Kristiina Kronholm

PAID FALSE REVIEWS AS CYBER DECEPTION

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

ABSTRACT

Kristiina Kronholm
Paid False Reviews as Cyber Deception
Jyväskylä: University of Jyväskylä. 2022, 65 pp.
Information Systems, Master's Thesis
Supervisor: Soliman, Wael

This master's thesis examines paid false reviews as cyber deception. Paid false reviews are not a distant and an abstract phenomenon somewhere on the internet platforms since they affect heavily on available information on internet which is available for consumers. False reviews take place on the scale of information security as a threat to reliability of information and they have severe potential to disrupt markets and services and decrease the reliability of information. A concept of crowdturfing, a mass manipulation campaign with an economic motive is presented as a key concept of paid false review's feature as a cyber deception. Specifically smaller organizations are facing severe issues, since they have fewer resources to spend when preparing against malicious attacks and cyber threats. The research questions of this study are defined as following: How familiar organizations are with paid false reviews? What actions organizations are doing against paid false reviews at the present time? What are organizations' future plans to deal with paid false reviews? The research approach is selected to be a concluded literature review of internet deceptions following a theoretical framework of deception theory and its tactics. Empirically the issue of paid false reviews is observed through interviews of 20 organizations by structured interviews. The research angle is observing organizations, which contained 13 micro and small organizations and 7 medium and large-sized organizations. The key findings of the study were concluded as the lack of knowledge of the concept or misunderstood belief of paid false reviews as harmless and predictable, current awareness and spontaneous reaction in the situation of upcoming attacks, and lack of interest towards actions in the future. Also, the interviewees did have clear uncertainty how to recognize a paid false review. The implications to theory and practice of this thesis are that paid false reviews a form of deception is from the point of organizations as detached and abstract threat which has no clear definition, and which can be easily disrupted with trolling or other non-economical motive base deception. This topic needs to be studied further and this thesis directs to point out the lack of serious preparedness. From theoretical aspect there are multiple ways to defend against paid false reviews, but the practical awareness and actions of the organizations are not coherent yet.

Keywords: Paid false review, Internet Deception, Cyber Deception, Crowdturfing

TIIVISTELMÄ

Kristiina Kronholm
Maksetut valearviot internetpetoksena: kohteena mikro- ja pienet yritykset
Jyväskylä: Jyväskylän yliopisto. 2022, 65 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Soliman, Wael

Tässä pro gradu -tutkielmassa tarkastellaan maksettuja valearvioita kyberpetoksena. Maksetut valearviot eivät ole kaukainen ja nimeämätön ilmiö internetalustoilla, vaan ne vaikuttavat voimakkaasti internetissä kuluttajan saatavilla olevaan tietoon. Valearviot esiintyvät internetin alustoilla ollen uhkana informaation luotettavuudelle. Ne voivat häiritä markkinoita ja palveluita. Crowdturfingin käsite eli massamanipulointikampanjointi, jolla on aina taloudellinen motiivi, esitetään maksetun valearvion keskeisenä piirteenä. Erityisesti pienemmille organisaatioille valearviot ovat vakava ongelma, koska niillä on vähemmän resursseja käytettäväksi haitallisten hyökkäysten ja kyberuhkien torjunnassa. Tämän tutkimuksen tutkimuskysymykset ovat seuraavat: Kuinka hyvin organisaatiot tunnistavat maksettuja valearvioita? Mitä toimia organisaatiot tekevät tällä hetkellä maksettujen valearvioiden suhteen? Mitkä ovat organisaatioiden tulevaisuuden suunnitelmat maksettujen valearvioiden suhteen? Tutkimusmetodi koostuu kirjallisuuskatsauksesta käsittäen internetpetosten teoreettisen käsitteistön, sekä petosteorian ja sen taktiikan teoreettisen tutkimuskehyksen. Empiirisesti maksettujen valearvioiden ongelmaa tutkitaan 20 organisaation haastatteluilla. Tutkimusnäkökulma keskittyy mikro- ja pienorganisaatioiden, sekä keskisuurteen ja suurten organisaatioiden vastausten havainnointiin. Tutkimuksen keskeiset havainnot koskivat käsitteen tuntemattomuutta, sekä väärinymmärrettyjä uskomuksia valearvioista vaarattomina ja ennustettavina. Lisäksi nousivat esiin nykyhetkellinen tietoisuus ja valmistautumattomuus tulevien mahdollisten kyberhyökkäysten tapahtuessa. Kiinnostuksen puute tulevaisuuden varautumista kohtaan oli myös keskeinen havainto. Organisaatioilla oli myös selkeä epävarmuus siitä, miten tunnistaa maksettu valearvio. Tämän tutkielman vaikutukset tieteelliseen teoriaan ja käytäntöön pyrkivät siihen, että maksettujen valearvioiden uhka vakavasti otettavana petoksena on organisaatioiden näkökulmasta irrallinen ja täsmentämätön uhka. Niillä ei ole selkeää määritelmää ja ne voidaan helposti sekoittaa provokatiiviseen kirjoittamiseen (trollaus) tai muuhun ei-taloudelliseen motiivin pohjalta tehtyyn petokseen. Tätä aihetta on tutkittava edelleen ja tämä opinnäytetyö osoittaa puutteen organisaatioiden valmiudessa. Teoreettisesti on useita tapoja puolustautua maksettuja valearvioita vastaan, mutta organisaatioiden käytännön tietoisuus ja toiminta eivät ole vielä yhdenmukaisia olemassa olevan tiedon suhteen.

Asiasanat: Maksettu valearvio, Internet-petos, Cyber-petos, Crowdturfing

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Online shopping and services have become a daily thing for consumers and their habit to search for products and information (Bigne et al., 2005; Román, 2010). The most fluent way to search information to back up purchase decision is to read other consumers' online reviews. Internet users have access to various sites that offer reviews and other users' experiences to help when they are forming opinions and making decision on purchasing something or not, or when they evaluate which service provider is reliable. (Puccinelli et al., 2009) In the thesis a literary review of concepts of internet deception and crowdturfing is presented. Internet deception can be defined as an action on online platform which targets to give malicious or manipulative information to the reader and lure them to act in a way that serves the deceiver's motives, such as economic benefit (Caspi & Gorsky, 2006; Hancock, 2007; Järvenpää & Grazioli, 2003). The key concept of the thesis, crowdturfing, can be defined by Lee et al, (2015), Li et al. (2017), Wu & Liu (2017) as a deception form that contains a crowd of deceivers who aim to manipulate a target by creating masses of false information, such as reviews or comments. These deceivers act by economical interest and the action is conducted by an agent, who has an assignment from a customer with malicious intentions to gain benefit. The study strives to emphasize the phenomenon of crowdturfing by relating it to a context of crowdsourcing, which means a group of people working for a paid fee on online platform completing tasks (Song et al., 2015). A phenomenon of crowdturfing as mentioned above, where an organization has manipulated reviews by appointing a third party with an economical motive to produce them. However, there are multiple tactics to deceive online. An internet deception is defined as an act of manipulation of information online with an objective to make someone do something that they would not consider without the manipulated information (Chen & Huang, 2011; Everett et al., 2016; Tsikerdekis & Zeadally, 2015).

Cyber deception has many forms, and it is not anymore about phishing emails, users' fake profile pictures or deceptive websites. Modern deception according to Zhang and Ko, (2013), contains highly complicated features, and targets to manipulate information to gain monetary benefit. Small and micro-

organizations are highly dependent on their online reviews on platforms. Also, medium, and large-sized organizations do suffer from the consequences of paid false reviews, and the thesis empirical method does contain conducted interviews of these organizations. This thesis studies organizations from the aspect of paid false reviews targeting them. The deceivers lure victims on technological platforms; they target to mislead consumers, deceive companies and its ecosystems by manipulating data. This phenomenon is a key concept of this thesis: crowdturfing. Crowdturfing is also known as malicious crowdsourcing, which has become an important security problem (Song et al., 2015; Wells et al., 2014; Wu & Liu, 2017). The consumer's right to reliability of information presented online of organizations needs to be studied more carefully. The essential problem gathers in difficulties for users of online review platforms to detect deception (Yoo & Gretzel, 2009), when there is no certain information. The importance of studying this topic can be defined to consumer's or internet user's right to access information that is correct and reliable. Mukherjee et al. (2012, p. 1) describe the process of deception: "a group of reviewers who work collaboratively to write fake reviews", which "is even more damaging as they can take total control of the sentiment on the target product due to its size." Trying deliberately mislead readers by giving unfair reviews does lead to manipulation of reviews that lure customers to avoid or prefer some service or product (Mukherjee et al., 2012). Motivation of the topic focuses on finding new aspects to the problem of internet platforms and internet deceptions.
The research questions are formed as follows:

1. *How familiar organizations are with paid false reviews?*
2. *What actions organizations are doing against paid false reviews at the present time?*
3. *What are organizations' future plans to deal with paid false reviews?*

The study uses Deception Theory which divides deceptions into tactics that hinder the formation of a correct representation of the core and to simulative tactics, which are tactics that foster an incorrect representation of the core. The research angle is however chosen to be a tactic of fostering the information in a form of manipulating reviews online. The current situation where a platform or internet user is deceived, and the responsibility is also falling on the user is not a positive future result. Societies and companies must step forward by enacting laws and obeying them. The globalized cyber responsibility is processing to an extent to became crucial to the human daily life and therefore as a human right. The writing process is based on the book of Hirsjärvi, Remes, and Sajavaara (2010) by analysis and practices of seeking and analyzing articles and research findings. The theoretical part is a summary of articles from the field of Information Systems science.

This thesis summarizes paid false reviews from the perspective views of the organizations as a victim, as well as by observing the phenomena from the angle of deception theory (Grazioli & Järvenpää, 2003). The thesis presents and summarizes relevant academic articles of internet deception from the perspective

of false reviews and adapts the theoretical relevance and research gap for the thesis. Theoretical framework is collected from key articles of Deception Theory and articles of paid false reviews as deception tactic. This aims to give the research questions a theoretical frame which places the dimensions of organizations awareness, acts and preparedness to the concept of paid false review as a deception tactic. An empirical study is conducted by interviewing organizations to find out novel information regarding the current state of their acts, awareness, and preparedness to false reviews from these three-dimensional aspects. Selected method to answer the research questions was chosen to be qualitative study with conventional content analysis (Hsieh & Shannon, 2005). The empirical study is conducted with structured interviews, containing questions that cover the research area and research questions. To discover this, altogether twenty Finnish organizations were interviewed: 13 participants were from small and micro-organizations, and seven participants were from medium and large-sized organizations. Small and micro-organizations, since they have a more vulnerable position on the market and fewer resources to defend against paid false reviews. However, seven medium and large-sized organizations' interviews are presented also to gather information of company size affecting the answers and findings.

Study findings are categorized by past familiarity, current awareness, and future plans towards paid false reviews. The answers of small and micro-organizations are categorized to separate phenomena and are presented to be findings how micro-organizations have gathered some knowledge, but they lack preparedness against paid false reviews. Micro and small-sized organizations's representatives explained that they did have emerging concerns towards paid false reviews, but the disbelief that they would be an interesting target did decrease their commitment to spend resources to preparedness against paid false reviews. Also, the concept of paid false review was not clearly defined and understood among the interviewed organizations, and they did have assumptions that they would recognize paid false reviews easily. Micro and small organizations' attitudes were relying to a situational reaction.

The implications based on the findings of the study does lead to an increasing concern of malicious information on the internet, but also the lack of interest to tackle the issue. On the other hand, the research points out the threat and lack of current responsibility of the organizations providing crowdturfing and which are unwilling to remove or observe truthfully their reviews.

2 LITERATURE REVIEW

This section is a summary of literature sources defining internet reviews and deception. The structure of the literature review contains definition for false reviews, methods to cyber deception and gives insight into ethical questions regarding online deception and to tools to defend with. Selection of the articles is done by either evaluating the articles and their publishers within www.julkaisufoorumi.fi website or by selecting them by relevance, by novelty, or exceptional relevance, such as citation popularity. Search words and combination of the search words were the following: "internet deception", "deception online", "internet review", "false review", "crowdturfing", "deception tactics", "paid reviews". Utilized search platforms are Google Scholar and Information Systems Science publishers and conferences. Oxford Dictionary, among other sites is used to define certain terms and concepts, that are not defined by publishers related to the Information Systems Science.

2.1 False Reviews

Knowingly transmitting a message to a receiver with the intent to foster a false belief or conclusion is deception (Buller & Burgoon, 1996). After the development of the Internet and the rise of home computers since 1980's, people have become further omitted to internet connection, doing business and sales on the Internet, and searching for customer reviews. The growing interest towards internet reviews is inevitably increasing because of the globalized rapid transformation of information and technological revolution: increasing number of people have access to Internet. This has led to increasing amount of search engines containing reviews (Norman Burrell et al., 2020; Mukherjee, Liu, & Glance, 2012). Growing numbers of internet users are searching reviews to back up their decision on consuming products and services. There is multiple research and studies that offer various concepts and taxonomy for online deception. Based on the observed literature, a clear definition of a paid false review does not have a ubiquitous

concept which would be widely acknowledged. The core definition of this thesis' key concept, a paid false review is chosen to be described through the following features of previous research shown in table 1.

TABLE 1 Table of concepts defining a paid false review's features.

Definition	Source
Demotes or promotes a product, masses of usage.	Mukherjee et al., (2012)
Authentical-looking and impacts the target's reputation.	Lappas, (2012)
Under and overrating, unfair treatment of products.	Lim et al., (2010)
Reviewer (agent) has economical motive; they get paid for the review(s) from external customer.	Wang et al., (2012)
Written by a reviewer that writes only positive or negative reviews.	Liu et al., (2010)
Written by benevolent agents, goal is to manipulate consumers beliefs.	Glazer et al., (2020)
Written without a real purchase or experience.	Anderson & Simester, (2014)
Unclear to distinguish based on structural properties.	Yoo & Gretzel, (2009)

The definition of paid false reviews can be defined as a review written by crowturfing deceivers targeting to have an effect on the organizations service or a product in a malicious way, and by exploiting the power of masses as Lee et al., (2015), Song et al., (2015) Wu and Liu, (2017) have noticed. A clear and specific, distinguishing feature for paid false review is a written content that either lavishly demotes the product or service or promotes it (Glazer et al., 2020; Mukherjee et al., 2012). One characteristic trait that describes paid false reviews is that the reviews are extremely authentic and there is no clear certainty that the reviews are containing false information. Therefore, it is vital to exploit analytical tracking strategies instead of trusting instinctive observations. As Lappas (2012) and Lim et al. (2010) have studied, paid and false reviews that aim to manipulate are genuine, but appear to have a strong punctuation to a more positive or negative way. In comparison a genuine review usually consists of somewhat neutral, negative, and positive remarks. When analyzing masses of reviews Liu et al., (2010) have concluded that a suspicious individual reviewer had a tendency to write only negative or only positive reviews in their record of reviews. However, it is not a clear process to divide false reviews from real ones, especially when many websites do not contain any restrictions for reviews; the form is an open field or there are no control whether a reviewer has genuine experience (Yoo & Gretzel, 2009). The key characteristic also for the concept of paid false review is that it is paid by external customer and therefore it fulfils the requirement of economical reward that is paid for a review which was not written otherwise for any reason (Wang et al., 2012). A paid false review does not

have any real-life contact with products or services. It does not matter, whether the reviewer would be contacted or later investigated why the review had a certain punctuation (Anderson & Simester, 2014).

