploit, but rather to emphasise that this was the target group that the present research focused on. The possibility that the number of targets is bigger in reality is not denied, nor is the fact that the technology sold by the NSO-Group to the Mexican government was only used in instances of targeting the civil society. But for the scope of the present analysis, only the targets from the Citizen Lab reports are discussed.

Another inference that can be drawn from the analysis of the targeted surveillances cases in Mexico is that, the given evidence shows that the NSO-Group faces serious issues with regards to "*preventing misuse of its export-controlled spyware"* software (Scott-Railton et al., 2017, Report 98). One of the main messages that can be extracted from the analysis of the present research reports is that the current market for "*lawful intercepts and government exclusive surveillance technologies has a fundamental problem of oversight"* (Scott-Railton et al., 2017, Report 98). In the following chapter, each of the CSR domain (i.e. economic, legal and ethical) will be thoroughly discussed based on the issues and allegations that surround the tech-company in order to accurately reveal an answer to the question at the core of the research.

5. NSO-Group and Corporate Social Responsibility (CSR)

The present chapter aims at bringing together the empirical data presented in the previous sections with the theoretical framework in order to reach the scope of the thesis. The aim of this chapter is to answer the research question that has been put forward, namely "*How far does responsible corporate behaviour apply in the case of the NSO-Group surveillance company?".* Until this point, the steps that have been carried out throughout the research were to illustrate the theoretical framework that will be used together with the empirical evidence to reach a pertinent answer to the afore-mentioned question. More specifically, it has been stated what the principles of CSR are and what is expected from businesses, in order to be considered responsible enterprises. Furthermore, the case selection has been justified in order to emphasize why the case of Mexico has been chosen in discussing the NSO-Group and what the social and political context in Mexico is, which can be argued that facilitated the use of the NSO-Group's technology. The fourth chapter has served as a thorough explanation with regards to what has happened in Mexico vis-à-vis the technology that was sold by the NSO-Group to the Mexican government, who the victims of the targeted surveillance were and what were the exploit-messages that the victims have received on their smartphones. Now, in this chapter the theoretical framework from the second chapter will be applied to the case of the NSO-Group, which will be mainly done by using a content analysis of the publicly available interviews with the CEO Shalev Hulio as well as open letters between various human rights organizations, NSO-Group and Novalpina Capital, a private equity UK-based firm owned by Stephan Peel who is one of the main investors in the tech-company.

For a detailed and systematic investigation and for making sure that all the necessary aspects are taken into account for accurately situating NSO-Group's position in the CSR debate, a content analysis was conducted in order to categorize the companies' public position generally speaking and as well with regards to their software (i.e. Pegasus). Besides the documentation that directly refers to the NSO-Group's position, of interest are the documents that discuss the statements of NSO-Groups' financial investors, such as Novalpina Capital, because it offers a bigger picture of the issue of interest based on the assumption that NSO's financial backers do share the same interests and ethical backgrounds (Kirchgaessner & Swaine, 2019). Novalpina Capital is a UK private equity firm founded by Stephan Peel who is an investor in the NSO-Group and has publicly announced that he will strive into making the business at the NSO-Group more transparent (Kirchgaessner & Swaine, 2019; Silverstein, 2019).

Highly relevant for the current analysis is the fact that Mr. Peel was on the board of Global Witness, an organization that "*campaigns to end environmental and human rights abuses driven by the exploitation of natural resources and corruption in the global political and economic system"* (GlobalWitness.org). On the 18th of February 2019 it was announced in a press release by Global Witness that Mr. Stephan Peel stepped down from the Board of Global Witness after investing and becoming a stakeholder in the NSO-Group company: "*Mr. Peel made his decision after his private equity firm* (i.e. Novalpina Capital) *announced it is supporting the acquisition of the technology company NSO Group"* (GlobalWitness, 2019). The Global Witness chair has announced that Mr. Peel's investment in the NSO Group might be mixed with some concerns with regards to spyware-producing companies in general. He stated that "*As an organization we have concerns about the potential for the abuse of surveillance technology. The misuse of this kind of technology can have a damaging effect on the work of NGOs and individuals and in the hands of repressive regimes, it can be used to deadly effect"* (GlobalWitness, 2019). It can be clearly stated that the position of the organization is clear and well-defined in a sense that the field of digital surveillance technology is seen as rather problematic and complex in relation to human rights and the potential damages that such technology can have. Stephan Peel's answers with regards to the above-mentioned statements was bound to a promise that he will do his best to ensure that the NSO-Group will adhere "*to the highest governance practices"* , fact that will be further discussed when establishing the adherence of NSO-Group to the third domain of CSR, namely the ethical one (GlobalWitness, 2019).

As already stated in the previous sections, one of the main sources of evidence for the analysis is the research done by the members of the Citizen Lab, organization which is highly involved with researching the involvement of the NSO-Group in Mexico, and world-wide. Citizen Lab has been involved in researching the illegal deployment of spyware technologies that had an impact on both basic human rights as well as the civil society as a whole (Anstis, 2019). The reason the Citizen Lab has conducted this investigation is to bring to the fore the issues regarding the manner in which private companies that are engineering and selling spyware technology, as in the case of the Israeli NSO-Group "*is not just used by legitimate actors and within the bounds of the law, but is also deployed against unlawful targets, such as journalists, dissidents and activists"* (Anstis, 2019, pp. 3). During the investigation, researchers at the Citizen Lab have established four trends in the spyware industry, but out of those four, of great

interest to the issue at hand is the second trend, namely that " *Private companies in the spyware industry justify the sale of their technology to any government, regardless of that government's human rights record, by arguing that they sell exclusively to sovereign States for the sole purpose of clients engaging in lawful activities and that such sales are done in compliance with all applicable laws"* (Anstis, 2019, pp. 3-4). This trend is highly relevant for the current research because it summarizes the main issues that are to be found in the relationship between private companies who sell spyware technologies, as well as the buyers of these technologies. The issue that comes to the fore with this trend is to be seen in the case of the NSO-Group as well. In the public domain, NSO is presenting the same narrative, namely that the products that are being sold by the company, such as the well-known Pegasus software, are only marketed to sovereign governments for the purpose of fighting crime and terror

