Digitization of manufacturing processes, a must, but also a Trojan horse?
A firm-level study
“Due to espionage you could lose bits, but it is the total package that makes us successful in the market and that cannot be copied."\(^1\)

\(^1\) Quote of one of the respondents, MC1.
Abstract

Stories of industrial espionage are as old as the industries themselves. The different stories arise from changes in technological developments, societal happenings, and from products to manufacturing processes. A recent development, the ongoing digitization of manufacturing processes, Industry 4.0, is an example of a series of technological developments that might result in new stories of industrial espionage, as it might increase firms’ attractiveness (to be spied on) and vulnerability. This, and other forms of innovation added together, could give insights regarding why firms become targets of industrial espionage, with all the associated consequences. To find insights regarding these aspects, this research focused on the relationships between innovation forms and the probability of becoming a target of industrial espionage. A mixed-methods study was conducted, using data of the European Manufacturing Survey 2015 to conduct a logistic regression, combined with semi-structured interviews to investigate the content of the assumed relationships. A distinction was made between several forms of innovation, namely: product innovation, digitization of manufacturing processes (process innovation), and open innovation (innovation process). One finding is that if firms innovate their product incrementally or radically, the probability of becoming a target of industrial espionage respectively triples or almost quadruples. Also, the digitizing of manufacturing processes increases this probability. The results of this research not only have theoretical implications, but are also useful for firms facing strategical considerations regarding innovation forms. The findings together with the suggestions for future research will help to understand and extent the body of literature about industrial espionage and its relation to innovation.

Keywords: Industrial Espionage, Innovation, consequences of Industry 4.0
Preface

Before you lies the final product of my master specialization ‘Strategic Management’. This thesis is the result of a process containing several months (more than expected) of thinking and writing, consulting, rethinking and rewriting, gathering data, analysing, and concluding. To be honest, it has been both a struggle as a highlight, and I am quite pleased with the end result.

In this master thesis I wanted to combine considerations in strategic choices in relation to security issues. By subscribing me for the topics supervised by dr. P.E.M. Ligthart, I got the chance to delve into industrial espionage. If you ask me, an interesting and very topical issue. In search of context, me and my supervisor spoke about the attractiveness of firms as potential targets. From there, the Resource-based view, Knowledge-based view, and theory on Innovation offered a framework, with this thesis as a result.

I would like to thank dr. P.E.M. Ligthart for his supervision. His support, enthusiasm, suggestions, energetic words, and, above all, patience, helped me in all stages of the thesis-process. Moreover, he was kind by allowing me to use the data of the European Manufacturing Survey 2015. Secondly, I would like to thank dr. ir. G.W. Ziggers for being the second examiner of the final version. Finally, I would like to thank all respondents that I interviewed. Our conversations have led to interesting quotes and insights, and all respondents have been very hospitable.

With finishing this thesis, my time as a student has come to an end. I look back at great years of academic challenges and enriching moments, and I am looking forward to bring all the gained knowledge and experiences into practice. Hopefully, I can combine Business- and Public Administration in my career.

Jasper Haen
Nijmegen, May 7, 2018
# Table of contents 1/2

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>3</td>
</tr>
<tr>
<td>Preface</td>
<td>4</td>
</tr>
<tr>
<td>Chapter 1 – Introduction</td>
<td>7</td>
</tr>
<tr>
<td>1.1 Background on industrial espionage and innovation</td>
<td>7</td>
</tr>
<tr>
<td>1.2 Research objective</td>
<td>10</td>
</tr>
<tr>
<td>1.3 Research question</td>
<td>10</td>
</tr>
<tr>
<td>1.4 Perspectives</td>
<td>11</td>
</tr>
<tr>
<td>1.5 Academic and practical/social relevance</td>
<td>11</td>
</tr>
<tr>
<td>1.6 Outline of the master thesis</td>
<td>12</td>
</tr>
<tr>
<td>Chapter 2 - Theoretical background Industrial Espionage</td>
<td>13</td>
</tr>
<tr>
<td>2.1 Industrial Espionage defined</td>
<td>13</td>
</tr>
<tr>
<td>2.2 Intensity</td>
<td>14</td>
</tr>
<tr>
<td>2.3 Reasons for Industrial Espionage</td>
<td>15</td>
</tr>
<tr>
<td>2.4 Forms of espionage</td>
<td>16</td>
</tr>
<tr>
<td>2.5 Impact</td>
<td>19</td>
</tr>
<tr>
<td>2.6 Summary</td>
<td>20</td>
</tr>
<tr>
<td>Chapter 3 - Theoretical background Innovation</td>
<td>21</td>
</tr>
<tr>
<td>3.1 Innovation</td>
<td>21</td>
</tr>
<tr>
<td>3.2 Product Innovation</td>
<td>23</td>
</tr>
<tr>
<td>3.3.1 Digitization as process innovation</td>
<td>25</td>
</tr>
<tr>
<td>3.3.2 Industry 4.0</td>
<td>27</td>
</tr>
<tr>
<td>3.4 Innovation processes</td>
<td>33</td>
</tr>
<tr>
<td>3.5 Towards a conceptual model</td>
<td>37</td>
</tr>
<tr>
<td>3.6 Summary</td>
<td>38</td>
</tr>
<tr>
<td>Chapter 4 – Research Methodology</td>
<td>40</td>
</tr>
<tr>
<td>4.1 Research design/strategy</td>
<td>40</td>
</tr>
<tr>
<td>4.2 Research process/data collection</td>
<td>40</td>
</tr>
<tr>
<td>4.3 Operationalization</td>
<td>42</td>
</tr>
</tbody>
</table>
Table of contents 2/2

4.4.1 Data analysis 45
4.4.2 Data inspection and preparation 45
4.4.3 Reliability and validity 46
4.4.4 Assumptions of the (multiple) logistic regression analysis 47
4.5 Research ethics 48
4.6 Summary 48

Chapter 5 – Results 49
5.1.1 Quantitative analysis 49
5.1.2 Sample statistics 49
5.2.1 The model 52
5.2.2 Logistic regression 52
5.2.3 Hypotheses 54
5.2.4 Summary 57
5.3.1 Qualitative analysis 58
5.3.2 Main concepts 58
5.3.3 Inter-concept relations 70
5.3.4 Other memorable quotes 75
5.3.5 Summary 76
5.4 Concluding words 76

Chapter 6 - Conclusions, implications and limitations 78
6.1 Summary 78
6.2 Implications 80
6.2.1 Theoretical implications 80
6.2.2 Practical implications 80
6.3 Limitations 81

References 84
Appendices 94
Chapter 1 – Introduction

It is probably not the first time that a rental company does not retrieve a rented car in its original state. Yet, this time it is a special story. The car, a Tesla model X, was returned in remarkable condition, after which the owners wanted to recover the damage from the tenant. But the tenant turned out to be without trace. After some investigation, a mysterious note in the glove compartment, and the GPS data from the ripped Tesla, the crime scene was unravelled: the Mercedes-Benz Technology Center in Sindelfingen (Andersen, 2017).