As mentioned in the deception theory, in beginning of the century: "victims of internet deception suffer financial damage, the psychological discomfort of being victimized, the loss of time necessary to file complaints and refund requests, and the theft of private information. (Järvenpää & Grazioli, 2003, p. 93)" However, the damages of the effects of misleading information can be severe for the company. Economical phenomenon of trust issues may occur when consumers have blurred image whether to trust or distrust a market. Ignatuschtschenko, Roberts, and Cornish, (2016) clarify the concept of cyber harm, which deception proceeded in internet is, as describing it understudied and lacking concrete concepts and definitions. The theory framework is leaning on relatively recent studies regarding crowdturfing as an ethically discussed phenomenon and economic damage for the companies and consumer. Regarding main theories of Järvenpää and Grazioli, (2003) and Mason, (1986), this study's theory focuses on finding the behavior of the current internet users, also focusing on the phenomenon of internet deceptions and crowdturfing that needs to be taken into further notice undoubtedly. The ethical principles of aspects of information and user's right to approach it can be found also in the motivation of the study (privacy, accuracy, property, and accessibility).

These attacks are i.e., according to Moens, Aksehirli, and Goethals, (2013) plausibly tracked down by frequent user mining (FIM), which is a technique to extract wanted knowledge from information source. In this case of false reviews, a certain frequency of certain user writing similar reviews, could be one of the extracted signs to detect false reviews. The false reviews can be found from similar webpage for different products, or different pages for the same product. (Moens, Aksehirli, & Goethals, 2013; Mukherjee et al., 2012). Also, (Song et al., 2015), have gathered detection method against crowdturfing, by detecting target objectives of crowdturfing tasks.

As Chen and Huang, (2011) have punctured in their studies, deception is a major form of crime, defined as a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver in order to achieve disbelieve or manipulation. Deception has been around from the time of the first sale ever made. The internet and business is increasingly (Pagani, 2013) emphasizing IS technologies to achieve results and catch up people and customers. As the e-business culture is rapidly growing especially for the sake of global crisis such as current COVID-19 pandemic, the importance of online business and therefore fake review appearance for a common customer is inevitable.

An ethical business practices in retailing online (Román, 2010) is including understanding the opportunity to perpetrate an online deception. A deception is always increased by three reasons. At first, the Internet is a representational environment in which consumers form decisions about products based on cognitive representations of reality. Therefore, a normal face-to-face interaction or social ability to track deception is not reached as in normal physical sale

situation. Secondly, the Internet lowers the entry and set up costs for new retailers or sellers, making it relatively easy for a deceptive online retailer to set up a storefront on the Internet. This could appear to look as genuine as its legitimate counterpart. The differences between large and small companies are not clearly visible in website's appearance which is a crucial enabler to deceive consumers to think that the company has a certain relevance in the market and therefore achieve trust. Third, the identity of the parties involved in communications and transaction is relatively difficult to verify. The Internet allows companies from different legal and regulatory environments to present their offerings without a strong international legal and consumer protection system, which would cover the protection of the consumer and create a reliable marketplace. Deception is inherently criminalized by law in various countries or trade unions but the actual observation and standards to police by authorities is not yet to completed. (Roman, 2010).

In the field of IS, deception is studied within business disciplines already during decades (Biros et al., 2002). The essential finding when observing IS systems is that deception is detected only in half of the cases, when a human is observing the potential deception. Deception detection is seen as a relevant resource whether it is about internal or external decision making. Experience is seen as an important factor to co-operate with.

The concept of crowdturfing could be placed in the year 2006, according to Wu and Liu (2017), which has a meaning that the theories of crowdturfing as internet deceptions is not yet formed. This thesis implicates to find relevant currents of the research, but also forming a consensus regarding the multiple undefined concepts. As Lee, Webb, and Ge (2015) have concluded in their study, some major platforms have already prepared to face crowdturfing and analyze the problem. However, an average internet user is facing difficulties and responsibility to seek information and share it with other users without facing the threat of being deceived. An insight for the theoretical background is also to cover some technical responses to the deceptions, that are an ongoing phenomenon. Crowdturfing, also known as malicious crowdsourcing, has become an important security problem (Song et al., 2015).

> "Traditionally, people assumed that malicious activities were generated automatically by automated systems, so existing systems dependent on the assumption are easy to be bypassed by real users. Crowdsourcing facilitates the attacks through gathering crowdturfing workers and connecting them with potential customers. Sophisticated attacks of crowdturfing intimidate ordinary users with overwhelming unwanted information." (Wu et al., 2017, p.3).

The globalized ecosystems of the societies, business and consumer's everyday life becoming increasingly exposed and related to customer reviews. Deception as a service is named to be crowdturfing from the upcoming academical bases addressed in next chapters. Deception as a Service requires further acknowledgement to be research as an independent concept of Information System science. The businesses are focusing strongly on user

valuations and reviews which punctuates the modern internet user culture to be based on other peoples' opinions. This culture has a potential to be endangered and manipulated from economical benefitting motives which can be originated usually from rivaling businesses or market areas. The theory framework is leaning on recent studies regarding crowdturfing as an ethically discussed phenomenon and economic damage for the business and consumer (Mukherjee et al., 2012). Theory focuses on this umbrella term by finding the behavior of the current internet by the crowdturfers and the companies, but also focusing on the phenomenon that needs to be taken into further notice undoubtedly. As Järvenpää and Grazioli, (2003) have presented in their theory, the tactics of the deception theory are essentially focused to observe internet user behavior in the direct concept of interaction. The concept of crowdturfing is as a part of deception as well as a phenomenon of the ecosystem of platforms providing false reviews. The future behavior and impacts of mass behavior and manipulated market reviews are in the need of updating, until to cover modern internet behavior. However, the deception theory is a core theory in this thesis to describe the field of fake reviews. The phenomenon of crowdturfing as a recognizable tool to mislead market has been noted an independent topic approximately from the early 2000's and is taking place as an object to observe economical risk factor (Li, Caverlee, Niu, & Kaghazgaran, 2017, Soliman & Rinta-Kahila, 2020).

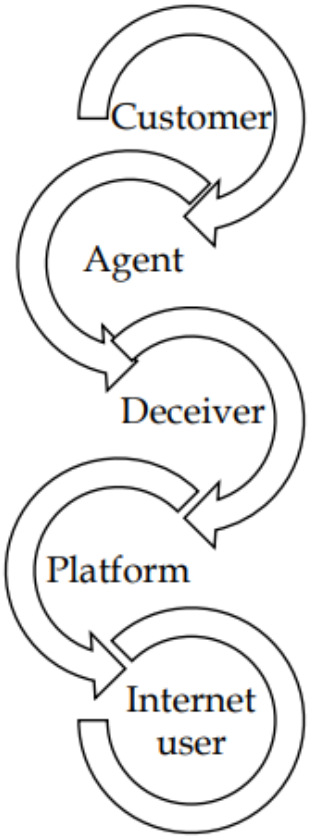

FIGURE 1 Information flow in Crowdturfing (Soliman & Rinta-Kahila, 2020).

As Rinta-Kahila & Soliman, (2017), Song et al., (2015), Wang et al., (2012) have studied, the concept of crowdturfing includes several actors, first the customer who orders false reviews to gain profit either by positively promoting their own service, or by negatively discrediting competitors' revies. The agent manages the service chain and provides deceivers who execute the malicious crowdturfing actions. This always includes the economic motive for the deceiver in a form of monetary reward or other benefit. It is a complex question whether the platform providing the services should be able to track or manage false reviews. In the end, the crowdturfing flow damages the information available for internet users by falsifying the reviews of services and products. (Rinta-Kahila & Soliman, 2017; Song et al., 2015; Wang et al., 2012).

2.2 Methods to Cyber Deception

The current state of users becoming further attached to internet and developing their buying process on the base of reviews is undisputed. The motive for deception to achieve economic or social benefit is the most common motive to a person to behave if they choose to deceive others. The deception as a concept leads to a monetary, social, or other benefit that profit that deceiver claims. A deceiver may have a motive to write discredited reviews due to a personal reason such as boredom or other non-economical reason or reason related to a customer experience, but in this thesis, the motive to perform paid false reviews is observed as to be always monetary based, as Hancock, (2007) and Zhang and Ko, (2013) have studied the concept the online deception:

> "According to Hancock (2007) … First, deception activity must be intentional or deliberate, which means unintentional mistakes or misrepresentations do not count as digital deception; second, the purpose of the deception has to be misleading or creating false beliefs, thus, joke and irony are not considered as deception; third, this is more relevant to digital deception; technologically mediated message has to be the information control mechanism in the deception activities." Zhang & Ko, (2013, p. 2)

False reviews are Internet ratings, which according to Glazer, Herrera and Perry (2020), Lappas (2012), Mukherjee, Liu, and Glance (2012) are increasingly used by individuals and organizations for their decision making in the selection of services and products. Internet ratings have become increasingly important, since they have an impact on how we sort out services and businesses, business to consumer (B2C), and how businesses rate each other as well as trying to compete, business to business (B2B). Ratings have power to optimize certain services over another by sorting them out i.e., Google or TripAdvisor on top lists by service quality and customer satisfaction. Low ratings lead to invisibility on different platforms, high rating to increased interest (Anderson & Simester, 2014). The power of reviews is inevitable.

As Li et al. (2017) have stated, when false reviews appear as an organized phenomenon and familiar as employment relationships it is a question of crowdsourcing. Theories based on crowdturfing clear out that the agent and deceiver are in a clear employment relation or at least the agent gives a compensation to the deceiver. When deception is presented as a phenomenon of crowdsourcing, it could also be seen as servitization of a product (which are manipulated false reviews). The concept of servitization is basically the equal of any product being crowdsourced and improved with some incentive. As Zhang and Ko (2013) have stated in their conference publication, the deceivers, the source of deceptive messages, should be investigated further.

Over the past decade, cyber security is considered as an uprising topic in the global internet. The so called fourth industrial revolution is at hand, which means that the complexity of socio-technical systems will increase due the ubiquitous digitalization and automation of technical processes (Dunn Cavelty & Wenger, 2020). Crowd-sourcing systems may pose a challenge to existing security mechanisms deployed to protect Internet services, as Wang et al. (2012) state in their study. This path then leads to a phenomenon called crowdturfing. Crowdturfing is justified as a concept of either profit or entertainment. Accepting the risks of Information Security Governance and direct responsibility, and that serious personal consequences, specifically legally, could flow from ignoring information security was already accepted in early 2000 (Von Solms & Von Solms, 2005).

Consumers are accessing global internet as an information seeking platform and utilizing internet reviews to back up their decisions made online. By Chen and Huang (2011) it seems that the future of electronic commerce is now being shaped largely by social computing and networking, and that these advances pose a significant influence on contemporary business models and strategies. It is uncontradicted that internet reviews are here to stay as a relevant way of seeking information and producing it. The user has two roles; user is reading reviews and evaluating the value of the information and then forming a decision- on the same time users are writing and producing new information and reviews.

As a feature of modern society, users seek increasingly more information to complete their buying process and favor the most convincing in one's opinion on various factors (Puccinelli et al., 2009; Zhuang et al., 2018). The buying process is often based on opinion of other users in negative or positive context. Optimization of search platforms such as www.googlereviews.com is also offering reviews, such as Google Review which presents other users' opinions' average grades. Users are increasingly accessing internet through various platforms and from various devices such as smartphones (Li et al., 2017). The current scale of internet sales and businesses is rapidly increasing as mail shipping, online retail, and megatrends to shop from home is trending almost as a social distancing (due to Covid-19 -virus). Websites offering information and reviews are also established, as well as the online retailers themselves are presenting customer value reviews. The common practice to organize surveys after buying a product is also inevitably broadened and therefore brought closer

to the user and customer. Customers' opinion is the key factor defining business' success.

The manipulation of the internet reviews is becoming extensively popular. Manipulation could happen in organized or unorganized matter. The internet user has several problematics to recognize misinformation as well as the misinformation which misleads one to a monopolized or poor service abilities. As Anderson and Simester, (2014) documented: "5% of product reviews on a large private label retailer's website are submitted by customers with no record of ever purchasing the product they are reviewing". This leads to a conclusion of a tangled market effect by malicious manipulation.

Various restaurants, online shops and other online businesses have experienced economic losses due to false reviews that mislead potential customers and relegate them. Most of the services and product retailers have internet sites that provide in some point automatic updates of customer reviews. The reviews are not necessarily checked out and inspected, which in that case brings an opportunity to deceivers. The first acknowledged study regarding the phenomenon of online fake review detection was published in 2007 (Zhang, Zhou, Kehoe, & Kilic, 2016). The consequences of crowdturfing whether intentional or unintentional has later shown to be a current and accurate trend. As Ivanova and Scholz (2017)have concluded in their article about dynamic aggregation of online reviews, that popularity of online ratings is combined to the fact that retailers clearly have a strong incentive to manipulate ratings to boost their sales not to forget the anonymity of online environments which creates an easy way to write and publish fake reviews. The reviews are seen as tool to boost revenue and measure the products profitability.

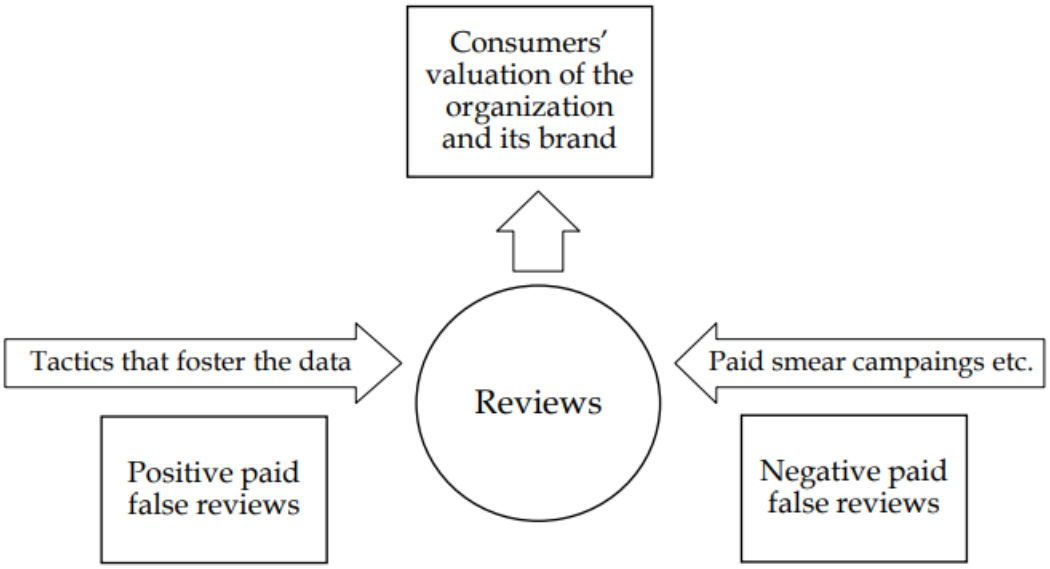

FIGURE 2 The effect of manipulation process and crowdturfing (Kim & Johnson, 2016; Song et al., 2015).

The target for paid false reviews is always to impact on victim organizations' brand and image on the eyes of consumers (Kim & Johnson, 2016; Mayzlin et al., 2014; Song et al., 2015). Malicious crowdturfing achieves to manipulate the review base and to cause twisted valuation for the benefit or favor of the deceiver. How the value is in fact created is a complicated process that includes various segments, but one is the effect of manipulation to consumers' valuation process which eventually leads to substandard decisions that would have not been done otherwise. The lack of trust towards reviews is eventually an outcome when the consumers face disappointments. (Kim & Johnson, 2016; Mayzlin et al., 2014; Song et al., 2015).