In the remaining of the chapter, three sub-sections will be presented, each representing one of the CSR domains, namely *economic, legal* and *ethical.* In each section, the general issues and allegations that resulted from the content analysis of the above-mentioned documents as well as the application of these domains to the NSO-Group will be presented in order to offer a clear illustration of each of the CSR domain discussed in relation to the acquired empirical evidence regarding the actions of the tech company. By systematically relating each of the CSR domain to the case of the NSO-Group it offers a clearer evaluation of the characteristics that are, or not, met by the company.

The content analysis that was performed on the CBS interview with CEO Shalev Hullio and the interview by Ronen Bergman for Ynet magazine, as well as open letters between NSO and Citizen Lab and Novalpina and Citizen Lab have looked into the following categories: justifications regarding the prevention of cyber-crime and terror, justifications regarding the lawful behaviour of the company, justifications regarding the economic implications (here, including the statements of the investor Stephan Peel and letters from Novalpina Capital), justifications regarding the ethical conduct of the company and lastly the justifications that convey a sense of liability and accountability of the company. Based on the products of the content analysis and the categorization that has been established, the NSO-Group follows a clear pattern of responding to possible allegations by justifying their actions with the narrative that the products developed by the company are helping in fighting (cyber)-crime and preventing terrorism. All these categories, together with their definitions and indicators can be found in the Appendix of the thesis.

5.1 NSO-Group's Pegasus: Applying the CSR domains

5.1.1 The Economic Domain of CSR

The first domain of CSR that will be discussed is the economic one, which according to Schwartz and Carroll (2003) "*captures those activities which are intended to have either a direct or indirect positive economic impact on the corporation in question"* (Schwartz & Carroll, 2003, pp. 508). As it was established in the theoretical chapter, this means that companies have the intention to maximize monetary profits but at the same time there are also non-economic activities in which companies engage. Among these non-economic activities are those actions undertaken by a company of not maximizing costs when a more profitable alternative occurs or engaging in certain activities that are not aimed at increasing profits (e.g. philanthropic activities).

Solely focusing on the economic behaviour of the NSO-Group, it can be established that the tech-company appears to be following the expected economical behaviour of CSR. More precisely, the company is selling the sophisticated spyware product in question, in this case the Pegasus software in order to make profit. The NSO-Group has the reputation of being one of the best software producers in the spyware domain and they sell their software to various governments and governmental agencies in order to prevent terrorism and fight (cyber)-crime. In this context the NSO-Group aims at finding solutions in order to facilitate economic growth by selling the spyware software and making profit by benefiting its customers (in this case governments and governmental agencies) with a tool to prevent crime and terror. In the 2019 CBS interview, correspondent Lesley Stahl has asked NSO-Group's CEO a number of questions that raised further questions due to their controversary and nonetheless the manner in which Shalev Hulio responded, or not to those questions. The correspondent started a dialogue with Shalev Hulio regarding the rumours that he himself went to Saudi Arabia and sold the Pegasus software for 55 million dollars (CBS, 2019). What Mr. Hulio has responded to this indirect accusation was stating in a jokingly manner that Mrs. Stahl shall not believe all the newspapers, meaning that he did not confirm, nor deny to the facts. He followed with an interesting statement regarding Pegasus, by stating that "*Pegasus is so expensive because it lets authorities do what they long couldn't: break into smart-phones remotely, making everything in them completely visible. All emails, contacts, texts -new, old, encrypted or not. Pegasus allows detectives and agents to track locations, listen in and record conversations, basically turning the phone against its user"* (CBS, 2019).

But what is important to point out in this instance of applying the economic domain of CSR to NSO-Group is the fact that this specific domain is not highly relevant for the analysis in question**.** In the case of the tech-company, the economic domain of the CSR Framework is not the most significant one in order to account the extent to which the NSO-Group adheres to the principles of CSR. The reason this is the case is because there is no evidence of corruption, be it in form of bribes or other monetary incentives or any evidence of financial mismanagement. Therefore, when accounting the economic domain of CSR, based on the existing evidence, it can be stated that the NSO-Group is adhering to this specific principle of CSR and from an economic point of view, the companies' actions are responsible.

On the contrary, the same cannot be stated with regards to the other two domains of CSR, namely the legal and ethical one, because the main issues that have been brought to light are with regards to these domains.

5.1.2. The Legal Domain of CSR

When considering the second principle of CSR as proposed by Schwartz & Carroll (2003), the legal one, the NSO-Group proves to be operating in a legal grey area in conducting their business. Before stating the extent to which the companies' actions are or not in full accordance to the law, it is important to make clear that there are three manners in which this domain will be further analysed, namely based on Israeli, Mexican- and International law and regulations with regards to (1) laws regarding human rights and (2) laws and regulations regarding export controls. This is necessary in the present case because without stressing the laws regarding human rights and export controls in Israel, the country where the NSO-Group company is and that of Mexico, which is the country of interest, there is no possible way in reaching a pertinent answer with regards to the extent to which the tech-company adheres to this second principle of CSR. With regards to principles of International Law, the Wassenaar Arrangement will be discussed and applied.