However, it is common practice in the automotive industry to buy and dismantle models of competitors - the American General Motors has a real 'demolition lab' for it --, it is not common to rent a car for espionage purposes. The mysterious note turned out to be a warning ticket for illegal parking, prepared by the parking watch of the Mercedes-Benz Technology Center (Andersen, 2017). This is just one of many examples of industrial espionage, in search of intellectual property (IP) and trade secrets to overcome discrepancies regarding competitive advantages.

1.1 Background on industrial espionage and innovation

Industrial Espionage

The topics of industrial/corporate and economic espionage are interesting ones. The first stories about these phenomena go way back in time. According to Harris (1998) this was already the case in the eighteenth century, where Britain and France were getting involved in these affairs. But also China got involved back then, with tea as the product in the centre of these spying activities (Rose, 2009). And of course, the race to space wherein eternal enemies Russia and the United States of America were spying on each other’s developments is a well-known example (Cadbury, 2006). These stories of espionage arise from changes in technological developments, societal happenings, from products to manufacturing processes, and with different purposes.

Industrial espionage is a form of information gathering. It entails purposeful gathering of information of economic and business value related to trade secrets, product formulae, concealed business strategies, trade negotiation strategies, business plans and product development of industry competitors (Crane, 2003). Especially espionage regarding products
and product innovations appeal to the imagination, as there are more and more Chinese counterfeit products for sale.

Corporate or industrial espionage could threaten any business, in particular of those whose right to exist depends on information. This risk of industrial espionage might eventually corrupt one’s competitive advantage with possibly devastating effects. One of the causes of sustainable competitive advantage could be the digitization of the businesses, which recently has been called a ‘megatrend’ (PricewaterhouseCoopers, n.d.). It is not unthinkable that industrial espionage and innovation develop in a parallel fashion.

Nowadays, in the so-called fourth revolution, new threats arise. One of the most significant changes has been the rise of information technology and security as important, integral parts of everyday activities and communication. Communication networks are used to transfer more sensitive information that can be valuable and confidential, requiring protection against human misuse and also attracting the attention of attackers. Almost all types of organizations are dependent on IT systems to carry out a large part of their business (Tripathi & Singh, 2012). In recent years, reports from the German government agencies for the protection of the constitution have shown that espionage activity in German Research & Development (R&D) is increasing steadily (Thorleuchter & van den Poel, 2013; German Federal Ministry of the Interior, 2011).

**Innovation**

Innovating is seen as an important driver of economic growth for a long time (Schumpeter, 1934). From an innovation perspective one could see how organizations respond to internal (technical divisions, marketing and sales, logistics, production etc.), or external (customers, suppliers, competitors, consultants, media, globalization etc.) opportunities, and use its creative efforts to introduce new products, processes or other ideas (Şimşit et al., 2014; Kelly & Kranzburg, 1978). But it is challenging to ensure that innovation is rewarding. To protect innovation outcomes, the Trade Related Aspects of Intellectual Property (TRIPS) is drafted. This international agreement ensures a minimum level of protection of trade secrets, often referred to as confidential information or industrial secrets (Dessemontet, 1998), for the members of the World Trade Organization. Intellectual Property, property of information (Cooter & Ulen, 2004), or, more specifically, “an intangible asset... which has been granted legal protection and recognition” (Anson & Suchy, 2005, p.16), allows innovators to
appropriate the returns from their innovations through legal monopolies over these innovations (Scotchmer & Green, 1990). One could question if this is enough, looking at the current developments in technology. According to the Oslo Manual (2005), there are four types of innovation, namely: product, process, organizational and marketing innovation. In addition, collaborative innovation forms, such as open innovation, have become hot topics in innovation management (Huizingh, 2011).

Due to new and innovative production technologies and the further integration of ICT in the entire production process, the manufacturing industry is changing radically. This era of ongoing digitization is also known as Industry 4.0 (originates in Germany), and has been frequently called Smart Industry² (term used in the Netherlands). Industry 4.0, in this research seen as process innovation, is being driven by digitization and integration of vertical and horizontal value chains, digitization of product and service offerings and the development of new digital business models and customer access platforms (Kagermann et al., 2013). What also could be critical, is the evolution of traditional supply chains toward a connected, smart, and highly efficient supply chain ecosystem (Schrauf & Berttram, 2016, p.4).

It is easy to see why there is a trend of investment rush. Supply chain experts expect digitization to bring significant economic benefits. Firms with highly digitized supply chains and operations can expect 4.1% efficiency gains, while increasing revenue by 2.9% a year (Schrauf & Berttram, 2016, p.11). This is because the main idea of the digital supply chain is to match the right customer with the right product as quickly as possible — and do this responsively and reliably, while increasing efficiency and cutting costs through automation (Schrauf & Berttram, 2016, p.12). But where the digitization era has come, new risks arise. One could assume that a firm which is digitizing the production technologies, creating a competitive advantage, becomes an attractive target of industrial espionage in the near future.

Therefore this trend goes hand in hand with an important security question which has to be addressed. This highly digitizing organizations are technologically advanced and are possibly easier to spy on due to their ongoing digitization. One the one hand, organizations would like to optimize their processes by digitizing, reaching the highest possible performance outcomes.