2.3 Ethical Questions and Defensive Tools

Almost every twentieth review could be potentially shown as false. The human ability as Biros et al. (2002) to detect deception is strongly related to sensitivity and training, being only 50& accurate nevertheless. This brings a question of whether the responsibility of the platforms should be appointed to eliminate the issue, as well as inform the users. The lack of clear regulation (Román, 2010; Riquelme & Román, 2014) and responsibility convention to companies and platforms. The emerged development of Internet has strengthened consumers' position, giving them a tool to gather information and to form and publish their own opinions. The better accessibility to different information sources comfort consumers to be less susceptible towards potential deceptive offerings online, as well as steering their perceptions and behaviors. Also, retailers' reputation and image has become wide open and vulnerable to the reactions of customers, given the unparalleled scope and diffusion that Internet allows of consumers' negative comments about potential deceptive online and traditional sellers (Riquelme & Román, 2014, 405-406). The motive to manipulate and improve bad reviews to achieve business profit and better image amongst customers has become further fundamental in the word of Internet, sometimes by any means necessarily.

As Mason (1986) has concluded, there are ethical issues of internet users' vulnerabilities on Information age. The first, privacy, covers the concerns regarding the information that should be revealed and what should not. Information technology is acknowledged to be an uprising trend since 1980s and two forces threatening privacy are technology's abilities to surveillance, (communication, computation, storage, and retrieval in malicious ways) and the increased value of information in decision making.

Information is increasingly valuable to policy makers; they covet it even if acquiring it invades another's privacy (Mason, 1986, (Mason, 1986; Tenbrunsel & Messick, 2004)). Accuracy is an issue regarding the validity of the information and how authentic it is. Information ownership and issue regarding the

responsibility to be vigilant in the pursuit of accuracy in information. People have an ethical right to rely on information they face online. Property, or more likely intellectual property rights, are one of the core elements in information age. The presumption that someone has a right to possess, reuse, copy or otherwise use an immaterial right is legislated by law. Property is an ethical issue due to the problem, who owns information and therefore the right to use it or manipulate it or present it in context. Accessibility is an ethical issue related to social economics. Not all have full access to information, time nor devices. Also, the educational fundamentality to detect misinformation and react to it by evaluating it valuable and reliable to make decisions is not equally actualized. These ethical problems are issuing the modern world of internet and its users, as well as the controversy of ethical behavior as acknowledged and unaware is a modern situation in the internet. (Mason, 1986; Tenbrunsel & Messick, 2004).

As Rinta-Kahila and Soliman, (2017) have concluded in their study of ethical issues of crowdturfing, accuracy is a fundamental question of authenticity, and is concerned when decision maker is misinformed. A potential and more generalized solution would be to enable the actualization of these, be relying on various web services that perform the review valuation and analyze the content. A false review could be analyzed for example by www.yelp.com, www.fakespot.com or page that covers Amazon reviews www.reviewmeta.com which are open databases for anyone accessing the internet. Social media and other users have posted online practices and common advice that help to track down the reviews. Also, by Abbasi, Zhang, Zimbra, Chen, and Nunamaker (2010) have presented, that several AI solutions spot reviews by statistical learning and this is most likely plausible. Statistical variety collected from databases and analyzed to achieve tendencies such as exactly similar reviews for different products, also on different platforms. The quantity of the false reviews is reaching higher numbers more increasingly, which evidently creates a market need for a services to root out maliciously intended or unjustified reviews (Abbasi et al., 2010; Chen & Huang, 2011). This market need is justified since the consumer must efforts to find reliable products in the end. On the other and, the market may as well become corrupted and unreliable, which would lead to a situation where the consumer is losing their trust to products and services. In a healthy environment of competition there is then a marketing gap for consumers, as well as businesses and organizations to seek reliable data sources that offer reliable information. Also, the common motivation for society and its political economy as well as economic allies, such as European Union, is to diminish and find economical actors that are not following rules and obey laws and orders. Ethically there is a strong pressure to maintain reliable databases and platforms. Currently there is a global discussion ongoing regarding the power that mega sized companies have among consumers (Kim & Johnson, 2016; Lupton & Southerton, 2021). In social media platforms a single user or consumer can rapidly effect on multiple other users by choosing a micro community or group as target. Therefore, information that is not confirmed or reliable may also spread

fast. This is, however, another topic on false information genre, which has an alternative motive besides monetary value or damage.

Influencers as agents creating false reviews were mentioned by one interviewee and they placed it on a category of grey area. When thinking about the concept of false review, what keeps conditions to benefit economically and without any real expertise, real motive or will to write a review, it is difficult to say if this phenomenon is a false review or not. On the other hand, it's about normal marketing methods and using personal brands to market and recommended (Jin et al., 2019) products for consumers that are seeking real life experiences. Personal brands can be even created digitally (Sands et al., 2022) in the form of creating virtual influencers that do not exist in real life. Consumers seek for peer evaluations and form their opinion based on other peoples' opinion, or peoples' who they admire. However, this thesis focuses on elaborating the term false reviews by focusing on the organizations attitudes towards it - even though an interesting future topic would be how a consumer forms and evaluates their opinion from different sources. In this case, may false reviews be more easily hidden in means of using influencers as writers. Companies hiring influencers to promote products and services on social media platforms is definitely considered to be an increasing and predominant phenomenon, especially in B2B marketing (Cartwright et al., 2022; Neumann & Gutt, 2019), as well as the next question of how uprising crowd influencing will be on its impacts. As Yoo and Gretzel (2009) have studied, only few webpages have restrictions or management regarding false reviews, or who is able to write reviews in any manner. Therefore, a defensive action would be to track down genuine customers, who have authentic experience of the service or product. This could be controlled with a policy of verified receipt number, or other similar action. Earlier trends to trail false reviews are punctured how numerously frequent a single reviewer has generated them or how multiple equivalent reviews have appeared on a particular platform. This is currently in transition by new techniques. For instance by dynamic rating aggregation by Ivanova and Scholz, (2017), false reviews and their damage can be measured and predicted, by creating a fraud-resistant ranking algorithm.

How organizations and their employees sense themselves in the world of reviews is the key questioning of this thesis. The theory and literature do identify multiple issues, which are generated by paid false reviews in conjunction with the techniques that deceivers utilize to manipulate reviews online. However, the knowledgeableness of organizations during the current time, experiences and attitudes towards future threats and opportunities is a topic that needs to be studied further.

3 THEORETICAL FRAMEWORK

The theoretical framework is leaning on relatively recent studies regarding crowdturfing as an ethically discussed phenomenon and economic damage for the companies and consumer but also exploiting the main theory as Deception Theory by Järvenpää & Grazioli (2003) and their studies regarding the area of internet deceptions in the early 2000s. The novelty of the study area is also an important framing subject and thesis aims to justify the subjects by overviewing and evaluating the theoretical substance from the publishers of the IS. The novelty of the area is also an important framing factor in the subject and thesis aims to justify the subject by overviewing and evaluating the substance from the publishers of the IS. As referred in the earlier chapter, well-known and distinguished articles are covered in the background section and the current gaps and possible future research areas are aimed to find and described. The concept of crowdturfing could be placed year 2006, according to Wu and Liu (2017), which has a meaning that the theories of crowdturfing as internet deceptions is not yet formed.

The interest of businesses to became reviewed by consumers' opinions is a growing trend that determinates organizations brand value in the eyes of a consumer. However, the reliability of the reviews is not necessarily verifiable, because they may not accurate, but false reviews. The information accuracy is facing problems when evaluating if something is true or false. According to Mason (1986), the information and its users have four ethical issues: privacy, accuracy, property, and accessibility. In this thesis, the topic focuses on the issue of accuracy, which ensures the principle that information found online is reliable and the user has a right to exploit it. The accuracy problem of false online reviews is observed through the user angle of deceptions and how they are made in online context. When the deceiver has a designed and planned action to influence on a certain review without an accurate information, the phenomenon is called crowdturfing (Song et al., 2015; Wang et al., 2012; Wu & Liu, 2017). The false reviews are created by certain deceptive tactics exploited online. The thesis uses Deception theory as a main theory for consumer and business deception online,

which concludes that deceivers select tactics as function of their targets and their identity.

3.1 The Deception Theory

The deception theory as a theory describing tactics that deceiver chooses (Järvenpää & Grazioli, 2003) is a core theory for this thesis. The following chapters aims to form initial idea of the content of the deception theory, whereas deception tactics are presented on a table. The deception theory is exploited to explain and understand tactics to explain modern deception style and preferences towards organizations. Theoretical part aims first to explain internet deceptions and their appearance, and by observing false reviews from the user perspective. The Theory divides and explains seven various tactics, which either hinder the formation of a correct representation of the manipulated information or the core or foster an incorrect representation. In a nutshell the theory explains the dynamics of a deception:

> "The theory of deception defines deception as a cognitive interaction between two parties under conflict of interest. One party, the deceiver, manipulates the environment of the other party, the target, so as to intentionally foster an incorrect cognitive representation of the target's situation and instigate a desired action, one the target would be unlikely to take without the manipulation." (Järvenpää & Grazioli, 2003, p. 95).

This manipulation strategy can be divided through seven tactics(Grazioli & Jarvenpaa, 2000; Järvenpää & Grazioli, 2003). First three are tactics are named as masking, dazzling, and decoying and these are tactics that hinder the formation of a correct representation of the core (item involved in a social exchange). The four last are tactics that foster on incorrect representation of the core: mimicking, inventing, relabeling and double play. The first tactics work by preventing the target from engaging in the process of representing key pieces of information about the deception core. The four more tactics attempt to induce a desired representation of the deception core. The table aims to attach the modern forms of internet deceptions regarding fake reviews as a main deception to observe and how they are created by different motives. Each of the models are presented. Deception theory explains crowdturfing as a phenomenon. (Grazioli & Jarvenpaa, 2000; Järvenpää & Grazioli, 2003).

In this thesis, deception theory is expanded to explain the modern behavior of internet deceiver and what kind of tactic they use. Deception is presented to be simultaneously performed by the deceiver, who can also be a victim of a deception. Modern day deceptions tend to adjust to a tactic of relabeling, where the deceiver describes the core and its characteristics in a questionably favorable way by producing false information. The deception theory is no longer sufficient when observing modern day internet deceptions and explaining a tactic deceiver

chooses when punctuating false reviews. However, relabeling as a fostering tactic producing manipulated information is relatively adjustable to expand to modern day circumstances, that would explain a tactic closest to a false review.

TABLE 2 Deception taxonomy. The deception theory combined with tactics of Johnson, Grazioli, & Jamal (1993) and observed through modern theories relevant to internet deceptions.

Form of tactic	**Description**	**Modern day example of deception**	**Sources**
Masking	Deceiver commits or eliminates crucial characteristics of the core.	Cyber-attack, manipulation	Bellekens et al., (2019), Mayzlin et al. (2014) & Hancock, (2007
Dazzling	Deceiver obscures or makes difficult to access crucial characteristics of the core. Deceiver makes up information about the core.	Spam & Sybil attacks	Mukherjee et al., (2012), Wang et al. (2012)
Decoying	Deceiver attracts target's attention away from crucial characteristics of the core.	Phishing	Bhat & Abulaish (2014), Tsikerdekis & Zeadally, (2014) Tsikerdekis & Zeadally, (2015)
Mimicking	Deceiver assumes an otherwise legitimate identity, or core copies a legitimate item.	Phishing, pagejacking	Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker Jr, (2010) & (Grazioli & Jarvenpaa, 2000)
Inventing	Deceiver makes up information about the core. Core does not exist or is ascribed unrealistic characteristics.	Scam	Caspi & Gorsky, (2006), Hancock, (2007) & J. Zhang & Ko, (2013)
Relabeling	Deceiver describes the core and its characteristics in a questionably favorable way.	Crowdturfing, fake reviews	Lee et al., (2015), Soliman & Rinta-Kahila, (2020) & Wu & Liu, (2017)

Double Play	Deceiver maliciously suggests that the target is taking unfair advantage of situation or that the core is exchanged against deceiver's will.	Masked manipulation	Chen & Huang, (2011), (Johnson et al., 2001)

3.1.1 Masking

Manipulation is an user-generated online reviews are increasingly important when it's about consumer's purchase decision (Mayzlin et al., 2014). The motive behind attempt to manipulate a certain information regarding a review of a product or service is often variously conducted. Online manipulated review has got several methodologies to detect these reviews, which are often related to factors, such likely neighborhood with another similar service, as Mayzlin et al. (2014) suggest. Bellekens et al. (2019) and Hancock, (2007) have an approach that the concept of deception is related to several complex motives, such as lying on a dating site to gain popularity. The ethical issues that are originated from manipulation through multiple aspects during the two decades are more closely to effect reviewers and users seeking information. Spam and Sybil attacks Mukherjee et al. (2012) are described as a phenomenon of opinion spamming refers to human activities (e.g., writing fake reviews) that try to deliberately mislead readers by giving unfair reviews to some entities. This is possible to obtain through a frequent itemset mining for opinion spamming. The spammers are tracked down by observing the data that they have produced in the system, which is a review page. Sybil attacks are a deception of using fake user as a source of information by Wang et al. (2012). This behavior is typical to a person or a group of persons that are manipulating a review page in order to achieve negative or positive image.

3.1.2 Dazzling

Phishing as an identity theft, in order to mislead and delude someone to reveal personal information and possible collect it as Bhat & Abulaish (2014), Tsikerdekis & Zeadally (2014) Tsikerdekis & Zeadally (2015) have described, is a deception that decoys as someone or somebody would be a trustful friend or a website to confide. A malicious website could impersonate as a trustful site to type one's personal information such as address, age etc. Fake reviews present a false impulse for a user to trust services or persons that have not clear and honest business logic.

3.1.3 Decoying

Pagejacking, or when Internet pages are mimicked to present as something fraud and misleading. The form of this deception is decreasing, because the frequency of certificates and other technological precautions that protect the victims (Abbasi et.al., 2010;Grazioli & Jarvenpaa, 2000). The fake pages are targeted to track down by various analysis of statistical data, such as Abbasi et al. (2010) suggest in their study for Statistical Learning Theory, which is created to track down suspicious activity. Problem of pagejacking is that there is no evident authority or common norms to detect false pages, except the user's awareness to seek suspicious activity and possible enthusiasm to turn in these pages to the original victim that was jacked, or even to police in certain country where the web-page's domain is located. However, the page jacked companies and communities are often exploiting certificates, well designed websites with accurate contact details and other reliable information, which diminishes the current number of this deception form.

3.1.4 Mimicking

As mentioned earlier, crowdturfing is a growing and relatively new phenomenon. The taxonomy of the concept is emerging, as Soliman and Rinta-Kahila, (2020) and Wu and Liu (2017) describe the global market is moving fast forward on Internet. Crowdturfers act upon economical motive to make a manipulated review, in positive or negative set. Consumer is struggling extendedly in the jungle of internet market to seek reliability and accuracy. Target platforms face multiple challenges detecting, preparing, tracking, and remedying false reviews. Effective methods to verify such behavior or reveal a content is not coherently created or even criminalized in this date, except some exceptions. Companies embracing internet reviews are facing a challenge verifying misuse and false behavior in the context of economic interest. This leads to a responsibility of the consumer and internet user. The detecting of the paid review written by a human customer is furtherly studied and technologically approached, but in the end, there is a little chance to evaluate technically who is giving a truthful response. This leads to a situation where a consumer must reflect one's internet environment more carefully. Twitter, by Lee et al., (2015), as an example is facing multiple attacks of crowdturfers in a form of fake bots, and therefore forming algorithms that detect suspicious activity. It is common that crowdturfers are related to campaigns that appear to be led by grassroots participants but are actually supported by intentionally masked sponsor (Wu & Liu, 2017).