According to the United Nation's Report (CCPR/C/81/Add.13) from 1998 focusing on Israeli Law, Israel has no official written constitution but it is committed to the International Covenant on Civil and Political Rights (ICCPR) when it comes to basic human rights, freedom of speech and political rights. Because there is no official constitution in place, "*it* (Israel) *has chosen to enact Basic Laws dealing with different components of its constitutional regime; these Basic*

Laws, taken together, comprise a 'constitution in the making'" (UN, Israeli Report, 1998). The Knesset is the House of Representatives of the state of Israeli, and the closest they have come to a form of written constitution is, as told by the representatives of the Knesset the online platform "https://knesset.gov.il/constitution/ConstIntro_eng.htm" which is "*the first step in this direction* (i.e. that of a formal constitution) *and includes historical background of the constitutional project in Israel; legal, social and political information presenting and explaining major constitutional issues and disputes; summaries of the Committee meetings; and Proposed drafts of chapter of the constitution"* (Knesset.gov, 2014). Under the proposed constitution, there are four main types of human rights that are secured under Israeli Law, namely: political rights (which includes, but it is not limited to freedom of expression, freedom of speech, freedom of press and the right of political participation), social and economic rights, minority rights and due process rights, which are highly important for the present thesis, because it guarantees the "*fair trials and the protection of one's privacy from inappropriate government interference"* (Knesset.gov, 2014).

Under the Israeli General Regulator Framework, the matter of export control is clearly stated in terms of laws and regulations. According to the Israeli Import-Export Order of 2006 (supervision of products, services and dual-use technology export), "*the export and trade of any product or technology explicitly mentioned in one or more of the Wassenaar Arrangement's (1996) nine categories as dual-use (said categories include inter alia: advanced material, computer and electronics products, data security products etc.) require a permit from the authorized regulators"* (Iliescu, n.d.) On top of the above-mentioned order, there is another Law with respect to export control, namely the Law for Supervision of Defense Export (2007) which hinders the possibility of trade of certain products that hold military competences (Iliescu, n.d.). Although Israel is not a member of the Wassenaar Arrangement, agreement which was established in order to set stone for international and national security by promoting *"transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations"* (Wassenaar Arrangement, pp. 4) and has a number of 41 participating states, Israel is considered a country which obeys the above-mentioned principles. Therefore, although not a formal member, the Israeli Ministry of Defense, which is the regulatory body for the export and trade of military or defence products has informally adopted the Wassenaar Arrangement and used the same definition for dual-use products and so on (Iliescu, n.d.).

Now moving towards the second country of interest, Mexico, the situation is quite complex. As mentioned in the case selection section of the third chapter, Mexico is quite an unstable environment from social, economic and political perspectives. The high level of corruption that is to be found in various sectors of the representative bodies and governmental organizations in Mexico undermines the true applicability of the law under the Mexican Constitution. Mexico's National Human Rights Commission (Comision National de Derechos Humanos, CNDH), which was created in 1999 is unfortunately "*failing to live up to its promises"* (HRW, 2008). The CNDH has had a significant role in the promotion of human rights in Mexico and in alarming the government when violations were taking place, but little has been done with this respect. In the report drafted by the Human Rights Watch (2008) regarding the mission of the CNDH, it is clearly stated that the organization is not meeting the needed requirements and could have a more active role in preventing the human rights abuses. As stated in the report, and highly relevant for the present research, one of the very serious human rights abuses that is to be seen in Mexico and the governmental authorities are not active in putting a stop to it is the infringement of the freedom of the press (HRW, 2008). Although there is significant evidence regarding the human rights violations journalist and human rights dissidents undergo in Mexico and the fight for the silencing of the press that the government has put up with (ref. see Tenz, 2019; Ahmed & Perloth, 2017), there are also instances where the CNDH has efficiently contributed to the promotion of the freedom of the press in Mexico. In 2006, the CNDH has sent a proposal to the Senate Human Rights Commission in order to "*protect journalists and communicators from having to reveal their sources"* and after the reform was passed the CNDH has "*also actively campaigned in support of legislation decriminalizing defamation"* (HRW, 2008, pp. 82-83). Therefore, the situation in Mexico is very complex to due to political environment which makes the legal mechanisms that are available hardly to be enforced. When it comes to laws and regulations concerning export controls, Mexico is one of the forty-one participating states that are in agreement to the laws and principles under the Wassenaar Arrangement, as mentioned in the previous section.

During the process of performing the content analysis, some quotes of NSO-Group's CEO have been analysed from various points of view and belonged to more than one category. This is the case of the quote that was extracted from the CBS interview in 2019 where Mr. Hulio explained what is making the Pegasus software so powerful (ref. 5.1.1. "*Pegasus is so expensive because (...)"*. The legal implications regarding this statement cannot be overlooked, because NSO-Group's CEO describes the manner in which such sophisticated technology can break all the

boundaries regarding the right of individual's privacy and can become very dangerous in instances of misuse, thus it can be argued that the boundaries of lawful behaviour are blurred out. Furthermore, in the same interview the CBS correspondent directly asked NSO's CEO whether he can state that he "*won't and haven't sold Pegasus to a country that is known to violate human rights and imprison journalists and go after activists*", Mr. Hulio's response was according to its well-known narrative: "*I only say that we are selling Pegasus in order to prevent crime and terror"* (CBS, 2019). The same justifications are present when answers regarding the legal and ethical use or sell of the NSO's software are desired. Mr. Hulio repetitively refrains from giving accurate and reasonable answers, thus heavily relying on presenting the same justification, namely that the NSO product prevents and helps fighting crime and terror.

Little accountability can be patterned further in the interview, when asked about the complexity and the underlying issues regarding the term 'terrorist'. Because there are difficulties in pin-pointing who a terrorist is, and various countries and (international) organizations have various takes on what the definition of a terrorist should entail, Mrs. Stahl's question is very equitable and accurate by specifically stating that there are countries where the opposition is considered to be terrorists. The answer received from the NSO leader was labelled in the 5th category, pertaining to the (lack of) liability and culpability of the NSO-Group's actions, namely "*No such thing. Every customer that we sold has a very clear definition of what terrorism is. And it's basically bad guys doing bad things in order to kill innocent people, in order to change the political agenda. I never met a customer that told me that oppositions are terrorists"* (CBS, 2019).