---

² A smart way to combine the real and virtual world by implementing Cyber-Physical-Systems and the Internet of Things in the products and industrial processes to create a flexible and self-managing network between people, machines, products, buyers and suppliers (Moester, 2017).
On the other hand, digitization asks for a different and more intensive way of protecting vital information in terms of maintaining a competitive advantage. This issue is crucial and a possible answer could lie in how the organizations innovate.

1.2 Research objective
Looking at innovation forms, the link between industrial espionage and product innovation appeals to the imagination. One could think of the stealing and copying of competitors’ products. But industrial espionage is definitely not only about products. The main objective of this research is to explore if there is a relation between firm-level digitization of manufacturing processes and an increasing threat of industrial espionage. By choosing the title of this research a controversy is recognized. As was cited by Cohen (2017): "For companies to survive a discontinuity, they must face the rather unpalatable reality that there may have to be fundamental changes in who they are, what they do, and how they do it, as wrenching and dislocating as it may be". In other words, it could be a must to go along with the trend of digitization. In contrast, digitization could make a firm vulnerable, resulting in an increase in attractiveness. In addition, digitization could also be an attractive aspect in terms of interconnectedness, a reason for other firms to collaborate. But collaborations could also increase vulnerability, being as weak as the weakest link. An interesting question is if these vulnerabilities strengthen each other. In other words, how do innovation forms influence the probability of becoming a target of espionage, with the digitization of manufacturing processes seen as central approach. A combination of these could increase the attractiveness of the firm, making it more likely to be chosen as a target to spy on. To capture the concept of firm-level innovation, product innovation and open innovation are included, whereas digitization is seen as a form of process innovation. The objective of this research is to investigate if and which forms of innovation influence the attractiveness of firms regarding being spied on. Firms in the Dutch manufacturing industry are the unit of research focus.

1.3 Research question
The research question is the leading guideline in this thesis and its design. It reads as follows:

What is the impact of digitization of manufacturing processes, product innovation, and open innovation, on the probability of becoming a target of industrial espionage for firms in the Dutch manufacturing industry?
By formulating this research question, four other questions pop up, namely:

1. **What is industrial espionage, what are the characteristics, and who is spying?**
2. **What is product innovation, what are the characteristics, and what forms are existing?**
3. **What is the digitization of manufacturing processes and what are the characteristics?**
4. **What is open innovation, what are the characteristics, and what forms are existing?**
5. **What is the impact of the forms of innovation on the probability of becoming a target of industrial espionage and is there a moderating effect of open innovation on the relation between digitization and industrial espionage?**

**1.4 Perspectives**
To come to a solid theoretical background several perspectives are used. The earlier mentioned Industry 4.0 is explained as well as the literature on Industrial Espionage. Also, the Resource-Based View and the Knowledge-Based View are used as underlying perspectives in understanding the attractiveness. The literature on product innovation and open innovation is used to understand what factors could affect the possible risk of becoming a target of espionage.

**1.5 Academic and practical/social relevance**
This research is trying to contribute to the existing knowledge on industrial espionage and mainly to answers to the question of how to value and counter any threats that come with this topic for organizations that are digitizing rapidly. The focus lies on mapping which factors influence being attractive as a potential target. Furthermore, it could be useful for managers to know best practices regarding choosing innovation practices in relation to the probability of becoming a target of industrial espionage, and implement these in their organizational processes, but that is beyond the scope of this research.

Besides that, there is also a social issue covered in this research. Not only the research domain of business administration is dealing with this question of industrial espionage and how to protect information properly, but other domains are also dealing with these issues. For instance, the domain of public administration and in the extension of that governments as well. The issue is not only about defending against espionage for the sake of the own firm but it could be seen far broader than that. If civilians can no longer rely on information being secure, they could be losing trust in firms, with all negative effects imaginable, as well as in the authorities which are in contact with these civilians.
1.6 Outline of the master thesis

In the following chapter, the context of industrial espionage is discussed. Questions like what is industrial espionage and in what forms does it occur are answered here. After understanding the context, the implications of industrial espionage are discussed, such as: what is the impact and which role plays cyber in this question.

In chapter three the characteristics and implications of innovation are addressed. A distinction is made between product innovation, process innovation (digitization of manufacturing), and innovation processes (open innovation), seen as a firm’s innovation activities. The different forms are discussed, especially Industry 4.0. Besides that, the how-question is addressed; how do innovation forms influence the attractiveness of firms concerning industrial espionage, and, in addition, how does open innovation affect the relation between the digitization of manufacturing processes and the risk of industrial espionage. Four hypotheses and a conceptual model are presented in this chapter.

In the fourth chapter, the methods used in this research are explained. A mixed methods research design is used to investigate the formulated hypotheses. In this chapter the operationalization of the concepts is presented and the assumptions of the logistic regression are addressed. This regression technique is leading in the quantitative analysis. Semi-structured interviews are used to give substance to the qualitative section.

In chapter five the results of the quantitative and qualitative analysis are presented. The chapter starts with a logistic regression with data from the European Manufacturing Survey (2015). This is followed by a qualitative analysis of the eight conducted interviews. These interviews are transcribed and theory-based coded.

The last chapter provides conclusions, implications and limitations of the research. A summary is given of the whole research and theoretical and practical implications are appointed. At last, the limitations of the research are addressed and recommendations for further research are presented. Figure 1 shows a visualization of the all chapters of this thesis.

Figure 1: Visualization of the outline
Chapter 2 – Theoretical background Industrial Espionage

The theoretical background of Industrial Espionage is explained in this chapter. The characteristics of the phenomenon are described and its forms are addressed. Also, the question to what extent the topic plays a role in organizations is answered. This is important information to come to formulating the hypotheses in the following chapter.