3.1.5 Inventing

Masked manipulation is a deception, when one is observing the deception form of masked manipulation, it takes an interaction situation between the deceiver and targeted person(s). Deceiver maliciously suggests that the target is taking

unfair advantage of situation or that the core is exchanged against deceiver's will. This could also been observed as phishing phenomenon to lure the victim to reveal their personal information such as bank account details or credit card numbers. (Chen & Huang, 2011; Johnson et al., 2001). Masked manipulation aims to lure the user to trust the person. The trust is usually formed with relatively simple tactics, such as offering some advice for the victim, which might be perfectly accurate advice, but later obviously this formed trust is used against the victim.

3.1.6 Relabeling

Relabeling as a tactic fit to modern-day crowdturfing, excluding the ecosystem of crowdturfing companies and as a concept. Relabeling, which is described as transaction expressly to mislead, selling questionable investments over the Internet as sound financial opportunities (Hancock, 2007) ought to be included when talking about crowdturfing in tactical level. Relabeling effects to mislead consumers in a form of tactic that should be observed in the context of false reviews. Chen and Huang (2011) have studied among two hypotheses, that deceivers are more likely to use the relabeling tactic against an individual than against a business target. Also, deceivers that purport to be businesses are more likely to select the relabeling tactic than deceivers that purport to be individuals. The first hypothesis was supported, but there is no evidence, that deceivers that purport to be businesses will use the relabeling tactic more often than deceivers that purport to be individuals. Relabeling as a tactic seems to be a suited and adaptable tactic that would pursue consumers and manipulate information in reviews. Johnson et al. (1993) concluded that individuals observing relabeled information have not a clear tactic or strategy to converse misinformation. More likely, the mislead reviews or manipulated information is tracked down by various factors, such as social factors which are complex, real-world-based, task in which success does not seem to depend directly on specific experience or incident.

3.1.7 Double Play

As Chen and Huang (2011) and Johnson et al. (2001) have made remarks in their studies, a deception done by exploiting double play, by conceiving a fictional situation where a deceiver lures a victim to take action with an offer that sound a rare opportunity and has to be take hold on very quickly before the opportunity is long gone. This tactic is exploited by deception theory model to individuals more than organization since it appeals feelings and deceiving "luck".

3.2 Paid False Reviews as a Cyber Deception

Paid false reviews are targeting to manipulate the consumer's image and valuation of a certain company or a product (Lappas, 2012). The Study is motivated by the Deception theory explaining and summarizing different models of deceptions and tools and motives to perform them. However, the theory does not answer completely to a rapidly changed and upcoming development of the global society as mentioned on the previous section. The deception theory has a limited ability to handle user as a victim and a deceiver at the same time. The research gap is aimed to cover by observing a deception tactic of relabeling (fostering) information. Tactic is described a modern tactic of producing deceptive information (Chen & Huang, 2011; Hancock, 2007). The research gap is placed between the user's double role: as a victim, but also as a deceiver.

Why and how a deceiver becomes a victim, is an essential question to this study aims to answer. Deception as a Service is placed to a large phenomenon of crowdsourcing and its variations. This study tries to cover the new concept of understanding fake reviews as a part of a form of crowdsourcing. The phenomenon of crowdturfing (Rinta-Kahila & Soliman, 2017) includes factors and subjects which are customers, who are a business practice, firm or other facet to pursuing business profit and sales. The customers approach an agent who is often a business unit providing employees or labor for the crowdturfing attack. It is possible to enable and organize crowdturfing also inside the business organization benefiting the deception. Customer and agent are the same unit in this occasion. The deception is performed when the employing agent gives an assignment for monetary (or other benefit related to monetary compensation) to a deceiver. The deceiver writes a fake text entity and posts or delivers it to a platform providing reviews. Internet user reads the review and possible forms an opinion towards the product or service on hand. The review could be positive or negative, however often either strongly for example zero starting from five or complete five star of five scale, depending minimum to maximum. (Zhuang et al., 2018; Rinta-Kahila and Soliman, 2017).

There are not yet multiple ways for company to prepare and protect themselves from paid false reviews. However, as malicious tactics (Biros et al., 2002; Mundra et al., 2013; Wu & Liu, 2017) for spreading false information increases, there is an incentive to develop antidotes for these issues. These tools are technically sighting to track down suspicious activity, for example an identical review on different product. These tools sight to take actions after the damage has been revealed and therefore deleting the malicious activity. Tools for defending can also be categorized by Straub and Welke (1998), Detmar, Straub and Nance (1990) in their studies as categorized according to previous studies to deterrence, prevention, detection and repair. Deterrence as a theory and a model is a famous strategical model that aims to create sanction or other frighten a deceiver to fulfil their malicious actions. This can also be done by cyber security

actions such as informing users and warning against deceivers' tactics. Prevention can be defined as strategy that shields information, such as a practice where a reviewer must verify that they have in real life used services or products. For example, a receipt with individual number series that can be used as a key in a review page is a way to exploit prevention model. Detection, as described above, is a model that tracks down suspicious activity and keep a record of them for example. Repair is an action that aims to have remedies for the influenced and damaged values. An example of this can be punishing the deceiver and recovering monetary or public refunds. Malicious online reviews are presented on online platforms, but they could be proceeded also on online social network, especially when a certain maliciously motived parties are fueling masses to attack certain companies. When a person represent oneself as someone who the deceiver is not as to achieve other than economic benefit, for example to have friends as Caspi and Gorsky (2006), Hancock (2007) and Zhang & Ko (2013) studied, the motive is considered user to behave other than external incentive. However, this form of phenomenon is not deliberately considered as a deception in this study, because the motive to deceive is seen as not organized, economical or repetitive from the nature as deception in the context of information system science would require. As the globalized and rapidly booming usage of social media, interactive media communities and other platforms requiring social interaction (Buckels et al., 2014) is increasing, the adverse effect of vast masses of data lures deception in the form of internet trolls. Motive to deceive is acknowledged to be antisocial when a person tries to achieve usually malicious reactions from the target group. False review written by antisocial motives is a possible scene, but nevertheless rarer phenomena than antisocial behavior in other form of communicate or produce information.

To reach out reactions for fun and themes such as of "boredom, attention seeking, revenge, enjoyment, and a desire to cause damage to the community" are named motivations for trolling (Buckels et al., 2014). However, trolling may be attached to a phenomena of mass trolling or organized trolling, which brings the term close to the phenomena of crowdturfing. The essential difference is the motive to troll and the mentioned motivations of social behavior. However, there are no factor present of gaining economic benefits for a troll that is trolling only for fun. This phenomenon is excluded from the concept of paid false reviews.

The research questions were placed as followings: How familiar organizations are with paid false reviews? What actions organizations are doing against paid false reviews at the present time? And what are organizations' future plans to deal with paid false reviews? The deception theory is linked to the research questions by explaining taxonomies of seven different deceptions (Johnson et al., 1993), and by observing them as a context of deceiver pursuing the victim in business areas. In the deception theory, the deceiver is a person or a business, but in this thesis the aim is to observe the preparedness of the companies to the malicious behavior.

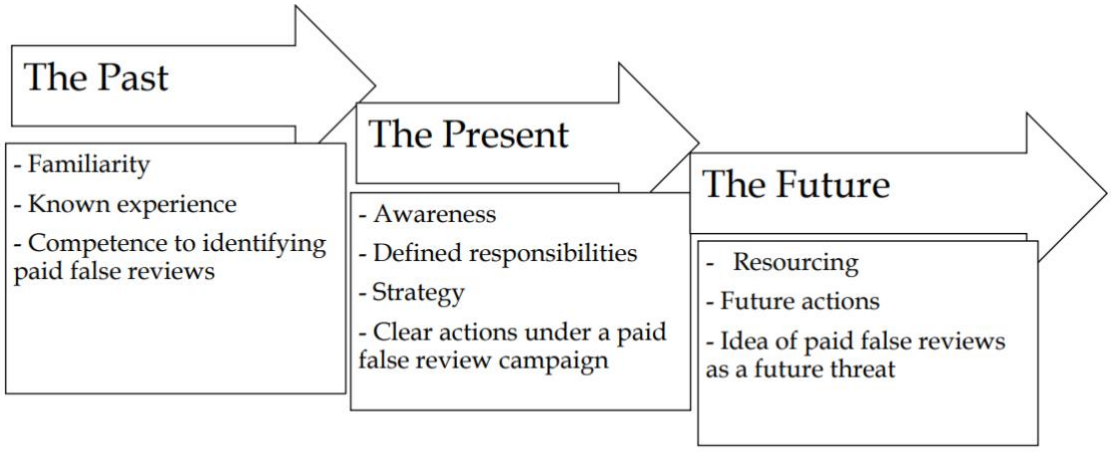

FIGURE 3 The research dimensions.

The key angle for this study is to bring forth perspectives of the past, present and future attitudes and opinions of organizations which have interest to their reviews online. The study framework focuses to cover and explain by the deception theory, a field of cyber deceptions and their vast adaptability to manipulate consumers, other businesses and reliability of internet reviews. Also, the concept of paid false review is established on the theoretical framework, and it supports the clarification of the research gap- not having a clear connection between organizational online review strategies and awareness with preparedness to avoid market manipulation. The management of online reviews is no longer an external nebulous concern. The past, current and future attitudes of the organizations should be studied further with the framework of clear concept and deception taxonomy. Deception theory provides an angle for false reviews as a phenomenon and is not including the subject of crowdturfing as an existing phenomenon. The existing phenomenon needs to be examined further; crowdturfing, which has created a user ability slot, whereas the users have become enablers to produce false reviews as well as being targets exposed and vulnerable to read them in order to make decisions on consuming or forming an opinion.

4 METHOD

This section describes the empirical part of the thesis. Methodology chosen for the research in empirical part was a process, which finally defined the method to be interviews of organizations suitable for the paid false review as targets, which were Finnish small and micro-organizations. Medium and large organizations were also interviewed to access to relevant research data regarding organizations' strategies when organizations have more available resources. In this section the methodology is described, and process of the empirical part is clarified. The empirical study is proceeded with a method of collecting data by a qualitative structured interview with nine questions. After collecting the material, it was arranged and analyzed. Summary of the analysis with the theoretical background creates a novel and coherent viewpoint of paid false reviews, and how they are attached to the science field of Information Systems science and cyber deceptions.

4.1 Research Method: Structured Interviews

Choosing qualitative method for the study's empirical section captures source material in a best possible way to cover aspects that are not measurable with quantity, amount intensity or frequency (Hunder, 2011). The study uses a qualitative interview approach which is proceeded through interviewing companies' representatives by face-to-face open beforehand structured interview to cover aspects of personal experience and various levels of studied issue of paid false reviews. Because of the aim to maintain integrity and truly reach honest opinions and possible reactions, the questions were not unveiled to the interviewees. Data was collected from 20 various organizations and businesses. Goldkuhl (2019) and Hirsjärvi et al. (2010) explain, that there are multiple ways to manage a qualitative study. An approach to analyze the data and organize findings was selected to be conventional content analysis. The results were openly analyzed as described with qualitative method of conventional content

analysis (Hsieh & Shannon, 2005), by coding the interview data. Keywords, findings and codes were defined and discovered during the data analysis. This also includes, that there are tables that contain coded data, a scope that places answer to a category section. Such as familiarity or existence of pursuing strategy is presented and measured by simple "Yes/No/Partially" and explained by number of existences, a quantity. The study combines qualitative and quantitative methods in the results and discussion section to produce measurements that clarify the results clearly and explain the findings.

The primary selected empirical group was micro and small companies. The selected organizations were picked from different business areas, but common nominator was that they had clear target groups that were most likely able to use search engines such as Google or other platform such as Apple store which contained reviews of the service or product provided. The participants were, in other words, interested in their public image offered to the consumers, potential and existing. Also, the size of the company/organization was various since the target was to cover as many business areas and/or entities as possible. Further study of false review, as later addressed on section 7: Future research, would suggest quantitative research methods to find out relations between business areas, company size or special customer group, or ability, or another variant. This thesis was aiming to answer to the research questions:

1. How familiar organizations are with paid false reviews?
2. What actions organizations are doing against paid false reviews at the present time?
3. What are organizations' future plans to deal with paid false reviews?

The Collected data was transcribed and later analyzed to findings. The data was also anonymized without any knowledgeable details, names, or any other special characteristics. Line of business, position in the organization and size were documented. Also, in the last section elements are found that are later analyzed to be relevant for phenomenon of false reviews effecting organization's image or brand online. Organization's business area is scoped to cover the main business field/main strategy target and defined to locate in certain economical industry area, for example retail or charity work. Position of the interviewee is reported as title or high-level hierarchy position. Company size, which are slotted as micro, small and small & medium-sized, or large. These definitions of company sizes are presented according to list of www.tilastokeskus.fi (2022) with how organizations are measured according their revenues and number of employees.

The empirical part was analyzed with anonymous results, because of the sensitivity of the security subject or possible information which could be used in advantage by competitors or to harm the organization in other way by exploiting their business strategies, tools, and approaches. However, the companies' broad business areas and the interviewees position are later presented in a table summary to clear out the research's target group. The interviews were performed in Finnish (or English, when necessary) and later transcribed in English. The attendants were found from around companies' business representatives, i.e.,

Chief of Executive operations or Chief of Information officer. The information is collected by arranging an interview situation that is approximately 1 hour long and the attendants answered to structured questions as freely as possible. Interviewer conducts the interview asking questions. Interview is arranged as structured method; however, the attendants are encouraged to answer openly from their own experience. The empirical part aims to answer to the research question: How do organizations react to, prepare against, and observe false reviews?

The empirical questions were placed to identify factors and phenomena of the organizations' past familiarity, current awareness, and future actions and plans towards paid false reviews. The results were categorized to three classes, that contained different findings regarding the actions and attitudes of the interviewees. The results are presented from general thoughts (past) and then defining the phenomenon (present) and finally spotting the future actions that formulate the answer to the research question.

After contacting of the organizations, the interviews were set up with the organization's representative and agreed to be held in a suitable time. All of the interviews were conducted via internet and phone, either by calling and recording the interviews or by using video conference application. In the beginning of each interview the thesis' writer did interduce herself by name and as a master's student from University of Jyväskylä. The thesis' topic of paid false reviews with an empirical research theme was defined: How familiar organizations are with paid false reviews, what actions companies are doing against false reviews in the present time and what are their future plans? After that an ethical explanation of anonymity was read and it was confirmed that the interviewee did understand it. 19 of the interviews took place in Finnish language and one in English. The results, summaries and quotations are translated by the thesis writer with the help of university dictionary https://www-sanakirja-fi.ezproxy.jyu.fi/. Interviews were recorded, transcripts and a table of data was created after them. In the beginning, the concept of paid false review was clarified with the interviewees. This was done by reading them aloud a definition:

> "A paid false review: It's an untrue review of a product or a service, appearing in some online platform. A false review is written by a paid reviewer in order to manipulate, by promoting or discrediting products, services or company's image." Glazer et al., (2020), Lappas, (2012, Lim et al., (2010), Liu et al., (2010), Mukherjee et al., (2012), Wang et al., (2012).

After the definition, there was a small section for small talk, free discussion, or questions for the interviews regarding the concept of paid false review. Also, there was a warmup question for interviewees, which was not recorded, to think about their own behavior on the internet and how they feel about negative and positive reviews. The interviews were held and intended to be as in a structured model, but if the interviewees did make interesting claims or otherwise had intriguing notes the interviewer did ask further refining questions. Also, the interviewee had an opportunity to return and elaborate and widen their previous

answers. It could be said that a reflective and retrospective atmosphere was cherished and sought after.