Therefore, to conclude with the second principle of the CSR-Framework, the NSO-Group seems to be making use of all the available legal loopholes in operating their business. It can be established that the company acts according to the law with respect to the manner in which they sell the software under International and Israeli Law. What can be considered here as a questionable behaviour is that the companies' actions are not in full harmony with the Wassenaar Arrangement when looking at the full definition of export of dual-use technology, more specifically with the part of "*seeking to prevent destabilizing accumulations within malicious intended entities"* (Iliescu, n.d.). Here, it can be argued that, although the NSO-Group officially declares that they sell Pegasus to sovereign governmental agencies with the sole purpose of fighting terrorism and stopping various criminal behaviour, in chapter four was

presented the evidence that the Mexican government made use of Pegasus beyond its official intentions. The issue in this case is that the legal domain represents a form of a 'grey area', because the NSO-Group has received the right to export its technology for the given purpose and Israel is not an official member of the Wassenaar Arrangement but at the same time the company has licensed the Mexican government to use the technology, where the Mexican government has used the software to target human right activists, innocent civilians, anti-corruption dissidents and journalists. In this case, if the NSO-Group was indeed aware of the multiple instances of misuse of their technology, their actions can be framed as portraying a high degree of negligence in their business conduct.

5.1.3 The Ethical Domain of CSR

The third domain brought to the fore in the CSR framework is the ethical one, which in the case of the NSO-Group can be perceived as the most problematic. According to Schwartz and Carroll (2003) responsible ethical activities in a business setting are expected to adhere to the set of ethical and (or) moral standards and principles of a given society. The results of the content analysis show that the NSO-Group repetitively frames itself in its public statements as being ethical and that the company produces a highly advanced software that helps in stopping criminal activities and terrorist offences world-wide. Certainly, it cannot be stated that the NSO-Group has only conducted unethical business or has not met its goal, namely that of preventing crime and terror. For example, CEO Shalev Hulio explained in his interview with Ynet how NSO's Software was a key player in catching the notorious drug lord El Chapo in February 2014, thus it can be stated that there are indeed cases where NSO's Pegasus delivered according to its intended purpose (Bergman, 2019). But regarding the targeting of El Chapo, in the CBS interview, Mr. Hulio touches upon the unethical implications of the use of Pegasus, namely that there are indeed cases where the phones of innocent people were infected by the authorities in order to track down a specific target. This occurred in the case of targeting the Mexican drug lord as well, where a journalist, an actress and a lawyer were victims of the Pegasus exploits because they were connected to El Chapo, but they were not considered a threat nor criminals. What Shalev Hulio further states with regards to targeting innocent people is labelled as a justification for the use of NSO-Group's technology in order to prevent crime and terror, because it led nonetheless to the capture of El Chapo: "*but if they are in touch with a drug lord… and in order to catch them, you need to intercept them, that's a decision that intelligence agencies should get. What if you can prevent 9/11 terror attack? And for that, you*

had to intercept the son, the 16-year-old son of Bin Laden? Would that be legit or not?" (CBS, 2019). He justifies intercepting the inner circle of the target for the 'greater good' with the sole purpose of preventing crime and catching terrorists without taking into account the collateral damage that is being done to innocent people.

Furthermore, the lack of transparency and ethical responsibility from behalf of surveillance companies such as the NSO-Group is a key concern in the public debate, thus giving rise to a series of allegations and controversaries. For the case of the NSO-Group, the series of such allegations began to rise from the famous case of prominent journalist Jamal Khashoggi's murder in 2018 (Bergman, 2019; Kirkpatrick, 2018). There were serious allegations that the NSO-Group's technology was linked to the brutal murder of the Saudi dissident, whereby in the Ynet interview, Hulio Shalev denies such allegation by stating that there is no connection between his company and the murder of Khashoggi (Bergman, 2019). A Saudi dissident that was close to the deceased journalist has filed a lawsuit against the NSO-Group stating that "*an Israeli software company* (i.e. the NSO-Group) *helped the royal court take over his smartphone and spy on his communications with Mr. Khashoggi"* (Kirkpatrick, 2018). The lawsuit was filed by Omar Abdulaziz who claimed that the NSO Group has wrongly helped the governments of UAE and Mexico to spy on journalists, dissidents among which, Omar himself was a target of the Pegasus exploits (Kirkpatrick, 2018). Among his statements, Mr. Abdulaziz has stated that he was targeted by operatives of Prince Mohammed who have been linked to the Khashoggi killing "*as part of a campaign to bring home or silence Saudi dissidents abroad"* and further approached in person as well (Kirkpatrick, 2018). When asked by reporter Bergman with regards to the NSO's involvement in the Khashoggi case, Hulio Shalev is emphasising that there was no involvement in the murder and touches upon the ethical conduct of the company, by mentioning that a thorough investigation of all clients was conducted and stressed on the fact that the governments who have the NSO technology are very limited in the number of targets that they can handle and that at that time (ref. 2019) there were no more than 150 active targets world-wide (Bergman, 2019). Finally, Hulio stresses again on the core purpose of the NSO-Group, namely that "*We are proud that the company's technology prevents terror attacks, leads to the arrest of terrorist and take part in the response to serious crime"* (Bergman, 2019).