2.1 Industrial Espionage defined

In this paragraph, the content of Industrial Espionage is addressed. As was mentioned in the previous chapter, Industrial Espionage is a form of information gathering. All organizations collect, in some way, and make use of forms of information about competitive and other organizations. The legal portion of espionage has given rise to accelerated business intelligence (Samli & Jacobs, 2003). It includes for instance, the examination of publicly available information – court records, corporate annual reports, market reports, trade fairs, and others. Intelligence gathering activities like these are quite a standard pallet of market research and competitor benchmarking, which could lead to effective competitive behavior. This sensitive information can usually be obtained legally, and with varying degrees of ‘ethics’ (Androulidakis & Fragkiskos, 2016). Once they are put together and analyzed, they can provide useful information to predict changes in company direction or to deduce the details of new products and innovations (Wright & Roy, 1999). Knowledge spillovers do also contribute to this problem.\(^3\)

Crane (2005) suggests that any means of gathering information is acceptable in a competitive context. Competitors are, in the end, being in an ongoing, zero-sum battle with each other for customers, resources, and other rewards. It becomes illegal espionage when it involves the theft of proprietary information, materials, or trade secrets (Nasheri, 2005). Also bribing, blackmailing and using advanced electronic means of surveillance and interception are known forms of Industrial Espionage (Androulidakis & Fragkiskos, 2016).

It has been established that in a continuously globalizing world, intellectual capital of industrial

---

\(^3\) Firms might seek external knowledge through indirect means of knowledge spillovers: involuntary leakage or voluntary exchange of useful technological information (De Bondt, 1997). Or as Agarwal et al. (2010) define knowledge spillovers: the external benefits from the creation of knowledge that accrue to parties other than the creator.
companies is a key force in enhancement of the competitive advantage (Samli & Jacobs, 2003). Littlejohn (1994) stated that the more successful an organization is, the more likely it might to become a target of industrial espionage. The combination of the steadily increasing value of trade secrets and the spread of technology throughout the globe creates a significant increase in both the opportunities and motives to perform economic espionage (Nasheri, 2005). This should be of big concern for industrial manufacturers since not only their finished products, but their processes to generate these products are in danger.

Not every organization is equally attractive or faces the same risks. An organization is more likely to be a potential target, if it has important clients, or if it operates in the aerospace, biotechnologies, chemicals, communications, computer, electronics, nuclear energy, oil and gas, or environmental industries (CSIS/SCRS, 1996). Silicon Valley is known to be one of the world's most targeted areas for espionage, though any industry with information of use to competitors may be a target (Nasheri, 2005). Depending on the industry, protection efforts might concentrate on marketing plans, manufacturing and production secrets, or even human resource policies (Wright & Roy, 1999).

### 2.2 Intensity

It is difficult to determine to what extent organizations become a victim of Industrial Espionage. Not only the frequency of this act is kind of undisputed (some espionage activities stay undetected) but also the impact is not easy to define. Concerning cybercrime, which is a part of Industrial Espionage, there are figures known, though these are probably only the tip of the iceberg.

To give a little insight two surveys are addressed. Thonnard et al. (2012) refer to a survey done by Symantec.cloud on cyber-attacks. In 2005, targeted attacks were observed at the rate of one attack per week, rising to one or two per day during 2006, to approximately 60 per day during 2010, and approximately 100 per day towards the end of 2011 (Symantec, 2011). From April 2008 to April 2012, approximately 96,000 targeted attack emails were identified and registered by Symantec, with only 30,000 of them identified in 2011 (Thonnard et al., 2012). Looking at these numbers it should be said that they must be interpreted in the context of the 500,000 malware and phish emails that are detected each day by Symantec.cloud. One could conclude that targeted attacks remain rare in comparison with non-targeted malware. It is this rarity that makes detection all the more difficult (Thonnard et al., 2012).
A survey by the Ponemon Institute showed the average cost of cybercrime for US retail stores more than doubled from 2013 to an annual average of US $8.6 million per company in 2014 (Ponemon Institute, 2014). Not only are the attacks more damaging, there also are more of them (CSX, 2015). The survey reported that the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48 percent from 2013 (Ponemon Institute, 2014). Another survey by PricewaterhouseCoopers (2015) showed that the number of detected information security incidents has risen 66 percent year over year since 2009. One could say that based on these figures the quantity of attacks has risen significantly.

2.3 Reasons for Industrial Espionage

There are several authors (Samli & Jacobs, 2003; Nodoushani & Nodoushani, 2002; Sommer, 1994) who wrote about possible reasons to choose for Industrial Espionage as a(n) (additional) firm’s strategy. There are general reasons as the need to establish or gain competitive advantage, the increasing value of trade secrets\(^4\) and the impact of globalization\(^5\), which all ask for reaction in any form (including Industrial Espionage). Most of the reasons can be divided into categories. The author suggests that the reasons could be categorized by a lack of knowledge on (1) products and (2) manufacturing processes, a lack of (3) resources, Causal Ambiguity\(^6\), lack of information on a specific competitor and others, which are summed up in table 1. Among others, the lack of protection is called, but also an overuse of security could aggravate the problem of Industrial Espionage. It could create a false sense of security resulting in slackness and over-relaxation (Androulidakis & Fragkiskos, 2016).

---

\(^4\) Most companies are unprepared for potential losses caused by espionage (Samli & Jacobs, 2003).

\(^5\) Globalization is a major force in bringing world markets closer together as it creates technology flow, information flow, know-how flow, and capital flows through cyberspace (Samli, 2002). But these flows not only enhance awareness of new products, new developments, and new technologies, but also forces many regional and local companies to protect themselves by competing with global firms.

\(^6\) In some cases competitors do not know where the competitive advantage arises from, which could be a reason to spy. This is called causal ambiguity. Causal ambiguity is explained as the degree to which a competitor is not able to determine what the decisive assets are which have given rise to the competitive advantage (Dierickx & Cool, 1989).
Table 1.