Interviews were recorded and conducted individually in a calm atmosphere, and they took approximately half an hour overall with preparation question and pre-questions included. One warm-up question was asked, which was about how the interviewee themselves behave with online reviews: are positive or negative ones more convincing and how they would describe their behavior as consumers? Also, further pondering was cherished in the interview situation to gain more inductively interesting findings.

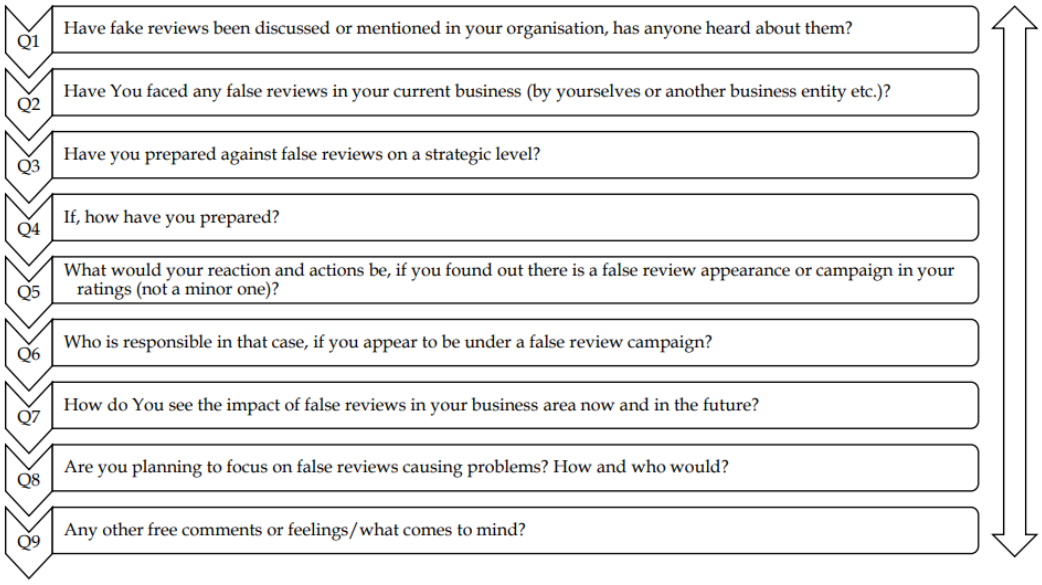

FIGURE 4 A figure explaining the process of structured interviews.

The interviews were structured and followed a construction described in a picture above. It was relatively common, that a participant wanted to return to specify or comment their response to a prior question.

4.2 The interview processes

The issue of paid false reviews is observed through interviews of employees of 20 organizations. The chosen interviewees were selected from 13 small and micro-organizations and 7 medium and large organizations. The interviewed participants were employees of the organization from different positions, which were in a possible contact with paid false reviews.

TABLE 3 Summary of the organizations interviewed in order, showing line of business, interviewees' position, and organization size.

	Economic area/ Line of business	Interviewees' position in the company	Organizations' size
O1.	Healthcare	Data security officer	Large-scale
O2.	Transport and storage	CIO	Micro
O3.	Information & communication	Performance marketing chief	Micro
O4.	Beverage industry	Store manager	Small & Medium
O5.	Beverage industry	CEO	Micro
O6.	Non-profit association	Chair of board	Micro
O7.	Clothing industry	Import & export manager	Medium-scale
O8.	Education	Director of working life services	Large-scale
O9.	Healthcare	CEO	Micro
O10.	Retail	Director of customer experience & service ecosystem	Large-scale
O11.	Retail	Store manager	Micro
O12.	Clothing industry	Online store manager	Micro
O13.	Non-profit association	Editorial manager	Micro
O14.	Consulting	Chief of customer consulting	Micro
O15.	Real estate	Expert	Medium-scale
O16.	Information & communication	CEO	Small
O17.	Real estate	Manager of sales	Small & medium
O18.	Entertainment	CEO	Micro
O19.	Transport and storage	CEO	Micro
O20.	Entertainment	Executive producer	Small

Organizations were selected by the following criteria. 1) Micro and small organizations were selected to be interesting area for thesis' research questions, since these organizations suffer more severe damages when their reputation is targeted. Medium and large sized companies on the other hand have better ability to respond and form various strategies to survive against false reviews. Therefore, the criteria to capture these viewpoints was considered to be important. 2) The organizations had some sort of review platform in use or/and there were reviews online regarding their performance and services. There were 13 micro and small organizations and 7 medium and large organizations. The interviewees did make remarks that are presented above and separated as interesting quotations to enwiden the attitudes they had regarding the research dimensions.

TABLE 4: A table describing empirical questions and their purpose to gain data of dimensions.

Question:	Findings:	Dimension

1. Have fake reviews been discussed or mentioned in your organization, has anyone heard about them?	Familiarity with the concept	Past actions
2. Have You faced any false reviews in your current business (by yourselves or another business entity etc.)?	Experience	Past actions
3. Have you prepared against false reviews on a strategic level?	Preparedness, strategy	Current state
4. If, how have you prepared?	Preparedness in practice	Current state
5. What would your reaction and actions be if you found out there is a false review appearance or campaign in your ratings (not a minor one)?	Processes & strategy	Current state
6. Who is responsible in that case, if you appear to be under a false review campaign?	Process/strategy responsibility	Current state
7. How do You see the impact of false reviews in your business area now and in the future?	Contingency planning	Future actions
8. Are you planning to focus on false reviews causing problems? How and who would?	Prioritization, attitude	Future actions
9. Any other free comments or feelings/what comes to mind?	Other	

The area of false review is relatively difficult to study because the certainty whether if a review is fake, or genuine, is hard and complicated to conclude. However, the tracking algorithms and applications are increasingly increasing to narrow down suspicious activity and fake review attacks as Lappas (2012), Mukherjee, Liu, and Glance (2012) have revealed. In this study, the research angle is chosen to be one of the victim angles: companies whose business revenue and brand suffers deprivation when fake reviews occur. The other victim is the consumer, and consumer's rights to reliable information (Mason, 1986). By targeting the victim side, motivation to falsify business entity is to achieve some economic benefit and profit, without any real effort easily via online branding. Also, it is learned earlier by Johnson et al. (1993), Johnson et al. (2001) and Zhuang et al. (2018) that companies with weaker brand or less resources are more vulnerable for false information and tend to recover more slowly.

This study aims to cover interviews done by qualitative empirical research to reveal new insights whether the companies have any familiarity with the

concept of fake reviews and have they prepared for them in any way and if there are any other interesting findings. Since there were no hypothesis and the main strategy was to collect concepts and ideas from the interviewees, the interview method was selected to be qualitative structured open interview. The results were analyzed after assortment by qualitative conventional content analysis technique, which included the coding of the transcript interviews (Hsieh & Shannon, 2005).

The study was conducted by following the process described below. First the theoretical literary sources of paid false reviews and internet deceptions were summarized to a literature review and theoretical framework sections. Then it was scoped to define the final research question, which followed to empirical study part, and thereafter the presentation and discussion of the results. Analysis of the theory mirroring to the empirical part was a process, which was simultaneous during the whole thesis writing time. The outcome was a coherent analysis of the findings and further discussion that can be defined in future research topics section.

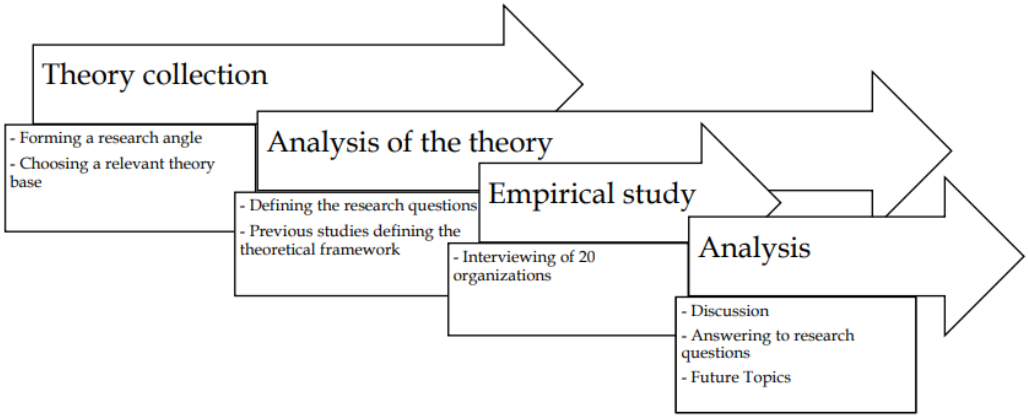

FIGURE 5 A Process diagram of the thesis

The results focus to give an answer for the research question, which is later explained and analyzed together on a section of results and discussion. Interviewees were selected within companies and organizations from business lines of healthcare, transport and storage, information & communication, beverage industry, non-profit association, clothing industry, education, retail, real estate, and entertainment. It was relevant for the study to gain multiple point of views from different areas of society and lines of business to approach entirety for perspective of internet users and their services. The organization were selected from micro-, and small organizations, as well as medium and large sized organizations (www.tilastokeskus.fi), which had liability for being a victim of

paid false reviews. Also, organizations with bigger size were interviewed to get a good comparison with the data: three large-scaled organizations and four medium-sized.

TABLE 5 Definition of an organization size according to www.Tilastokeskus.fi according to European commission definition (*Echa.Europe.Eu*, n.d.)

Size class	**Employees**		**Turnover**		**Balance sheet total**	**Number of organizations interviewed**
Micro	<10		≤ 2 million		≤ 2 million	11
Small	<50		≤ 10 million		≤ 10 million	2
Medium	50-249	AND	≤ 50 million	OR	≤ 43 million	4
Large	>250		>50 million		>43 million	3

All interviewees had a key role in their organization, and they were aware of organization's strategy or tactics about their currently existing reviews online. The participants were contacted by approaching them on e-mail or another written message and they were collected from LinkedIn, acquaintances of the thesis writer or with the help of network. The organizations were involved with online reviews, either they had an existing platform activity, own platform, or intentions to gain interest for their reviews on consumers or customers eyes. However, it is important to observe that interviewees were not specialized on reviews.

5 RESULTS

The results of the empirical part are presented here in this section. After the empirical research was done and the interviews were transcript, the results were summarized and categorized in collective tables. This was prepared with conventional content analysis technique by Hsieh and Shannon (2005). This technique was conducted by organizing the transcript interviews. After the categorized data, the content was analyzed, and key elements of the interviews are presented here on the result section. This technique also examined findings to be defined during the result analysis. The found correlations are presented further on discussion section.

5.1 The Past: Familiarity and Previous Experience

The first question (Q1) was selected as following: have fake reviews been discussed or mentioned in your organization, has anyone heard about them? Question number 2 (Q2) was: Have You faced any false reviews in your current business (by yourselves or another business entity etc.)? Question number 1: "Have fake reviews been discussed or mentioned in your organization, has anyone heard about them?" This is noted to be a limiting factor for the empirical part of the thesis, since the targeted interviewee group contains from various organizations and various interviewee subjects that are not expertized on reviews or otherwise familiar with the defined concept. This has an impact on some of the interviews, since the interviewee has not fully understood what the concept is about and how it differs from coincidental or casual trolling or feeling-based writings on the internet.

> "It's really difficult to know from 1–5-star scale reviews, which ones are fake and which ones are not." (O3).

As interviewed claimed above, it is not easy to track down the actual reliability of the reviews, especially when the review could be in non-written form. It is

impossible to track down why there are one out of five reviews give, even though some answerers claimed that they would be sure that who of their customers did gave them a rating, and even they had a clear situational awareness at the moment. However, this is something that a customer or consumer does not know, and if there would be masses of reviews, it was unclear how they would react to this.

TABLE 6 Familiarity and experience: key findings.

	Size	**Familiarity of the concept (Q1)**	**Real life experience in organization and awareness to recognize paid false revies. (Q2)**
O1.	Large-scale	Yes, but not directly on our business.	Considered to be more individualistic issue such as trolling.
O2.	Micro	Yes, mentioned and discussed somewhat with an application project.	A one separate poorly written review was noticed that could have been a paid false review.
O3.	Micro	No.	Not directly in our reviews, but there have been overly positive reviews as well as negative reviews that are tried to be hidden away that the interviewee had confronted on competitor.
O4.	Small & medium	Yes.	Not noticed.
O5.	Micro	Yes.	Not really, but suspicious reviews have appeared: not sure if paid.
O6.	Micro	Partially, but not under a name "paid review".	Not really, one emotional angry review existed.
O7.	Medium-scale	No.	There are always negative reviews.
O8.	Large-scale	No.	Not really, there are overall weird reviews existing in this line of business.
O9.	Micro	Partially.	One suspicious review from "a known mass reviewer". All customers have written a review.
O10.	Large-scale	Somewhat yes, but on a different name.	Yes, the content of the review was always the same and it has a pattern.
O11.	Micro	Yes.	Yes, easily trackable.
O12.	Micro	Yes. (Not under the name of paid review.)	No.

O13.	Micro	No.	Not really, but we have a lot of negative feedback.
O14.	Micro	No.	No.
O15.	Medium-scale	No, marketing brand has been relevant only for a short period.	No.
O16.	Small	Yes. Practices to track these. (Q3)	No.
O17.	Small & medium	Yes. (Not under the name of paid review.)	No.
O18.	Micro	Yes.	Few cases with false identities that have written a review.
O19.	Micro	Not really.	Not really, but a customer made a remark of many positive reviews. One is written by a relative.
O20.	Small	No.	Yes, we had masses of positive reviews for some reason – not ordered by us.

Micro and small organizations had known familiarly of 9 out of 13. Overall, 12 organizations stated that they were familiar with the concept of paid false review as well as might having confronted those in their business's ecosystem. The answers were different how and why they would know that they had faced a paid false review, and a key finding therefore is that experience of paid false reviews is not necessarily true in a mean of exact definition. However, there were few answers that claimed that their reviews are reliable, but this was also explained by the novelty of their business, or the lack of reviews as they explained by themselves.

5.2 The Present: Preparedness and Strategy

Questions three (Q3): "Have you prepared against false reviews on a strategic level?", and question four (Q4) "If, how have you prepared?" were placed to find a view to organizations practical preparedness towards paid reviews. Questions also tried to find out how in the real-life companies systematically value paid false reviews as a threat that needs to be taken into strategy level. Q5 was placed to cover an answer to question: "What your reaction and actions would be if you found out there is a false review appearance or campaign in your ratings (not a minor one)?" Question 6 (Q6) defined a responsibility in the organization: "Who is responsible in that case, if you appear be under a false review campaign?"

O13 mentioned that they did not have any familiarity with the concepts, or they did not have any discussion regarding the topic, but nevertheless they could name a clear process how they would react when a smear campaign would occur.