Putting together the results of the content analysis with the available empirical data on NSO-Group's statements regarding their ethical conduct in the public sphere it can be stated that it

results in a discrepancy in terms of what the proposed core values of the company are in comparison to their actions in reality. As per the website, NSO-Group's core values are the following: "*accountability"* whereby they state that it is crucial for their business to apply rigorous ethical standards and that the process of export-control is highly regulated by the Governance, Risk and Compliance committee; "*excellence"* where the success of the company is being emphasized and the fact that NSO-Group's technology (i.e. Pegasus) has helped governments in saving numerous lives and prevent terrorist attacks; "*integrity"* where the companies' commitment is emphasised regarding the proper use of their technology and that any allegations of misuse will be investigated; and "*boldness"* where the idea of '*being bold, yet accountable'* is stressed out by the tech-company (NSOGroup/about-us).

Taking the above-mentioned four core values of the tech-company in consideration, cases of human rights abuses and ethical issues concerning the breach of individual's privacy and data protection shall not be occurring in reality. But having the case of Mexico at hand and the abuses that took place by targeting the civil society with the companies' technology is in fact a reality, leading to the conclusion that the acquired evidence opposes the above-mentioned business values. Although in the interviews analysed with the CEO of the NSO-Group Mr. Shalev Hulio little information was specifically concerning this issue, Mr. Hulio himself stated that there are cases of maltreatment of NSO-Group's technology whereby he strictly refrained from stating concrete names of those entities who have misused Pegasus. More specifically with regards to the misuse of Pegasus and on targeting innocent individuals, Mr. Hulio Shalev told the CBS respondent that he cannot discuss about specific customers but if they have spotted that someone has misused the system the NSO-Group can, and will shut the system down immediately by emphasizing that they (i.e. the NSO-Group) have the right and the technology at hand to do so (CBS, 2019).

The fact that approximatively twenty-five individuals who cannot be categorized in the terrorist- or criminals' group were targeted by the Mexican government with the technology provided by the NSO-Group highlights the unethical aspect of the current debate. Although from a legal point of view, the NSO-Group has the legal means to sell their technology to the Mexican government and meets the regulations imposed, the purpose for which the purchasers of the Pegasus software, in this case the Mexican government, are not meeting the established norms, such as using the technology for preventing crime and terror. Instead of creating a safer place for the Mexican citizens, the government has used the sophisticated technology on

infringing the right to privacy and data protection for twenty-five people who are active in helping the society (cf. Citizen Lab Report 89), fighting corruption in Mexico (cf. Citizen Lab Report 93) and investigating organized crime and cartels (cf. Citizen Lab Report 116).

The discussion surrounding the lack of transparency that the NSO-Group is portraying in the public sector has been publicly addressed by Stephan Peel in the period after investing in the tech company. He has focussed on this issue in his public statements, partly due to the public pressure that has been seen on the NSO-Group since the numerous allegations, and partly due to its peculiar and sudden withdrawal from the board of Global Witness and making the partly acquisition public. The series of open letter between Novalpina Capital, Citizen Lab, Amnesty International and other organizations that are highly involved in the research surrounding the case of interest are to be found on the '*Business & Human Rights Resource Centre'* database. Of interest are the letters concerning the misuse of the NSO-Group's technology and those concerning the commitment of Novalpina capital to ensure that the tech company becomes more transparent (Business & Human Rights Resource Centre, 2019).

The UK private firm, Novalpina Capital is the majority owner of the NSO-Group and has stated since the acquisition that it will impose and establish new rules for the tech company in response to the public spyware accusations and targeting of dissidents and journalist (Kirchgaessner, 2019). Stephan Peel has stated with regards to the changes proposed for the NSO-Group that "*Novalpina is committed to do whatever necessary to ensure NSO's technology is used only for its intended lawful purposes"* (Kirchgaessner, 2019). Furthermore, he publicly promised that NSO-Group aims at releasing "*all information of relevance and important about the firm's work, unless it was prohibited by law from doing so, risked public safety, national security, or employee's safety, or if needed to protect legitimate commercial confidentiality"* (Kirchgaessner, 2019). This is indeed the main issue that was voiced by organizations such as Amnesty International (in a public affidavit directed to Stephan Peel and NSO-Group in 2019) and in numerous letters drafted by the researchers of the Citizen Lab.

The public statements and promises voiced by Stephan Peel in relation to the new governance framework that will be issued as guidelines for the ethical conduct of the tech company are in harmony with what the public has been asking. But the question remains if the framework will be indeed applicable and what the conditions will be for purchasing the NSO-Group's Pegasus technology. As stated in the previous sections, there are multiple allegations that the Pegasus

software was licensed to authoritarian regimes and governments with poor human right records in order to target journalists, activists, governmental opposition and anti-corruption dissidents, as in the case of Mexico. There are still many controversaries regarding this topic because the NSO-Group fails in taking public actions that would give a sense of accountability and culpability for the misuse of their technology. At the same time, there is still a contradiction to be seen from behalf of the financial investor, Stephan Peel, who publicly admits the flaws in the companies' ethical conduct and has promised to ensure that since his investment and that the companies' technology will *only* be used for lawful purposes, which nonetheless hints the unethical misuse in the past. These promises unveil the same issues that have been raised by various NGO's and civil society organizations regarding the possibility for the misuse of NSO-Group's technology and that the ethical domain and the legal regulations regarding the spyware industry are in need of constant regulation and adaptation to the changing environment.

By concluding the application of the CSR Framework on the case of interest and answering the research question at the core of the study, it can be stated that considering the data that has been analysed the NSO-Group's adherence to the principles of CSR is precarious. As the analysis suggested, the only domain where it can be argued that the tech-company adheres to the mentioned principles is the economic one, because both in the legal and ethical domains significant issues came to the fore. Based on the products of the content analysis and the categorization that has been established, the NSO-Group follows a clear pattern of responding to possible allegations by justifying their actions with the narrative that the products developed by the company are helping in fighting (cyber)-crime and preventing terrorism. But little is stated regarding the culpability of the company considering the manner in which their technology was used by their buyers and it seemed that little has been emphasized on the duality of the technology and the extent to which it could endanger basic human rights, of course in the context of technological misuse. The NSO-Group, as one of the main suppliers of such sophisticated spyware technology, has failed in displaying any form of will, capability or sense of liability in preventing the present abuses and diminishing the human rights abuses and the unethical use of their technology. Moreover, the NSO-Group continues to market their software in countries where there are high level of corruption and poor records of acknowledging basic human rights such as Mexico and the UAE, fact which emphasizes that there is no 'lessons learned' from the previous cases of misuse considering the technology is still being sold and used in those areas.