<table>
<thead>
<tr>
<th>Knowledge of Products</th>
<th>Knowledge of Processes</th>
<th>Resources</th>
<th>Causal Ambiguity</th>
<th>Information on specific competitors</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>- To acquire new technology at the lowest possible cost.</td>
<td>- Timing and process know-how;</td>
<td>- Lack of Resources to Innovate;</td>
<td>- To uncover marketing plan, product launches, etc., planned by competitors.</td>
<td>- To expand a list of potential customers and clients by seeing who buys from competitors;</td>
<td>- Lack of Protection;</td>
</tr>
<tr>
<td>- To obtain research material at the lowest possible cost.</td>
<td>- Lack of corporate intellectual capital: human capital (power of information);</td>
<td>- To lower R&amp;D costs by discovering what has already been achieved by others;</td>
<td>- To determine competitors’ sales figures;</td>
<td>- To discover trade terms offered by competitors;</td>
<td>- To ascertain that the company is paying the lowest possible price for its raw materials;</td>
</tr>
<tr>
<td>- To avoid wasting research resources in pursuing what others have already found unprofitable.</td>
<td>- To lower R&amp;D costs by discovering what has already been achieved by others;</td>
<td>- To calculate competitors’ detailed cost breakdown.</td>
<td>- To aid a merger or acquisition, or to fight off a hostile takeover.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.4 Forms of espionage

There are many forms of or tactics in Industrial Espionage. These forms are consistent with the reasons for industrial espionage in the previous paragraph. Samli and Jacobs (2003) divide twelve major spying practices, among which dumpster diving, industrial theft and reverse engineering. All practices are shown in Appendix A. It is remarkable that Samli and Jacobs (2003) did not mention cyber-espionage in their article, though it is an important aspect in relation to digitization. Therefore, at the end of this paragraph, cyber-espionage is addressed. Also, the distinction between insiders and outsiders is made in this paragraph.

---

7 Cyber-espionage was less seen and known as threat, and not yet that far developed.
Outsiders

Nasheri (2005) defines outsiders as “individuals or corporations that steal trade secrets for their own use or to sell to a third party”. One interesting outsider is the information broker. This middle-man will obtain information from one source and sell it to organizations that want it. This just adds to the complexity of the problem, because this causes that the person who has obtained the information no longer needs to have a direct connection with the organization that could benefit from it. Those can now operate through a third party making the identification of the source of an information leak more difficult (Jones, 2008). So outsiders can either sell or use the stolen goods themselves (Nasheri, 2005).

Outsiders can use a whole spectrum of ways to snatch useful information. “The most frequently used collection method is the recruitment of someone who has access to information (employees, contractors, consultants, students, etc.). However, other methods include break-ins, briefcase tampering, photocopying, and communications interception” (CSIS/SCRS, 1996). There are clear illegal forms, such as entering and breaking in competitors’ offices to steal information, but there are also more gray areas. One could think of searching through a competitor’s garbage (dumpster diving), hiring private detectives to follow competitor’s staff, infiltrating with industrial ‘spies’, pressuring the customers or suppliers of competitors to reveal sensitive information about their operations, and more (Crane, 2005). Some of the more common international snoops include competitors, vendors, investigators, business intelligence consultants, the press, labor negotiators, and government agencies (Nasheri, 2005; Murray, 2003). The tools of the espionage community include scanning trade-show floors, combing through websites, reviewing filings with regulatory agencies, eavesdropping in airline terminals and on airline flights, taking photographs of factories and business offices, using data-mining software to search the Internet at high speeds for information, using ‘shadow teams’, stealing laptop computers, tuning in to computer monitors from a nearby location using surveillance equipment, attending competitors’ court trials, and even the earlier mentioned ‘dumpster diving’ (Nasheri, 2005; King & Bravin, 2000; Gomes, 1999; Wingfield, 2000; McCarthy, 2000; Bennett & Mantz, 2000). These are all tactics that have been, and indeed continue to be, used by intelligence gatherers in industry (Crane, 2005).

Insiders

Insiders do have immediate access to enormous amounts of valuable information in comparison to outsiders. They don’t use all the tactics as outsiders do. From the insider threat perspective
the most frequent way is accidental exposure, usually owing to employee negligence, ignorance or carelessness (Littlejohn, 1994). Benny (2013, p.13) mentions that the decision of insiders to take part in industrial espionage might be for personal gain, to make a political or ideological statement, for thrill-seeking, or for rancor or revenge. Steel and Wargo (2007) complement this sum up with ‘sense of entitlement’, ‘personal and social frustrations’, ‘ethical flexibility’, ‘reduced loyalty’, and ‘lack of empathy’.

Sometimes employees are forced to provide essential trade secret information. Recruitment of these persons for espionage is often accomplished through the use of the MICES principle (Fitzpatrick & Burke, 2001; Cornwall, 1991; Barron, 1985). MICES stands for recruitment methodologies based on money, ideology, compromise, ego and sexual entrapment (Fitzpatrick et al., 2004).

**Insider Threat**

Only a few cases of insider threats eventually become public, due to the negative impact of publicity or corporate reputational damage upon reporting of an insider incident (Boateng, 2013). Insider threats are characterized as malevolent, already trusted entity with access, privilege knowledge of systems and networks. An insider could be anyone who has the corporate ‘power of attorney’ to act for and on behalf of the organization (Boateng, 2013, p. 17). The greatest security threat comes from the person with authorized access (Sarkar, 2010). Insider activities can significantly result in losses such as revenues, intellectual property, and corporate reputation – if the firm fails to prevent, detect and investigate insider threats (Mills et al., 2009). These activities include denial of service of resources, corruption of databases and file servers, and disruption of international network operations. Mills et al. (2009) claim that big amounts of dollars could be lost to stolen information, intentional or inadvertent, or become lost, deleted or corrupted by a click of a button.

**Cyber**

Cyber-espionage is defined as “the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward” (O’Hara, 2010). With cyber-espionage, there is a high risk of non-detection. Non-detection was explained by one expert this way: "If I [physically] steal your car, you know because it is gone, but if I steal your customer list or a design plan . . . you will not know that I
have it, and you will remain comfortable” (Charney, 2000). In addition, cyber risk can be defined as: “a multitude of different sources of risk affecting the information and technology assets of a firm” (Biener et al., 2015).

One could distinguish two different types of cybercrime – targeted and non-targeted attacks. In targeted attacks, there is evidence that the attacker has specifically selected the recipients of the attack. This is not the case by non-targeted attacks whereby it appears as if the attacker wishes to compromise a number of systems without regard to the identity of the systems. (Thonnard et al., 2012, p.66). In this research, the first type is leading.

Cybersecurity could be defined as the protection of data and services in (digital) systems against misuse, e.g. unauthorized access, modification or destruction (Kagermann et al., 2013). It is actually a business concern and not really a technological issue, as perceived by most business executives and even IT administrators. It is more of a human problem than it is technical (Boateng, 2013). It is therefore important to monitor organizational processes and design them in a way to reduce the insider threat.