TABLE 7 A named responsible and actions

	Size	Strategic preparedness (Q3 & Q4)	Action(s) under paid false review campaign (Q5)	Defined responsibility or team under a false review campaign (Q6)
O1.	Large-scale	Not considered to be a technical issue.	Probably contacting the platform. Internal communication steps.	Public relations team.
O2.	Micro	Not directly.	Reacting and contacting the reviewers and platform. Analyzing the reviews if they are from real reviewers.	Everybody collectively
O3.	Micro	No.	Contacting the platform to find out who is behind it. Answering with market strategy.	Not named. (A head of company probably.)
O4.	Small & medium	No.	Internal communications and actions.	Local or operative chief.
O5.	Micro	No.	Contact to an individual reviewer and later platform. Otherwise, no clear idea.	CEO or head of marketing and sales
O6.	Micro	For certain type of reviews that can be tracked.	Contacting Google, deleting reviews, writing a public note for different social media accounts.	Chairperson/a social media responsible person.
O7.	Medium-scale	No.	Crisis meeting, conducting a strategy and hit back on a consumer level.	CEO
O8.	Large-scale	Partially, not directly.	Crisis communication is a known and clear: how a chain would work.	Head of department.
O9.	Micro	Yes.	A consultant would help (market strategy). Would pay for positive reviews.	CEO

O10.	Large-scale	Not directly.	Model responses. "Situation center", crisis management and communication.	Customer service/communication department, Chief marketing director.
O11.	Micro	Partially, upcoming.	Contacting the company/person quietly. Public announcement in second option.	Manager.
O12.	Micro	No.	Tracking, deleting If proven false. Discussion about a process of product. No clear idea.	Not named.
O13.	Micro	Yes.	Not defined. Closing comment sections.	Operative lead.
O14.	Micro	No.	No clear idea.	Chief content strategist.
O15.	Medium-scale	No.	Individual contacting, especially public reaction is important.	Not named.
O16.	Small	Partially, careful observance at the moment.	Public question and answer-model.	CEO
O17.	Small & medium	No.	Communicational response for "clear" false reviews	Not named: maybe CEO.
O18.	Micro	Partially.	Public response, contacting the customers, tools to track reviews.	Marketing responsible
O19.	Micro	No, but cyber security insurance is valid at the moment.	No clear idea; using a consultant.	CEO
O20.	Small	Partially, processes for similar issues.	Contacting the consumers and finding out why. No actions with positive reviews.	Social media responsible.

Q3 did gain some interesting answers, since there was one organization that was not familiar with false reviews in such a concept and had not been active in talking about them but did - in fact - have a clear strategy on how to prepare against negative reviews and how to react against them. They trained their employees, were moderating their public image through an updated list of words that would alert when used and even block certain texts, and even had a legal process ready to take place in certain issues. However, if it would be about mass

reviews, there would be no clear process how to prepare against them on a detailed and carefully pre-thought manner.

> "If you can identify why a certain product/service is negative, it is most likely a real review, not just a general rant." (O11).

As O11 claims that a genuine review has identifying marks when it is specific enough. A review that has descriptions of the product and detailed information is genuine in the eyes of a victim. Also, processes and current strategies were key findings among the interviews.

> "We would try to find out why there are so many negative reviews and contact the consumers… try to remove them… Positive reviews would probably just lay there, and we would just wonder and think that this is a good thing." (O20).

O20 describes that they would have actions with malicious reviews, and they would spend quite a lot of resources tracking the writers and reasoning their behavior, but they would ignore positive and untrue reviews. This is an interesting ethical fact, that can be elaborated further: how many of the victims would exploit paid false reviews themselves if they had a chance and therefore became deceiver themselves.

Question number 6: "Who is responsible in that case, if you appear to be under a false review campaign?" did also contain some variation. Almost all the respondents were able to give an answer that was somewhat convincing, but only were able to tell that they have a clear role definition or a certain process for incidents such as this. In the first cases the responsibility would only fall on someone's shoulders, such as the communication department or CEOs without any preceding thoughts or strategy. O16, claimed that they could identify a tactic that would be preventive by setting "traps" for the reviewer to make sure that they would have genuinely bought the product, but majority would form a specific strategy depending on each case. There were answers that described that they would tackle a smear campaign by contacting a platform (which contains the reviews) silently, and from those then would as secondarily spend resources on communicational campaign. Interviewees claimed that if they had to take actions within the issue of pursuing false reviews, they would contact the platform, where the reviews are appearing.

5.3 The Future

Question with reference to future, for example how crucial organizations considered, were placed to cover findings on attitudes and prioritization of the phenomena of false reviews and deception. All the interviewees did answer that reviews are important, but only X was able to define that they would act. X did consider that they would act after something would happen - for instance, a

smear campaign would already happen and real time affecting the company. Also, question of focusing paid false reviews in the future did raise an interest for every single interviewee, but only very few could say that they were for sure to tackle this topic and even name a certain responsible team or person with resources to address this issue in the future. Also, interviewee number 19 said that it is more likely that a smaller competitor would harm them in a physical way of sabotage in real life, than that they would create a smear campaign against them. As it is previously studied by Zhuang et al. (2018), weaker brands tend to suffer more from flood of reviews. This was an interesting finding; majority did admit that they are dependent on reviews and would need to do something to prepare or otherwise think about this. However, only 4/20 did answer "yes" to the question whether they are going to do some actions with the preparedness or otherwise focus on reviews as a threat.

Open question was placed for open opinions and gave the interviewee a change to express their own opinions and topic that they felt that were important or worth to add. Exactly half of the interviewees (10/20) commented that they felt that the topic was important or relevant for them. 9/20 did mention that this is an important topic but not crossing their path in a severe way. They planned to have further pondered with the topic either by themselves through their role if they could spend resources on it, or by introducing the topic somehow in the future. However, only two of the respondents did confirm that they would positively take clear actions regarding false reviews on a strategy level and change existing processes or plans.

An interesting discovery was that two of the interviewees did consider paid false reviews as an opportunity. If they would have access to those or be able to use them without the risk, or they knew how to pursuit false reviewers of getting caught, they would exploit them. Also, if there were positive false reviews this would not take any concerns or actions for most of the respondents – by and large all the answers were focusing on negative threat and how that would require actions.

How does a false review differ from a review that a friend has written for a good will? This is an exceedingly difficult question, but if we approach this by a point of view that a reviewer always has an economic motive to gain monetary value: money, services or products, just a nice gesture to help a friend would not fall into that category. This would more likely suit to be an emotional review, as a positive meaning such as compassion, but not a false review with a clear motive to target a company's image with an economic motive. The difference between a paid anonymous reviewer army and a well-known friend exists in quite various places on the scale far from each other. But on the other hand, if an entrepreneur would encourage a friend to give a hand just a little and then provide a discount or a pint of beer etc. for the favor, this makes no difference to a false review: motive (economic) and action (improve friend's ratings) are fulfilled.

This includes a definition of what a false review is not. It is not written for an angry motive or just for fun, such motives that internet trolls might have. On the contrary it is always written by a paid evaluator, on an economic motive to

gain money or other benefits from an external factor. The false evaluator has not (necessarily) any connections or familiarity with the target company or service. The review targets only to manipulate the organization's image or separate service or product to a negative or positive direction. Nevertheless, some of the interviewees did associate all kinds of negative reviews to false reviews, even though according to the previous definition the explicit expression of false reviews was not coherent based on their experience. Therefore, the results of the interviews are interpreted very strictly on a question 1 and 2, the familiarity of false reviews as a concept and as an experience. If an interviewee has answered that they are familiar with false reviews but clearly, they describe their experience to be specifically different from false reviews (such as only negative, but still accurate reviews), this has been statistically catalogued to thesis' material under "no experience". However, the actual term of "false review" did not need to be familiar, because the concept can be defined also under different names. These answers were included in the results as a familiar singularity, since it also included that a company had used time and resources even when talking about false reviews. However, just negative reviews and general interest on reviews were not reported as familiarity with false reviews.

TABLE 8 Future actions and findings

	Size	**Attitude towards paid false reviews in the future (Q7)**	**Planned actions for the future (Q8)**
O1.	Large-scale	None on a technical level. Not considered to be a threat.	No, not relevant.
O2.	Micro	Perhaps a motive to frame someone to be unreliable. Not considered to be a realistic thread.	Perhaps if the company size would go bigger, then a careful analysis and market analysis for the case of false reviews would take place.
O3.	Micro	Not that important because we sell our services directly, but of course everything effects everything. "Leads" might have effects.	No. Perhaps on a later state of business growth this would be more accurate.
O4.	Small & medium	Not necessary targeting us because we have no physical product or online retail etc. Trolling or hate reviews are more severe.	Not really becoming to be in a huge role.
O5.	Micro	Reviews do effect on consumers buy decision heavily.	Yes, this might be one topic for next year's strategy.
O6.	Micro	Separate reviews with economical motive are	Not first on the list but reviews generally are important.

		acknowledged as a threat. But not anonymous mass reviews.	
O7.	Medium-scale	Would affect heavily on core business since we think about public image of a company even on a single negative review. Really difficult to say if it's a real campaign or a false one.	Looking up to consumer reviews, following movements in the world: if Finnish our industry is facing these, then reactions will take place.
O8.	Large-scale	A need to keep up with modern social media which has its ups and downs: there are always a risk.	No- but these are topics that are needed to take into consideration: how to keep the promises made for customer.
O9.	Micro	Increasing topic.	Yes, since this is very important to focus on. Would buy paid false reviews.
O10.	Large-scale	Increasing.	Not under that term, but yes in overall picture.
O11.	Micro	Issue would create more issues. Very dangerous for early-stage companies. It would destroy a business.	Not yet, focus for positive thing instead of (telling employees) negative things. Emotional reaction would be bad in case of realization.
O12.	Micro	Not relevant, we are so small. We would courage our friends to write positive reviews, but we would not buy them because it would collide with our ethics.	Not really, not considered to be relevant.
O13.	Micro	Not really affecting on customer field, but it would have impacts.	This raised a lot of thoughts but not an acute issue now. Would not affect that much or would really diminish our customer amount. Would not know who would focus.
O14.	Micro	Yes, when business and familiarity would grow, but now risk might be more in other business area than B2B.	No, growth company is not really that important. But for instance, in a hotel business etc. it is really a problem, and these are not reliable in tourism industry.
O15.	Medium-scale	An important issue.	We aim to exploit trust pilot, because we need customer feedback which is difficult to have.
O16.	Small	Very small effect on my business, but on the big picture it is important and could damage other companies image a lot and cause customer loss.	No. Reaction when necessary.

O17.	Small & medium	Very big in the end. If someone diminish a product this would lead to losses in sale.	"Something should be done. Should observe competitors all the time."
O18.	Micro	Yes, seems to be important for consumers.	Marketing person, but the business entity would act if needed.
O19.	Micro	Not that probable in our line. False reviews are easily track I think - they have not that much effort.	Not a threat since our business line is uninteresting and competitors have ethical restraints.
O20.	Small	These can be exploited in positive and negative meaning and affect the brand.	Considered a really big risk, or really big reward. Tools for other similar issues.

It is noted that O9 and O20 mentioned and pondered the possibility exploiting paid false reviews, and O9 claimed that they would be ready to buy them if they knew how. O20 mentioned that this would be against the ethics of the organization and there was a clear deterrence for sanctions and therefore a risk.

> "I would pay for false reviews... This is a line written on sand… If I had more poker face, I would ask the customers to write positive reviews more often." (O9).

As noted above, it is not clear who is the victim and who is the deceiver when there is a question of market share and hectic competition. O9 mentioned that it would also be disastrous if there would be in minor quantities of negative reviews because of the narrowness of the business area. This would require a termination of the current business.

> "We are so small that we don't think that anyone – hopefully – would attack us. Positive reviews are important, but it would be ethically wrong to buy them… we would ask our friends to write positive reviews about us however." (O12).

O12 stated that their organization has no future threat since they are a small actor and they have not raised an interest of public attention or otherwise there would be no clear cause for anyone to manipulate their reviews. However, they did not have a clear idea whether a competitor from the same line of business would target them, or they felt dubious that this would be a realistic scene.

> "I don't think that our competitors would make the effort. Our competitors are great multinational companies who would not do it." (O19).

Also, O19 stated to have doubts with the realistic issue of paid false reviews targeting them. They expressed an ethical point of view that company size would protect them from false attacks, but also that the competitors must go along with law and order.

> ”These can be exploited in positive and negative meaning and affect the brand. It’s a really big risk, or really big reward. Getting caught would be a bad thing but on the other hand it’s really difficult to track these. On the grey area are influencers who get paid for promoting things.” (O20).

The future of paid false reviews is summarized aptly by O20. They explain that the line is unclear, as O9 earlier has said, and it is really difficult to separate real information from falsified. Tracking the deceivers and agents who had ordered the mass manipulation campaign is considered to be almost impossible action.

6 DISCUSSION

In this section, a discussion of findings and interesting and novel insights and implications are presented. Paid false reviews targeting organizations and how did the research question was answered is presented through literature sources. The research questions were formed: How familiar organizations are with paid false reviews? What actions organizations are doing against paid false reviews at the present time? What are organizations' future plans to deal with paid false reviews? These questions are analyzed in this section explaining what kind of findings and new aspects there were regarding the entity of interviews. As Wu and Liu (2017) conclude, a key problem is that victims tend to assume that malicious activities are occasional, or easily tracked by bad grammar. However, this is not the case. The most relevant tactic adjusting modern day deception and deceiver behavior is focused to be Relabeling in this thesis. When talking about deception tactics adjusting the modern-day deception focusing on the internet user as a deceiver are not taking into notice, that a deceiver can be a victim of a deception simultaneously. However, the deception tactic fitting for a modern-day false review deception is a tactic that is fostering information, as well as producing new information in false meaning.

By a false review, a deceiver aims to affect communication between deceiver and targets in a relabeling deception and targeting markets. The target of this intention is to mislead consumers. (Järvenpää & Grazioli, 2003). As deception theory explains, the tactic that a deceiver chooses is adjusted to the victim: is the victim an individual or an organization. In the case of paid false reviews, the chosen tactic is to affect both of them by falsifying the information by exploiting deception tactic relabeling, in a way that the product in questionably too positive or negative (Lim et al., 2010).

As can be summarized from work of Lappas (2012), Mukherjee et al. (2012) and Wang et al. (2012) paid false reviews aim to manipulate and target organizations reputation or products in a manner that misleads consumers, potential an current. Based on the findings of this thesis, the micro and small organizations have concerned attitudes towards paid false reviews. They are not positive how severe the issue is, and what kind of effects it might carry, which

reduces the ability to resource actions and strategies. Medium and large organizations are not concerned in a manner that they pay the effort the reach the topic on a specified strategy level. They nevertheless have clear frameworks that they exploit to maintain control of their public image. It is considerable that organizations need to focus on their internet presence, since it is vital to react when smear campaigns occur. The phenomenon of market manipulation is an upcoming issue (Li, Caverlee, Niu, & Kaghazgaran, 2017). Also, it can be analyzed that if micro and small organizations are afraid of malicious actors, they name bigger organizations (in addition of malicious individuals without economical motives). Paid false reviews require always an economic motive and agents working for economic compensation, which directs to a deceiver who has monetary resources and motives to occupy or manipulate a market (Anderson & Simester, 2014; Glazer et al., 2020).

TABLE 9 A table of summary of the interview questions regarding summaries to paid false reviews.

Corresponding answers	**Dimension**	**Content of the finding**
13/20	Familiarity	Had heard somewhat of false reviews or had discussed those within the company.
6/20	Familiarity	Had confronted paid false reviews in their current business.
11/20	Awareness	Were not strategically prepared against them on a detailed level which would include clearly documented processes or chosen tactics.
12/20	Awareness	Did have a clear responsible person/team who would act under a smear campaign.
10/20	Awareness	Would contact an individual reviewer on a public platform or create a public answer in the first remedial action.
8/20	Awareness	Would contact the platform where false reviews appear.
5/20	Awareness	Would not have a clear plan in the case of smear campaign.
10/20	Future plans	Would observe paid false reviews as an issue and focus on them, if there would be development on their business size, market area or on another significant factor.
4/20	Future plans	Would focus on them in the future and were able to define clear actions.

The analysis of the table is explained through the three dimensions which answer to research questions.