6. Discussion and Conclusion

As seen from the analysis with regards to the NSO-Group's adherence to the CSR framework, the main debate breaks down to what can be categorized as (il)legal behaviour of the company and what can be categorized as (un)ethical. Accounting on the economical approach of the company, overall it appears that the NSO-Group follows the expected behaviour of CSR as proposed by Schwartz & Carroll (2003), by selling their technology under the economic principles and aiming at maximizing their profits. From the performed analysis, there is no evidence of financial mismanagement in the organizational behaviour of NSO-Group and its investors.

The main debate that can be drawn and further discussed from the analysis regarding the extent to which the NSO-Group adheres to the principles of CSR breaks down to the 'legal' vs. 'ethical' debate, because most of the companies' actions can be considered legal, but unethical. As put forward by Schwartz and Carroll (2003), all three domains of CSR (i.e. economic, legal and ethical) must be met by a company in order to state that a business is in complete harmony with its environment and the society. Whether the NSO-Group can be considered to adhere to the three core principles of CSR is highly questionable. Throughout the analysis, it has become clear that the NSO-Group does not fully meet all the characteristics that are issued in their official aim with respect to the principles of CSR. The idea is that it cannot be stated that the NSO-Group is in full compliance with the law because its actions prove the contrary. The fact that the NSO-Group has sold its Pegasus software to governmental entities in countries with weaker human rights principles or where the legal standards are questionable illustrates that little accountability is shown on behalf of the company. One aspect that could explain this issue could be that after all the NSO-Group is a business, and the aim of any business is to make profit. Thus, the NSO-Group does not take into account the ethical and legal standards of the governments' they market their technology to, but focus more on the aspect of maximizing their profit. Be it this case, the NSO-Group still undermines its statements of selling the technology solely to governmental entities for the purpose of preventing terrorism and fighting crime by breaching the basic principles of the Wassenaar Arrangement. Even though, as mentioned in the application of the legal domain to the companies' approach, Israel is not an official member of the Wassenaar Arrangement, it has taken the role of obeying to the stated principles, as if it would be a formal member. The economic aspect has a significant weigh when discussing NSO-Group's responsibility towards the society in general, because profit

maximization shall not occur by any means. Any means, in this case could be seen in the case of Mexico, where the NSO-Group has licensed the Mexican government to use Pegasus, but the purpose of using the software was not only to eliminate crime and terror, but to target innocent individuals such as journalists, politicians and lawyers because they were holding sensitive information that could shed a different light on the Mexican government.

6.1 Theoretical and Practical Implications

In the remaining of this Master thesis, both theoretical and practical implications will be discussed, as well as the limitations of the research and thoughts regarding further research that can be done in order to expand the exploration and comprehension regarding the sale of targeting surveillance technologies while at the same time adhering to the core principles of CSR.

Starting with the theoretical implications, the present research has thoroughly analysed the extent to which the NSO-Group adheres to the principles of CSR, when marketing their Pegasus Software. The focus was on the case of Mexico, but for broader implications the limits shall not be set there and aim at a greater data set for a broader understanding of the issue. Targeting surveillance technology is becoming more of a demand in today's society in order to aim at digitalizing the manner in which governments and intelligence agencies make use of sophisticated and complex technologies to target criminals and prevent (cyber)-terrorism. The findings that have been presented in this Master thesis support the current trend in the cyber-security literature as well as from the perspectives of human rights documentations, business-ethics and the available legal documents regarding the issues concerning export control. The aim was to shed innovative light on previous researching regarding the topic of digital surveillance in the private sector by analysing the current and pressing issues that civil society has been put through when cases of misuse of such technologies occurred. The results of this thesis present the facts that there are both legal and ethical issues with the NSO-Group tech-company in the manner in which they sell and export their technology, in this case the Pegasus software. Moreover, as stated in the conclusion of the 5th chapter where the answer to the core question was given, the lack of accountability plays a significant role in the current debate. As seen from the results of the content analysis, the NSO-Group's CEO has stated that, if instances of misuse will be indeed spotted by the company, the technology will be permanently shut down in those areas, fact which is not in harmony with the given results. If that would have

been the case, the numerous instances of abuse throughout a period of two years would not have been the reality in Mexico and the Mexican government would not have been licensed to continue in using Pegasus.

Moving towards the practical implications, the present Master thesis aimed at presenting relevant findings for the current professional practice in the sphere of digital surveillance in the private sector. More and more companies produce sophisticated technologies and software's that can aid states, governments and intelligence companies in fighting crime and terror. At the same time, such technologies are categorised into the 'dual-use' technologies group, which implies that besides their aimed purpose, such technologies can have a different impact on the populations and individuals which is beyond the initial scope. This is the case with the NSO-Group's technology, where per their website clear aims are stated and the actual reality shows instances where these aims are not met and their technology is misused, fact leading to immense ethical and legal issues.

As the present research examined the extent to which responsible corporate behaviour applies in the case of Israeli based NSO-Group, one of the main practical implication of the Master thesis is to have an impact on future research and/or policy decision in the field of digital surveillance and to raise awareness regarding the importance of the economic, legal and ethical domains of business in delivering their product to the society. Constant research and an improvement in the existing regulations surrounding the relationship between CSR and corporations, as well as the high responsibility businesses have towards the society as a whole. When businesses, such as NSO-Group are delivering technologies with a high degree of duality and sophistication, the level of responsibility shall automatically rise in order to ensure the safety of the users, buyers and society as a whole. Therefore, this study can be further applied in the research of how the spyware industry is perceiving their responsibility level and nonetheless, what are the steps that could lead to a more regulated industry.