The research of Thonnard et al. (2012) shows that not only large corporations, governments and Defense industries, and more particularly senior executives and subject matter experts, are being targeted by ‘targeted’ attacks. They have evidence that at least for their set of targeted attacks collected in 2011, this was true only for 50% of the attacks. Moreover, while the ultimate goal of attackers is more than often to capture the knowledge and intellectual property that senior-level employees have access to, they do not have to attack them directly to steal the information they want (Thonnard et al, 2012, p.65).

2.5 Impact
To determine the impact of Industrial Espionage a comparison is made between knowledge leakage and industrial espionage. This is based on earlier research done by Brunnermeier (2005). The mindset is that if it is a good measure for the sensitivity of a Research & Technology (R&T) project from an organization concerning espionage is the risk of an information leakage within this R&T project (Brunnermeier, 2005; Matsui, 1989), it should be also the other way around.
Leaking (and therefore Industrial Espionage) could have potentially devastating consequences in terms of competitive advantage, and occurs on a number of fronts (Ahmad et al., 2013). There are several ways in which leakage can influence organizations. One could think of loss of revenue, loss of productivity, reputational damage, and costs arising from breaches of confidentiality agreements. With significant efforts of recovery, organizations get over such incidents. But if the leakage concerns knowledge related to an organization’s valuable, rare, inimitable and non-substitutable resources that provide and sustain competitive advantage, recovery could be considerably more challenging (Ahmad et al., 2013).

2.6 Summary
In this chapter, the characteristics and reasons of Industrial Espionage are addressed. Also, the forms of Industrial Espionage are summed up, with an important role for the cyber-related aspects. Now these features are explained, the following chapter will go deeper into Innovation, and its relation to Industrial Espionage. The described aspects of innovation pose risks of becoming a target of Industrial Espionage, clarifying the relationship and explaining the attractiveness of a firm.

---

8 From the Resource-based View
In this paragraph, the characteristics and forms of innovation are addressed. Product- and process (manufacturing) innovation, and innovation processes are discussed. Also, the link between these forms and Industrial Espionage, and why these might increase risks, are explained. The focus on innovation and innovation activities arises from the idea that these could be aspects of attractiveness. This will lead to four hypotheses at the end of the chapter, creating the conceptual model.

3.1 Innovation

Innovation can be defined as “the production or adoption, assimilation, and exploitation of a value-added novelty in economic and social spheres; renewal and enlargement of products, services, and markets; development of new methods of production; and establishment of new management systems” (Crossan & Apaydin, 2010). On one hand, innovation consists of the ability to discover connections, to see opportunities and to take advantage of them, but on the other hand, it is not only about finding and opening up new markets as it is also about offer new ways of serving established and mature ones (Tidd et al., 2005). The current Oslo Manual (2005) divides four categories of innovation: product-, process-, organizational- and marketing innovation. These are defined as:

- ‘product innovation’ – the introduction of a good or service that is new or significantly improved with respect to its characteristics or intended uses. This includes significant improvements in technical specifications, components and materials, incorporated software, user-friendliness or other functional characteristics;
- ‘process innovation’ – the implementation of a new or significantly improved production or delivery method. This includes significant changes in techniques, equipment and/or software;
- ‘organizational innovation’ – the implementation of a new organizational method in the firm’s business practices, workplace organization or external relations;
- ‘marketing innovation’ – the implementation of a new marketing method involving significant changes in product design or packaging, product placement, product promotion or pricing.
Knowledge and innovation management

Innovation is about knowledge – creating new possibilities through combining different knowledge sets (Tidd et al., 2005). Henderson and Clark (1990) state that innovation is rarely about dealing with a single technology or market. It is rather a bundle of knowledge which is brought together into a configuration. This approach could be an important motive for the mentioned ‘open innovation’ paradigm, which will be discussed later this chapter.

Innovation management is about organizations responding to internal or external opportunities, and use its creative efforts to introduce new ideas, processes or products (Şimşit et al., 2014; Kelly & Kranzburg, 1978). As a result of increased competition and shifts in the demand and taste of customers (Danneels, 2002), it is of importance for firms to manage innovation in a fast and flexible way in order to achieve a sustainable competitive advantage by overcoming competitors (Takeuchi & Nonaka 1986; Pooleton & Barclay 1998). Also, the resource-based view emphasizes the importance of innovation as source of competitive advantage (Hall, 1993). Tidd et al. (2005) state that innovation is about taking risks and deploying what are often scarce resources in projects, which are no guarantee for success. A possible solution is to design innovation in such way (networking) that it can help spread risks and in the process extending the range of things which might be tried (Tidd et al., 2005). For successful innovation management, it requires to get hold of and use knowledge about components but also about how those can be put together (Tidd et al., 2005) – Henderson and Clark (1990) termed this the architecture of an innovation.

It is very often believed that higher R&D spending heightens the level of research activity within a firm and builds specialized scientific/technological expertise as a result. The tangible outcome of it is the ability to develop several significant product technologies (Parthasarthy & Hammond, 2002). Recalling the previous chapter, one could imagine that this makes a firm attractive to spy on.

Development in time

Since the 1950’s there has been an increase of innovation models, each of which explains and/or guides the process of innovation within industrial firms. Rothwell (1992) studied these

---

9 To gain competitive advantage over its rivals, a company must either perform technologically and economically distinct activities (value chain) at a lower cost or perform them in a way that leads to differentiation and a premium price (Porter & Millar, 1985).
changing perspectives on industrial innovation and divided this phenomenon into five generations. Şimşit et al. (2014) supplemented these by another one.

The models of innovation develop from technology push-models to network models and even to an open innovation model. First, the models\(^{10}\) emphasized only on R&D and science, after which the second generation models (1960-1970) began to stress the role of the marketplace and market research in identifying and responding to customer needs. The third generation models (1970-1980) emphasized on feedback loops between R&D and marketing, after which the fourth generation (1980-1990) combined of push and pull models and focused on external linkages. A noticeable difference was introduced in the fifth generation (1990-2000) model as it emphasized on knowledge accumulation and external linkages, systems integration and extensive networking. At last, the sixth generation model (2010- ), could be seen as a network model of the innovation process. Instead of only focusing on internal idea generation and development, internal and external ideas can be combined, as well as internal and external paths to market, to advance the development of new technologies (Preez and Louw, 2008). These are known as Open Innovations.