6.1 The familiarity

The first research question aimed to find an answer how familiar organizations are with paid false reviews. For the interviewees it was difficult to define that what is a paid false review, and have they understood that what is the concept is. This would require a strategical familiarization and measurement of reviews in order to be sure George et al. (2004). However, it could be summarized that even almost all of the interviewees did recognize or had heard of suspicious reviews, only 9 of 13 micro & small organizations' representatives stated that they did have had some discussions regarding the concept or similar topic and 4 of 7 medium and large companies had had discussions regarding this threat. An insightful conclusion of this is that the idea of awareness in organizations is that they think to have a good picture of the situation when an incident or smear campaign appears, but they do not have clear processes or resources to defend themselves. Lappas (2012) and Mukherjee et al. (2012) have concluded as mentioned earlier in this thesis, that it is extremely difficult to separate false paid reviews from real ones, or even ones that have been written without economical motive, in purpose to troll or under anger emotions. Generally, a tools and strategies to track reviews is required and only one large organization, was certain that they have resources, and that they are in the pulse of the situation during the time. They had experiences of same review that was used multiple times identically. The complexity of false reviews was poorly acknowledged and therefore it is a clear finding that familiarity with the topic is not on a level that would be convincing for organizations to be in a top of the situation. An interesting entity is the familiarity of interviewees to paid false reviews. Since the number of interviewees is relatively small as twenty research objects, there are no accurate relative analysis provided if the economic area, position, or organization's size would indicate any further drivers or conclusions to better awareness of false reviews. Instead, the data collected focuses on finding common nominators and attitudes towards false reviews, as well as finding out strategies how organization is prepared against them. Also, awareness without any practical thought of preparing or strategical level awareness was an interesting element when collecting data.

6.2 The Current awareness

The second research question was formed as following: what actions organizations are doing against paid false reviews at the present time? Participants had experiences regarding smear campaign, or at least vast number

of negative reviews from troll accounts and untrue reviewers with malicious intentions. Therefore, this organization could be named as an exception in the research data: they could describe a clear process how they would exploit tools, pursuit sanctions after the perpetrator and how they would apply the existing option – although there would be a panic. Also, organizations with small resources did explain their fears but also, they felt that the threat is not actualized, and it is distant: they would not see it worth to spend resources. It was a rear answer that organization would avoid public answer by any means to avoid negative effects that would create more problems by giving attention to false information. The vast majority considered to be a very good remedial access to helping to recover from damage that was caused by a smear campaign. Reacting to smear campaign was somewhat noticeable as a process, even though 12 respondents could name the responsible team or role who would take actions. Relatively popular strategy was to contact the platform where false reviews exist, as well as reacting them separately. As Liu et al. (2010), Mukherjee et al. (2012) and D. W. Straub and Welke (1998) have stated, it is very difficult to observe the false reviews and detect them without technical analysis. Also, they summarize, that a repairing action which would demand a procedure to contact or publish an answer separately to each review is not studied to be a good idea, since it is an enormous work which does not pay any effort. Crowdturfing is defined to be according to Lee et al. (2015), Song et al. (2015) and Wang et al. (2012) a phenomenon that does not have anything to do with real reviews, and therefore it is drastically difficult to influence on separative reviews by trying to open a discussion with the malicious reviewer. The deception existing on a platform and platform's responsibility was not discussed furtherly by any of the interviewees – however, as defined bellowing section, had relatively adapted tools or ideas to start to approach the issue (when occurred) from strategical point of view.

6.3 The future plans

The third research question was placed to answer to a question of what organizations' future plans are to deal with paid false reviews. The future of internet deceptions is occurring increasingly (Ott et al., 2012; J. Zhang & Ko, 2013) and reviews are strongly present in the future. An interesting analytical finding of the thesis is that organizations have awareness in the past experiences, somewhat of tool or ideas that what they would do in the case of emergency. However, even though the majority of the interviewed did express that paid false reviews are a problem and will be, they had little intentions to spend resources or actively prepare a strategy for the issue. None of the large or medium sized companies had a clear concept for false reviews, but on the other hand they did not consider it to be a serious threat for them.

> "It would be horrible. If I would get a big company creating false reviews against me, that would be horrible, because I think it… could kill the company. Especially its direct

> competitor. I don't have market share or enough customer bases to defend my company against the company that has stayed in the same market for a longer time." (O11)

As the quotation from interviewee of small size explain, it is a disastrous situation to suffer a smear campaign. Small and medium sized companies exclaimed mostly that they are afraid for paid false reviews, but they did not had intentions to focus on them. A risk is identified but it is not taken seriously enough that strategies and preparedness would take place. Also, small and micro-organizations considered it to be an issue when there would be significant growth and the line of business would raise attention or they would still consider it to be uninteresting for deceivers. In these cases, the conclusion that organizations as victims do not realize that they might be under attack by the competitor or anyone, who benefits by manipulating their line of business in the eyes of consumers.

An interesting finding was that 13/20 participants did state that they had somewhat familiarity with the topic. The concept of false review was not necessarily the same, but answers with clearly similar understandings of the concept were accepted to fulfil the criteria of familiarity. Six answers stated that they had confronted paid false reviews, but the issue was as they themselves were not necessarily noticed, that it is really difficult to observe and confirm a paid false review from genuine reviews, since the reviews are genuine looking (Lappas, 2012; Liu et al., 2010). The answers of participants did unfold that frequency of paid false reviews felt as a threat was considerable low, which indicates that organizations have idea of them being disconnected from the subject. 11/20 were not strategically prepared or had given any thoughts for the topic. 12/20 were able to name a clear response team or an employee, who would intermediate the process when a possible smear campaign would occur. A very common answer was that participants did not have any clear technique to tackle paid false reviews, excluding few respondents with a budget or previous experience. Therefore, a relatively ineffective approach of contacting individual reviewers or a platform "who would do something" was named. (Ivanova & Scholz, 2017).

A certain action what would happen in concrete manner after the contact was not named by any of the participants, they felt that it was important to clear out why the reviews where occurring. This is a key finding since paid false reviews already have a motive that cannot be altered by contacting or appealing to the malicious reviewer (Lim et al., 2010; Wang et al., 2012). Future actions were considered eminently mild for almost all of the participants. 10/20 did state that if a explicit change on the market or in their business size, or on the global market would occur, then there would be interest towards paid false reviews. Currently the organizations mentioned that they did not have any concern, and that they would react when an incident would occur. Only four respondents were positive that they would prepare some actions. The data also revealed that 2 organizations were forward-looking to paid false reviews and would exploit them for their own vested interest.

6.4 Countermeasures

The thesis summarizes paid false reviews to be an uprising information security issue, which causes manipulation on the market and platforms that contain internet reviews written or otherwise produced by reviewers. Internet deception is a phenomenon that exists always when there is interest to reviews and market shares or organizational competition.

There are numerous research covered in the area of Deception Theory, but relevant angle for organizations to prepare against paid false reviews could be explained through the studies of Straub and Welke (1998) and Detmar Straub and Nance (1990) which cover the area of security planning models. These models were categorized according to previous studies to deterrence, prevention, detection, and repair in the theoretical section of the thesis. As described in the results, organizations had insecurities to select a strategical approach how they would adopt an attitude and actions. When only four organizations had a clear steps and strategies which included somewhat named processes, these could be mostly placed to detection and prevention. The usage of repair was explicitly all-embracing for all the companies, but this was not clearly defined for majority that how and who would react – more likely remedial actions would take place in situational and anxious occasion. Other tools to prepare against paid false reviews can be observed through text-based deception detection model Mbaziira and Jones (2016) by focusing on analyzing the current review masses.

Manipulation of reviews is proceeded by phenomenal concept of crowdturfing, which was defined earlier: An untrue review of a product or a service, appearing in some online platform. A paid false review is written by a paid reviewer in order to manipulate; by promoting or discrediting products, services and it effects the company's image (Glazer et al., 2020; Lappas, 2012; Lim et al., 2010; Liu et al., 2010; Mukherjee et al., 2012; Wang et al., 2012). Micro and small organizations are tempting targets for deceivers to use paid false reviews, since they have significantly fewer resources and strategical interest to prepare against them, or even use them themselves. Crowdturfing as a deception tactic enables mass smear campaigns, which are difficult to identify without tools and detection methods. Paid reviews are written by genuine agents, which can be hired by original deceiver who has a motive to manipulate competitor's reviews (Song et al., 2015, Wang et al., 2012). When the market is manipulated and it is affected by twisted reviews that lead consumers and businesses (Järvenpää & Grazioli, 2003) to make false opinions, it is inevitable that the trustworthiness of the internet reviews overall is endangered. The key consequence of manipulated and false reviews may lead consumers to mistrust all review (Mayzlin et al., 2014).

6.5 Key findings

As listed above, the key findings for the study are added up to be revealing the answer for research questions, how dimensions are felt and acknowledged:

1. How familiar organizations are with paid false reviews?
2. What actions organizations are doing against paid false reviews at the present time?
3. What are organizations' future plans to deal with paid false reviews?

As presented on the analysis of the results, the past familiarity and knowledge of the phenomenon has not yet clearly led to a strategical action, or even future topic to focus on. Reliability is considered as a current and fundamental element of modern organization's business models and functions, nevertheless this relevance and entity are not yet recognized. According to Agrafiotis, Nurse, Goldsmith, Creese, and Upton (2018) future research needs to fill a gap of defining the impacts of and the potential quantity of misbehavior: "The threat landscape of cyber- attacks is rapidly changing and the impact of such attacks is uncertain". Also, as Järvenpää and Grazioli (2003) and Grazioli and Jarvenpaa (2000) have studied during the early decade, the concept and definitions of the business platforms and consumer or user impacting amongst them, are not clearly defined and presented in academic world. Cybersecurity and organizations' strategies have been widely studied, as well as the behavior effects of employees. This study's ambition was to pinpoint the modern dilemma of an understudied concept of paid false reviews as a deception. Also, a crucial finding was that the organizations representatives did have no clear idea of the concept of the paid false review, but they also associated the concept of internet trolling or other non-economic motive-based deception to crowdturfing. Nevertheless, they did not consider that paid false reviews would be de facto a threat to them, although they were considered to be interesting and dangerous topic – only few organizations were ready to spend resources on a strategy level.

TABLE 10 Micro & small organizations: dimensions

	Line of Business	**Past experience**	**Strategic preparedness**	**Considered as a future threat**	**Future actions**
O2	Transport and storage	x	Partially.		If growth.
O3	Information & communication				If growth.
O5	Beverage industry	x		x	x
O6	Non-profit association	x	Partially.	x	
O9	Healthcare	x	x	x	x
O11	Retail	x	Partially.	x	

O12	Clothing industry	x			
O13	Non-profit association		Partially.	x	If growth.
O14	Information & communication				If growth.
O16	Information & communication	x	Partially.	x	
O18	Entertainment	x	Partially.	x	Not sure (Marketing's responsibility to take actions).
O19	Transport and storage	x			
O20	Entertainment	x	Partially.	x	

Below is presented a table of medium and large sized organizations with dimensions that are compared with causalities and relations.

TABLE 11 Medium & large organizations: dimensions.

	Line of Business	**Familiarity**	**Strategic preparedness**	**Considered as a future threat**	**Future actions**
O1	Healthcare	x	Partially.		
O4	Beverage industry	x	Partially.		
O7	Clothing industry			x	x
O8	Education		Partially.	x	
O10	Retail	x	x	x	x (not under a name of paid false review)
O15	Real estate	x		x	
O17	Real estate	x		x	

There are multiple findings from the table above. For instance, it is interesting to observe the fact that 9 of 13 micro and small organizations had familiarity with the concept of paid false review, and 8 of those had somewhat a strategic preparedness or preparedness for the possible risk. O13 is an interesting object, since they did not have recognizable familiarity, but they had very good and clear process what to do in the case of attack. 7 out of 13 would have somewhat actions in the future, but only 3 were convinced that they would focus on them in any case. 8 did consider paid false reviews to be a threat for them, but relation with future actions and preparedness was not discoverable since only two would take serious action, and 4 would have first condition to grow in their line of business and one would place it under the evaluation of marketing team.

The medium and larger organizations have a result that 5/7 were familiar with the topic, but it was found in their strategy only partially, except O10 which had already experience of the same identical reviews that appeared several times,

however it was defined to be a separate individual writing them. Even 5 did consider that paid false reviews are a possible threat, only two would focus on them and conduct future actions. A good situation analysis is almost impossible to have, since detecting the paid reviews is requiring auditing and developed tools in constantly reflective manners (Lim et al., 2010; Liu et al., 2010; Mukherjee et al., 2012). It is a concerning finding that since tracking of the paid reviews require resources to prevent crowdturfing, the most vulnerable are not spending resources to prepare against them.

6.6 Limitations

There were recognizable limitations for the empirical part. One issue was the number of interviews. But using a different method for gaining a higher number of answers – for instance quantitative research there would have been a risk for answerers to misunderstand the topic, elaborate and not explain their actions and thought. Qualitative research was chosen on that base since the participants did answer open questions and elaborate their feelings amongst the topics. Second issue was that had the interviewees fully understood the concept of false review? Despite it was explained to them, it was not certain that the interviewees did understand it and were able to separate for example a malicious trolling review from an actual paid false review that aims to manipulate the organizations' brand. However, it is a difficult from a research point of view to separate these since there are only few technical ways to deal with false reviews and research is only to begin. Third issue was recognized as how many of the interviewees were honest since the questions were placed on the area of sensitive and ethical behavior on the internet. Did all the interviewees admit that they had created reviews or would use them by themselves or encouraged others to do it - relatives and friends for example? There was no research question that would have asked directly if this was an option at some point, but few interesting findings among the answers took place.

6.7 Ideas for Future Research

False reviews as a method to gain positive reviews for one selves and negative reviews for competitors will become increasingly general phenomenon amongst organizations. How many of the organizations are ready to exploit them, how many of the consumers want to gain sufficient knowledge of the reviews and observe them critically, how platforms take actions and responsibility on their public data, as well as the responsibility of the society in a form of laws and regulations are the key questions and possible future topics to study. The topic of internet deception is existing and increasing with the variety of multiple platforms, medias, and users. Specific updated taxonomy and observance of the

phenomenon of paid false reviews are something that this thesis proposes to create and update in the future.

As Lee, Webb, and Ge (2015) have concluded in their study, some major platforms have already prepared to face crowdturfing and analyze the problem. However, an average internet user is facing difficulties and responsibility to seek information and share it with other users without facing the threat of being deceived. An insight for the theoretical background is also cover some technical responses to the deceptions, that are academically studied phenomenon. Cybersecurity is current and fundamental element of modern organization's business models and functions. According to Agrafiotis et al. (2018) future research needs to fill a gap of defining the impacts of cyber-attacks and/or the potential quantity. "The threat landscape of cyber- attacks is rapidly changing, and the impact of such attacks is uncertain". A drastic misuse of reviews will affect heavily on consumers trust towards all the reviews in the internet. (Mayzlin et al., 2014).

Thus, the taxonomy of deception tactics covered in modern days phenomena and risks for organizations, from micro to large, should be focused as future research topic. Deception and selected tactic to manipulate victim is a concern that is here to develop, within the upcoming technologies. Deceiver will adapt to different platforms, but will deceiver exploit the same tactics to influence on company's image. One key question is, who has the responsibility in the end to ensure that platforms are providing reliable information for the internet users (Zhuang et al., 2018).

The deceiver also requires resources and is keen to manipulate markets in their own benefit. A clear study topic in the future would be to research that reveals how prepared micro and small organizations are to exploit paid reviews themselves, and on the other hand how probable is that medium and large organizations are using them to hold their market shares.

7 CONCLUSION

This study's motive was to represent a clear entity of theoretical framework and empirical findings which answer to research questions: How familiar organizations are with paid false reviews? What actions organizations are doing against paid false reviews at the present time? What are organizations' future plans to deal with paid false reviews? Paid false reviews are used to target and manipulate organizations reviews of products and services available for consumers. This thesis summarized relevant literature with deception tactics and a concept of crowdturfing. The past, present and future of paid false reviews from the point of view of organizations were categorized and analyzed trough these three dimensions.