6.2 Limitations and Further Research

The rapid technological developments will continuously set the scene for new emerging issues regarding the use and misuse of such advanced spyware technology to reach the public sphere. The dangers with dual-use technology, as in the case of the NSO-Group's Pegasus Software will continue to be present in our contemporary society and becoming a target for such technology by governmental entities could become the reality of many countries. The political, social and economic environment is highly important in this scenario, as seen in the case of Mexico. Mexico is already a country where distrust in the governmental bodies is highly voiced by the Mexican citizen and where big social and economic inequalities can be perceived. Furthermore, as seen already the legal standards in Mexico as well as the importance of human rights are highly questionable as well as the freedom of speech, press and expression. Journalists, human rights activists, politicians and lawyers appear to have a hard time doing their job, as seen from the Citizen Lab Reports and have become targets of governmental officials because of the sensitive information they were having.

The main limitation of the study is the lack of direct official documentation that has been found available regarding the issues of interests, such as accurate and detailed information on how the NSO-Group has, for example, legally obtained and at the same time maintained its export control, taking into account the many instances of being publicly blamed for the misuse of their technology. Furthermore, another limitation is the fact that there was no means by which to directly and openly communicate with members of the NSO-Group, in order to receive information regarding the BEC (Business Ethics Committee) of the company. Rumours regarding that members of the Board of the NSO are at the same time members of the BEC were circulating on the media, but due to the lack of evidence and reliability of the information this issue was not taken as an argument in the present thesis. It would have enriched the results of the thesis to perform a comparative analysis between countries where misuse of the technology has been marked, but due to space limitation solely the case of Mexico was analysed.

For further research it can be considered to perform a statistical analysis for acquiring a big picture regarding the manner in which countries where Pegasus has been sold to perceive NSO-Group's technology and the extent to which the software is actually used as intended per its official aim. Comparing statistical data which explicitly states the instances where Pegasus was

used to prevent cyber-crime and terrorism and the instances in which Pegasus was used for malicious purposes could convey a strong argument in terms of how dual-use technology, such as Pegasus, is mostly being used by its buyers. Moreover, further research is greatly needed in the area of legal regulation of spyware technologies and ensuring that the regulations and policies in place are not breeched by the users of the technology and business who produce such technology, as the case of Israeli's NSO-Group fully adhere to the CSR principles and do not make use of the available loopholes.

References

Ahmed, A. (2017, December 25). Using Billions in Government Cash, Mexico Controls News Media. Retrieved from https://www.nytimes.com/2017/12/25/world/americas/mexico-press-government-advertising.html

Ahmed, A., & Perlroth, N. (2017, June 19). Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. Retrieved May 29, 2020, from https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

Amnesty supports legal action to stop chilling spy web. (2019, May 13). Retrieved from https://www.amnesty.org/en/latest/news/2019/05/israel-amnesty-legal-action-stop-nso-group-web-of-surveillance/

Anstis, S., Deibert, R. J., & Penney J., (2019). *Submission of the Citizen Lab to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on the surveillance industry and human rights*

Asokan, A., & Ross, R. (2019, September 12). Cyber-Intelligence Firm NSO Group Tries to Boost Reputation. Retrieved May, from https://www.bankinfosecurity.com/cyber-intelligence-firm-nso-group-works-to-repair-reputation-a-13085

Bazaliy, M., Hardy, S., Flossman, M., Edwards, K., Blaich, A., & Murray, M. (2016). Technical Analysis of Pegasus Spyware. *An Investigation Into Highly Sophisticated Espionage Software Available online: https://info. lookout. com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis. pdf (accessed on Jan 10, 2019)*.

Bergman, R. (2019, November 1). Weaving a cyber web. Retrieved from https://www.ynetnews.com/articles/0,7340,L-5444998,00.html

Carroll, A. B. (1999). Corporate social responsibility: Evolution of a definitional construct. *Business & society*, *38*(3), 268-295.

Cathcart, W. (2019, October 29). Opinion | Why WhatsApp is pushing back on NSO Group hacking. Retrieved from https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/

Citizen Lab, NSO-Group Statement 2018 https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf

Deibert, R. J., & Poetranto, I. (2017). Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović.

Epstein, E. M.: 1987, 'The Corporate Social Policy Process: Beyond Business Ethics, Corporate Responsibility, and Corporate Social Responsiveness, California Management Review 29(3), 99–114.

Fidler, M. (2015). Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis. *ISJLP*, *11*, 405.

Fischer, J. (2004). Social responsibility and ethics: clarifying the concepts. *Journal of Business ethics*, *52*(4), 381-390.

Flyverbom, M., Deibert, R., & Matten, D. (2017). The governance of digital technology, big data, and the internet: new roles and responsibilities for business. *Business & Society*, *58*(1), 3-19.

Globalwitness.org/about-us https://www.globalwitness.org/en/about-us/

Global Witness Press Release https://www.globalwitness.org/en/press-releases/stephen-peel-has-stepped-down-member-global-witness-board/

Human Rights Watch, Mexico's National Human Rights Commission. *A Critical Assessment* February 2008, Volume 20, No. 1 (B). Retrieved from https://www.hrw.org/sites/default/files/reports/mexico0208_1.pdf

Kane, A. (2016). How Israel Became a Hub for Surveillance Technology. *The Intercept*, *17*.