Remarkable is the increase of interconnectedness of firms, as innovation has become more a joint activity. Industry 4.0, the process of digitization, fits this concept and could be seen as a 6th generation model, maybe even a 7th generation model\(^{11}\). It is a form of process innovation as it changes the ways of manufacturing and delivering of goods, and by this, the interconnectedness of firms increase. After addressing product innovation in the following paragraph, the digitization of manufacturing processes is further explained.

### 3.2 Product Innovation

Dewar & Dutton (1986) define innovation “as an idea, practice, or material artifact perceived to be new by the relevant unit of adoption”. In this definition product innovation is viewed as an outcome. Unfortunately, this way of defining product innovation does not distinguish the degree of perceived newness regarding the content embodied in the innovation. Therefore Dewar & Dutton (1986) supplement their definition to this fact and divide two forms: radical and incremental innovations. The major difference is that incremental innovations are characterized by minor improvements or simple adjustments in current technology, while

\(^{10}\) 1950-1960

\(^{11}\) Which does not yet exists.
radical innovations involve fundamental and revolutionary changes in technology that represent a substantial departure from the existing practice (Dewar & Dutton, 1986). The more radical an innovation is, the higher is the level of new knowledge embedded in the innovation. And with knowledge, there is knowledge leakage, as was discussed.

Product innovation is a potential strategic weapon for all businesses, and of all the different types of innovation, product innovation presents a rich variety of competitive options (Johne & Snelson, 1988). It is, without questioning, important for businesses which want to compete on the basis of quality and suitability of purpose. Foster (1986) states that all businesses, sooner or later, need to update their products, and if possible, develop completely new products, especially when new technology makes this attractive. Businesses who refuse do this, will be overtaken by competitors, either from inside their own industry or from outside (Foster, 1986).

Freeman (1982) defines product innovation as a ‘complex coupling’ between market needs and technologies over time. It is challenging to link technological and market possibilities. It asks for choices to be made, among multiple design options, each with different outcomes. Moreover, the potential market may be new, which makes it difficult to determine who the most likely customers are and what they actually need (Clark, 1985). Developing innovative products should therefore be a process of double loop learning (Argyris and Schon, 1978), incorporating new insights and reconsidering the premises.

There are three important suggestions in the literature which predicts successful product innovation. Firstly, the commercial success of a new product depends on how well the product’s design meets customers’ needs (Rothwell et al., 1974; Lilien and Yoon, 1988). The second finding is that cooperation among the manufacturing, technical, marketing, and sales departments contributes to a new product’s success (Bonnet, 1986; Dean and Susman, 1989). Though, and that is the third finding, product innovators often do not link technological and market issues, and forget to cooperate across departments (Cooper and Kleinschmidt, 1986; Souder, 1987). But if product innovation is successful, others will notice sooner or later, with corresponding risks of industrial espionage.
3.3.1 Digitization as process innovation

Digitization is the process of converting analog information to a digital format (Katz et al., 2013) or a digital representation of a physical item, with the goal to digitize and automate processes or workflows (i-Scoop, n.d.). In the Oxford English Dictionary, digitalization is described as ‘the adoption or increase in use of digital or computer technology by an organization, industry, country, etc.’. Gartner (n.d.) complements this definition by adding that “the use of digital technologies is to change a business model and provide new revenue and value-producing opportunities”. In this sense, it could be seen as a process of moving to a digital business and therefore digitalization requires digitization of information (i-Scoop, n.d.). Friedrich et al. (2011), on the other hand, define digitization as “the pervasive adoption of a wide variety of digital, real-time, and networked technologies, products, and services that will enable people, companies, governments, and even machines to stay connected and communicate with one another, gathering, analyzing, and exchanging massive amounts of information on all kinds of activities”. Comparing the definition of digitization and process innovation one could see that digitization is a form of process innovation. Digitization and digitalization trigger a radical transformation of the manufacturing environment, which requires response. “It potentially represents a complete overhaul of the economic rationale behind business” (Blachet & Rinn, 2016).

As was mentioned, innovation is about knowledge. The knowledge-based view suggests that firm-specific knowledge constitutes the most strategically important source of competitive advantage (Grant, 1996; Grant & Baden-Fuller, 2004; Jiang et al., 2013). The importance of knowledge as a source of competitive advantage has also heightened interest in understanding how firms identify, acquire, and use externally-generated knowledge (Alcácer & Chung, 2007). With regard to the latter, firms might seek external knowledge through indirect means of knowledge spillovers: involuntary leakage or voluntary exchange of useful technological information (De Bondt, 1997). Agarwal et al. (2010) define knowledge spillovers as the external benefits from the creation of knowledge that accrue to parties other than the creator.

---

12 Process innovation is the implementation of a new or significantly improved production or delivery method. This includes significant changes in techniques, equipment and/or software (Oslo Manual, 2005). Process innovations can be intended to decrease unit costs of production or delivery, to increase quality or to produce or deliver new or significantly improved products, creating competitive advantage.
Digitization could be seen as a process of converting tacit to explicit knowledge. Tacit knowledge is comprised of both cognitive and technical elements (Nonaka, 1994). The cognitive element refers to an individual’s mental models consisting of mental maps, beliefs, paradigms and viewpoints. The technical component consists of concrete know-how, crafts and skills that apply to a specific context. Tacit knowledge is perceived to be less susceptible to leakage\(^\text{13}\) (compared to explicit knowledge) because it is difficult to articulate or codify (Hildreth and Kimble, 2002; Nonaka and von Krogh, 2009; Polanyi, 1966).

Explicit knowledge is knowledge that can be codified. Nonaka et al. (2000) describe explicit knowledge as what can be embodied in a code or a language and as a consequence, it can be verbalized and communicated, processed, transmitted and stored relatively easily. It is then available to all members of the firm, or for others in a way that they can access, discuss and transfer it (Tidd et al., 2005), also increasing the vulnerability of the firm.