The structure contains overall 6 sections which contains introduction, literature review theoretical framework, empirical research, presenting the results, and finally by analyzing the results with theoretical framework in the discussion section. The Method that was used was picked to be structured interviews with 20 organizations. The empirical research in section 3 were held with 13 micro and small organizations' representatives and 7 medium and large organizations' representatives. Structured interviews were used as a method, and later the data was transcribed and analyzed with qualitative analysis with conventional content analysis.

Key findings for this study were that even the organizations' representatives did have awareness of reviews and about false reviews, most of the respondents did consider it to be out of the question that they needed to have strategy or that they should spend resources on focusing them now or in the future. Majority also considered that they would react to a false information campaign regarding them, only in the case when something happens and that would have also severe impact. By and large, all the participants did agree that internet reviews in general cannot be overlooked, they have significant impact on customers and consumers. However, the variation of the importance was large when they pondered their business field and how a paid false review would affect them. There were limitations with the study that were explained in the

discussion section together with the summary of key findings and future research topics in the discussion section.

This study summarized key findings and presents future topics that need to be studied further from these aspects that were familiarity, awareness, and future actions. Concept of paid false reviews is a severe threat for organizations, but especially for micro and small organizations, since they do not have resources against them. This needs to be studied further to protect markets from cyber deception, but also by securing information for consumers.

REFERENCES

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. F. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory. *MIS Quarterly*, 435–461. https://doi.org/10.1017/CBO9781107415324.004

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. In *Journal of Cybersecurity* (Vol. 4, Issue 1). Oxford University Press. https://doi.org/10.1093/cybsec/tyy006

Anderson, E. T., & Simester, D. I. (2014). Reviews without a purchase: Low ratings, loyal customers, and deception. *Journal of Marketing Research*, *51*(3), 249–269. https://doi.org/10.1509/jmr.13.0209

Bellekens, X., Jayasekara, G., Hindy, H., Bures, M., Brosset, D., Tachtatzis, C., & Atkinson, R. (2019). From Cyber-Security Deception to Manipulation and Gratification Through Gamification. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11594 LNCS*, 99–114. https://doi.org/10.1007/978-3-030-22351-9_7

Bhat, S. Y., & Abulaish, M. (2014). Using communities against deception in online social networks. *Computer Fraud and Security*, *2014*(2), 8–16. https://doi.org/10.1016/S1361-3723(14)70462-2

Bigne, E., Ruiz, C., & Sanz, S. (2005). The Impact of Internet User Shopping Patterns and Demographics on Consumer Mobile Buying Behaviour. *Journal of Electronic Commerce Research*, *6*(3), 193.

Biros, D. P., George, J. F., & Zmud, R. W. (2002). Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study. *MIS Quarterly*, *26*(2), 119–144. http://www.jstor.org/stable/4132323

Buckels, E. E., Trapnell, P. D., & Paulhus, D. L. (2014). Trolls just want to have fun. *Personality and Individual Differences*, *67*, 97–102. https://doi.org/10.1016/j.paid.2014.01.016

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, *6*(3), 203–242. https://doi.org/10.1111/j.1468-2885.1996.tb00127.x

Cartwright, S., Liu, H., & Davies, I. A. (2022). Influencer marketing within business-to-business organisations. *Industrial Marketing Management*, *106*, 338–350. https://doi.org/10.1016/j.indmarman.2022.09.007

Caspi, A., & Gorsky, P. (2006). *Online Deception: Prevalence, Motivation, and Emotion*. *9*(1), 54–59.

Chen, C.-D., & Huang, L.-T. (2011). Online Deception Investigation: Content Analysis and Cross-Cultural Comparison. *International Journal of Business and*

Information, *6*(1), 91–111.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

echa.europe.eu. (n.d.). https://echa.europa.eu/support/small-and-medium-sized-enterprises-smes/how-to-determine-the-company-size-category/step-5

Everett, R. M., Nurse, J. R. C., & Erola, A. (2016). *The anatomy of online deception*. 1115–1120. https://doi.org/10.1145/2851613.2851813

George, J. F., Marett, K., & Tilley, P. (2004). Deception detection under varying electronic media and warning conditions. *Proceedings of the Hawaii International Conference on System Sciences*, *37*(C), 327–336. https://doi.org/10.1109/hicss.2004.1265080

Glazer, J., Herrera, H., & Perry, M. (2020). Fake Reviews. *The Economic Journal*. https://doi.org/10.1093/ej/ueaa124

Goldkuhl, G. (2019). The generation of qualitative data in information systems research: The diversity of empirical research methods. *Communications of the Association for Information Systems*, *44*(1), 572–599. https://doi.org/10.17705/1CAIS.04428

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans.*, *30*(4), 395–410. https://doi.org/10.1109/3468.852434

Grazioli, S., & Wang, A. (2001). Looking Without Seeing : Understanding Unsophisticated Consumers ' Success and Failure To Detect Internet Deception. *ICIS 2001 Proceeding*, 23. http://aisel.aisnet.org/icis2001

Hancock, J. T. (2007). Digital Deception: Why, When and How People Lie Online. *Oxford Handbook of Internet Psychology*, 289–301.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2010). *Tutki ja kirjoita* (15th & 16t ed.). Tammi.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Hunder, M. G. (2011). Qualitative Research in Information Systems. *The Handbook of Information Systems Research*. https://doi.org/10.4018/9781591401445.ch016

Ignatuschtschenko, E., Roberts, T., & Cornish, P. (2016). Cyber Harm: Concepts, Taxonomy and Measurement. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2828646

Ivanova, O., & Scholz, M. (2017). How can online marketplaces reduce rating manipulation? A new approach on dynamic aggregation of online ratings. *Decision Support Systems*, *104*, 64–78. https://doi.org/10.1016/j.dss.2017.10.003

Järvenpää, S., & Grazioli, S. (2003). *Consumer and Business Deception on the Internet : Content Analysis of Documentary Evidence*. *7*(4), 93–118.

Jin, S. V., Muqaddam, A., & Ryu, E. (2019). Instafamous and social media influencer marketing. *Marketing Intelligence and Planning*, *37*(5), 567–579. https://doi.org/10.1108/MIP-09-2018-0375

Johnson, P. E., Grazioli, S., & Jamal, K. (1993). Fraud detection: Intentionality and deception in cognition. *Accounting, Organizations and Society*, *18*(5), 467–488. https://doi.org/10.1016/0361-3682(93)90042-5

Johnson, P. E., Grazioli, S., Jamal, K., & Glen Berryman, R. (2001). Detecting deception: Adversarial problem solving in a low base-rate world. *Cognitive Science*, *25*(3), 355–392. https://doi.org/10.1016/S0364-0213(01)00040-4

Kim, A. J., & Johnson, K. K. P. (2016). Power of consumers using social media: Examining the influences of brand-related user-generated content on Facebook. *Computers in Human Behavior*, *58*, 98–108. https://doi.org/10.1016/j.chb.2015.12.047

Lappas, T. (2012). Fake reviews: The malicious perspective. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7337 LNCS*(Springer, Berlin, Heidelberg), 23–34. https://doi.org/10.1007/978-3-642-31178-9_3

Lee, K., Webb, S., & Ge, H. (2015). Characterizing and automatically detecting crowdturfing in Fiverr and Twitter. *Social Network Analysis and Mining*, *5*(1), 1–16. https://doi.org/10.1007/s13278-014-0241-1

Li, S., Caverlee, J., Niu, W., & Kaghazgaran, P. (2017). Crowdsourced app review manipulation. *SIGIR 2017 - Proceedings of the 40th International ACM SIGIR Conference on Research and Development in Information Retrieval*, 1137–1140. https://doi.org/10.1145/3077136.3080741

Lim, E. P., Liu, B., Liu, B., & Lauw, H. W. (2010). Detecting Product Review Spammers using Rating Behaviors University of Illinois at Chicago Detecting Product Review Spammers using Rating Behaviors. *Proceedings of the 19th ACM International Conference on Information and Knowledge Management*, 939--948.

Liu, B., Jindal, N., Morgan, S., & Liu, B. (2010). *Finding unusual review patterns using unexpected rules Finding Unusual Review Patterns Using Unexpected Rules*. *2010*.

Lupton, D., & Southerton, C. (2021). The thing-power of the Facebook assemblage: Why do users stay on the platform? *Journal of Sociology*, *57*(4), 969–985. https://doi.org/10.1177/1440783321989456

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly: Management Information Systems*, *10*(1), 5–12. https://doi.org/10.4324/9781315259697-8

Mayzlin, D., Dover, Y., & Chevalier, J. (2014). Promotional reviews: An empirical investigation of online review manipulation. In *American Economic Review* (Vol. 104, Issue 8). https://doi.org/10.1257/aer.104.8.2421

Mbaziira, A., & Jones, J. (2016). *A Text-based Deception Detection Model for Cybercrime*. *December*, 1–8.

Moens, S., Aksehirli, E., & Goethals, B. (2013). Frequent Itemset Mining for big data. *Proceedings - 2013 IEEE International Conference on Big Data, Big Data 2013*, *1*, 111–118. https://doi.org/10.1109/BigData.2013.6691742

Mukherjee, A., Liu, B., & Glance, N. (2012). Spotting fake reviewer groups in consumer reviews. *WWW'12 - Proceedings of the 21st Annual Conference on World Wide Web*, *November*, 191–200. https://doi.org/10.1145/2187836.2187863

Neumann, J., & Gutt, D. (2019). Money makes the reviewer go round – Ambivalent effects of online review elicitation in B2B markets. In *25th Americas Conference on Information Systems, AMCIS 2019*.

Norman Burrell, D., Bhargava, N., Bradley-Swanson, O., Harmon, M., Wright, J., Springs, D., & Dawson, M. (2020). Supply Chain and Logistics Management and an Open Door Policy Concerning Cyber Security Introduction. *International Journal of Management and Sustainability*, *9*(1), 1–10. https://doi.org/10.18488/journal.11.2020.91.1.10

Ott, M., Cardie, C., & Hancock, J. (2012). Estimating the prevalence of deception in online review communities. *WWW'12 - Proceedings of the 21st Annual Conference on World Wide Web*, 201–210. https://doi.org/10.1145/2187836.2187864

Pagani, M. (2013). Digital Business Strategy and Value Creation: Framing the Dynamic Cycle of Control Points. *MIS Quarterly*, *37*(2), 617–632. https://doi.org/10.25300/MISQ/2013/37.2.13

Puccinelli, N. M., Goodstein, R. C., Grewal, D., Price, R., Raghubir, P., & Stewart, D. (2009). Customer Experience Management in Retailing: Understanding the Buying Process. *Journal of Retailing*, *85*(1), 15–30. https://doi.org/10.1016/j.jretai.2008.11.003

Rinta-Kahila, T., & Soliman, W. (2017). Understanding crowdturfing: The different ethical logics behind the clandestine industry of deception. *Proceedings of the 25th European Conference on Information Systems, ECIS 2017*, *2017*, 1934–1949.

Riquelme, I. P., & Román, S. (2014). The Influence of Consumers' Cognitive and Psychographic Traits on Perceived Deception: A Comparison Between Online and Offline Retailing Contexts. *Journal of Business Ethics*, *119*(3), 405–

422. https://doi.org/10.1007/s10551-013-1628-z

Román, S. (2010). Relational consequences of perceived deception in online shopping: The moderating roles of type of product, consumer's attitude toward the internet and consumer's demographics. *Journal of Business Ethics*, *95*(3), 373–391. https://doi.org/10.1007/s10551-010-0365-9

Sands, S., Ferraro, C., Demsar, V., & Chandler, G. (2022). False idols: Unpacking the opportunities and challenges of falsity in the context of virtual influencers. *Business Horizons*. https://doi.org/10.1016/j.bushor.2022.08.002

Soliman, W., & Rinta-Kahila, T. (2020). *Unethical But Not Illegal : Uncovering the Persuasive Messages Leveraged by Providers of the "Real" Online Social Impressions*. *4*(2018), 4652–4661.

Song, J., Lee, S., & Kim, J. (2015). CrowdTarget: Target-based detection of crowdturfing in online social networks. *Proceedings of the ACM Conference on Computer and Communications Security*, *2015-Octob*(i), 793–804. https://doi.org/10.1145/2810103.2813661

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management 1Decision Making. *MIS Quarterly*, *6*, 26–28.

Straub, Detmar W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly*, *14*(1), 45. https://doi.org/10.2307/249307

Tenbrunsel, A. E., & Messick, D. M. (2004). Ethical fading: The role of self-deception in unethical behavior. *Social Justice Research*, *17*(2), 223–236. https://doi.org/10.1023/B:SORE.0000027411.35832.53

Tsikerdekis, M., & Zeadally, S. (2014). Online deception in social media. *Communications of the ACM*, *57*(9), 72–80. https://doi.org/10.1145/2629612

Tsikerdekis, M., & Zeadally, S. (2015). Detecting and Preventing Online Identity Deception in Social Networking Services. *IEEE Internet Computing*, *19*(3), 41–49. https://doi.org/10.1109/MIC.2015.21

Von Solms, B., & Von Solms, R. (2005). From information security to...business security? *Computers and Security*, *24*(4), 271–273. https://doi.org/10.1016/j.cose.2005.04.004

Wang, G., Wilson, C., Zhao, X., Zhu, Y., Mohanlal, M., Zheng, H., & Zhao, B. Y. (2012). Serf and turf: Crowdturfing for fun and profit. *WWW'12 - Proceedings of the 21st Annual Conference on World Wide Web*, 679–688. https://doi.org/10.1145/2187836.2187928

Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, *2*(2), 74–77. https://doi.org/10.1016/j.mfglet.2014.01.005

Wu, L., & Liu, H. (2017). Detecting Crowdturfing in Social Media. *Encyclopedia of*

Social Network Analysis and Mining, *December*. https://doi.org/10.1007/978-1-4614-7163-9

Www.tilastokeskus.fi. (2022). *Tilastokeskus*.

Yoo, K., & Gretzel, U. (2009). Comparison of deceptive and truthful travel reviews. *Information and Communication Technologies in Tourism 2009*, *May 2014*. https://doi.org/10.1007/978-3-211-93971-0

Zhang, D., Zhou, L., Kehoe, J. L., & Kilic, I. Y. (2016). What Online Reviewer Behaviors Really Matter? Effects of Verbal and Nonverbal Behaviors on Detection of Fake Online Reviews. *Journal of Management Information Systems*, *33*(2), 456–481. https://doi.org/10.1080/07421222.2016.1205907

Zhang, J., & Ko, M. (2013). Current state of the digital deception studies in IS. *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, *2*(Proceedings of the Nineteenth Americas Conference on Information System), 985–992.

Zhuang, M., Cui, G., & Peng, L. (2018). Manufactured opinions: The effect of manipulating online product reviews. *Journal of Business Research*, *87*(February 2017), 24–35. https://doi.org/10.1016/j.jbusres.2018.02.016

APPENDIX 1: INTERVIEW QUESTIONS

1) Have fake reviews been discussed or mentioned in your organization, has anyone heard about them?
2) Have You faced any false reviews in your current business (by yourselves or another business entity etc.)?
3) Have you prepared against false reviews in strategical level?
4) If, how you have prepared?
5) What your reaction and actions would be if you found out there is a false review appearance or campaign in your ratings (not a minor one)?
6) Who is responsible in that case, if you appear be under a false review campaign?
7) How do You see the impact of false reviews in your business area now and in the future?
8) Are you planning to focus on false reviews causing problems? How and who would?
9) Any other free comments or feelings. What comes to mind over this topic and interview?