Kirchgaessner, S., & Swaine, J. (2019, June 18). WhatsApp spyware: UK firm promises new 'respect for human rights' following allegations. Retrieved from https://www.theguardian.com/world/2019/jun/18/whatsapp-spyware-israel-cyber-weapons-company-novalpina-capital-statement

Kirkpatrick, David D. "Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says." *The New York Times*, The New York Times, 2 Dec. 2018, www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html.

Iliescu, A. S. (n.d.). Israeli Import, Export and Cyber Regulation and Enforcement. Retrieved May, from https://www.shibolet.com/export-and-cyber-regulation-and-enforcement/

Israeli Law: https://knesset.gov.il/constitution/ConstIntro_eng.htm

Kurbalija, J., & MacLean, D. (2007). Internet governance.

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to operations in 45 countries*.

"Mexican President Denies Spying on Journalists, Lawyers and Activists." *BBC News*, BBC, 23 June 2017, www.bbc.com/news/world-latin-america-40376891.

Business & Human Rights Resource Centre, 13 Sept. 2019. "Novalpina Capital Buys Spyware Co. NSO Group & Commits to Helping It Become More Transparent.", www.business-humanrights.org/en/novalpina-capital-buys-spyware-co-nso-group-commits-to-helping-it-become-more-transparent.

NSO-Group Values: nsogroup.com/about-us/

NSO-Group Governance: nsogroup.com/governance/

Nichols, S. (2020, April 4). NSO Group: Facebook tried to license our spyware to snoop on its own addicts – the same spyware it's suing us over. Retrieved from https://www.theregister.co.uk/2020/04/03/nso_facebook_pegasus_whatsapp/

Open Letter Citizen Lab 2018 https://citizenlab.ca/wp-content/uploads/2018/09/Citizen-Lab-NSO-Group-09-2018.pdf

Open Letter NSO Statement 2018 https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf

Perlroth, N. (2016). How Spy Tech Firms Let Governments See Everything on a Smartphone. *New York Times, September, 2,* A1.

Peppet, S. R. (2014). Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, *93*, 85.

Raghavendra, T. S., & Mohan, K. G. A Conceptual Framework for Securing Privacy and Optimization of Personally Identifiable Information.

Scheer, S. (2019, September 10). Cyber firm NSO vows to tackle human rights misuse. Retrieved from https://uk.reuters.com/article/us-cyber-rights-nso/cyber-spying-firm-nso-to-follow-human-rights-guidelines-idUKKCN1VV11

Schwartz, M.S., & Carroll, A.B. (2003). Corporate social responsibility: A three- domain approach. *Business Ethics Quarterly, 13*(4), 503-530.

Scott-Railton, J., Marczak, B., Guarnieri, C., & Crete-Nishihata, M. (2017). *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*.

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. (2017). *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*.

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. *Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware*.

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. *Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware*.

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. (2017). *Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware*.

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. *Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware*.

Scott-Railton, J., Marczak, B., Anstis, S., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. (2018). *Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague*.

Scott-Railton, J., Marczak, B., Anstis, S., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. *Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware*.

Silverstein, R. (2019, February 19). After Buying Major Stake in Israeli Cyber-Attack Firm, NSO Group, Global Witness Director Quits Board. Retrieved from https://www.richardsilverstein.com/2019/02/18/after-he-buys-major-stake-in-israeli-cyber-attack-firm-nso-group-global-witness-director-quits-board

Stahl, L. (2019, May 29). CEO of Israeli spyware-maker NSO on fighting terror, Khashoggi murder, and Saudi Arabia. Retrieved from https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/

Tenz, C. (2019, February 19). 'There is no free press': Media freedom in Mexico: DW: 19.02.2019. Retrieved from https://www.dw.com/en/there-is-no-free-press-media-freedom-in-mexico/a-47568810

United Nations, Human Rights Committee, *Human Rights Council Consideration of initial Report of Israel, CCPR/C/81/Add.13,* (9 April 1998), available from https://www.un.org/unispal/document/auto-insert-188794/

United Nations, General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc A/HRC/23/40 (17 April 2013) available from https://undocs.org/A/HRC/23/40

The Waasenaar Arrangement https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf

Appendix

1. Codebook Content Analysis

CODE [2]	CATEGORY [3]	DEFINITION [4]	INDICTAROS [5]
1	NSO-GROUP: Prevention of cyber-crime and terror (Justifications)	Action taken that help in the prevention of cyber-crime and terror	- Actions taken by the organization in preventing crime and terror - Justifications on the use/sell of Pegasus - Justifications regarding NSO's customers
2.	NSO-GROUP: (Un)Lawful behaviour (Justifications)	Actions of the organization that are in compliance with the law (or not)	-NSO-Group's software is only sold to governmental entities and sovereign actors → activities are to be found in countries with weaker human rights records and/or questionable legal standards
3.	NSO-GROUP: Economic implications (Justifications)	Action that maximize profits (+ the actions and involvement of their financial backers)	-Improving public image by not focusing only on maximizing the profits but acting according to their core regulations -Statements of their financial backers -Actions taken by the NSO-Group to increase profits
4.	NSO-GROUP: (Un)Ethical behaviour (Justifications)	Actions taken by the organization that follow the societal norms (or not)	-Actions that follow unwritten standards/and norms -Only ethical issues concerning privacy and data protection of individuals are included

5.	NSO-GROUP: Sense of liability & accountability (Justifications)	Actions taken by the company that show they are (or are not) accountable for their actions	-Actions that show a sense of accountability and responsibility (towards society, human rights and overall CSR & business ethics)

[1] **Unit of analysis: Paragraphs & Sentences**

[1]Unit of analysis refers to the part of the text (sentences, paragraphs etc) that will be assigned to a given category.
[2]Code refers to the number/letter by which each category will be identified during coding (e.g. 1,2,3).
[3]The categories must answer the RQ.
[4]Definition refers to the meaning of each category.
[5]Indicators are pointers that "indicate" how to actually identify each category when you analyse a document.