There are three types of explicit knowledge: cognitive knowledge, advanced systems skills and systems understandings. These types could also be described as the know-how, the know-what, and the know-why questions (Quinn et al., 1996). According to Kikoski and Kikoski (2004), competitive advantage will only be gained if companies value their tacit knowledge, as explicit knowledge can be known by others as well. Tacit knowledge creates the learning curve for others to follow and provides competitive advantage for future successful companies (Kikoski & Kikoski, 2004).

The leakage of sensitive information through unidentified channels and conduits is a particularly challenging management problem (Ahmad et al., 2013). Ornaghi (2006) wrote a paper about spillovers in product and process innovation. He states that there are several channels of technological spillovers, and distinguish differences between the two forms of innovation. “Imitation of a product innovation can be simply achieved through reverse engineering while diffusion of process innovation may require more sophisticated channels, such as industrial espionage or recruitment of engineers and experts of rival firms” (Ornaghi, 2006). The ongoing digitization of processes could eventually change this perspective. In addition, some studies have pointed out that increasing circulation of knowledge increases the risk of leakage (DeSouza, 2006; DeSouza and Vanapalli, 2005; Easterby-Smith et al., 2008;

\(^{13}\) In the previous chapter a comparison was made between knowledge leakage and Industrial Espionage.
Trkman and DeSouza, 2012), which is an expression of the growing interconnectedness of firms.

### 3.3.2 Industry 4.0

As was shortly mentioned in the first chapter, Industry 4.0 is seen as an important concept of process innovation in this research. The first transformation in production and automation was a consequence of the introduction of steam and water power (Industry 1.0), followed by the introduction electrification (2.0), and more recently by the digital computer (3.0). The four revolutions are shown in figure 2.

![Figure 2. The four Industrial revolutions. Source: DFKI (2011)](image)

Industry 4.0 focuses on the establishment of intelligent products and production processes (Brettel et al., 2014). It makes use of three technological innovations – automation, the Internet of Things and artificial intelligence – to create ground-breaking industrial and economic models (Blachet & Rinn, 2016, 2016). McKinsey Digital (2015) defines Industry 4.0 as “digitization of the manufacturing sector, with embedded sensors in virtually all product components and manufacturing equipment, ubiquitous cyber-physical systems, and analysis of all relevant data”. This focus on analyzing these data is important as it is the means to get to cognitive

---

14 Big Data: Huge quantities of information are generated by systems and subsystems and it is stored and analyzed in the Cyber-Physical Systems (Wang et al., 2016).
manufacturing, which is key in productivity improvements in quality, efficiency, and reliability of the manufacturing environment (Zhang, 2017). According to Kagermann et al. (2013), the main features of Industry 4.0 include horizontal integration\(^{15}\) through value networks to facilitate inter-corporation collaboration, vertical integration\(^{16}\) of hierarchical subsystems inside a factory to create flexible and reconfigurable manufacturing system, and end-to-end engineering integration\(^{17}\) across the entire value chain to support product customization (figure 3). These features, in particular horizontal integration, include a degree of interconnectedness of firms. The ultimate goal is that virtually every aspect of business will be transformed through the vertical integration of research and development, manufacturing, marketing and sales, and other internal operations, and new business models based on these advances. End result, full evolution towards a complete digital ecosystem (Misthal et al., 2016).

**Figure 3. End-to-end engineering across the entire value chain.**  
**Source:** Final report of the Industrie 4.0 Working Group (2013)

In near future production processes, factories must cope with the need of rapid product development, flexible production as well as complex environments (Vyatkin et al., 2007). One important objective will be to enable the communication between humans, machines and products alike. In the smart production environment, intelligent and customized products

---

\(^{15}\) One corporation should both compete and cooperate with many other related corporations. By the inter-corporation horizontal integration, related corporations can form an efficient ecosystem. Information, finance, and material can flow fluently among these corporations. Therefore, new value networks, as well as business models, may emerge (Wang et al., 2016).

\(^{16}\) Vertical integration refers to the integration of the various IT systems, such as enterprise resource planning (ERP), at the different hierarchical levels (e.g. the actuator and sensor, control, production management, manufacturing and execution and corporate planning levels) in order to deliver an end-to-end solution (Kagermann et al., 2013). By this integration, the smart machines form a self-organized system that can be dynamically reconfigured to adapt to different product types; and the massive information is collected and processed to make the production process transparent (Wang et al., 2016).

\(^{17}\) In a product-centric value creation process, a chain of activities is involved. By integration, a continuous and consistent product model can be reused by every stage. The effect of product design on production and service can be foreseen using a powerful software toolchain so that the customized products are enabled (Wang et al., 2016).
include knowledge\textsuperscript{18} of their manufacturing process and consumer application, and independently manage themselves through the supply-chain (Kagermann et al., 2013).

**Why Industry 4.0**

Kagermann (2015) states that digitization — the continuing convergence of the real and the virtual worlds - will be the main driver of innovation and change in all sectors of the economy. Developing new innovations has always been seen as an important driver of economic growth (Schumpeter, 1934). For instance, for Germany, a successful transition to Industry 4.0 will contribute over 25\% of the GDP and provides over 7 million jobs (Brettel et al., 2014). But industry players are mainly investing significant resources in Industry 4.0 because traditional productivity levers have been widely exhausted, as the innovation agenda is more and more about sustainability\textsuperscript{19} (Tidd et al., 2005), and the European industry has been de-industrializing due to the movement of labor-intensive work to countries with lower labor costs and global supply chains with suppliers outside the EU (Davies, 2015).

The international price competition, the fast changing demand of customers and the fast commoditization of products are also seen as drivers of the revolution. These require industries to adapt to flexible, in-time and inexpensive manufacturing processes through modularly designed machines to achieve the required production paradox: standardized adaptation (Smit, et al., 2016). Besides that, the new role of servitization is going to distort the current industry and business models. In this trend services become the main revenue driver instead of the traditional production process (Smit et al., 2016; Vargo & Lusch, 2008).

At last, the development of exponential technologies such as sensor technology, Industrial-Internet-of-Things, artificial intelligence, robots and cyber physical systems enables individualized solutions, flexibility and cost savings in industrial processes (Schlaepfer & Koch, 2015), and makes it possible to switch from mass production to mass customization\textsuperscript{20} (Blachet & Rinn, 2016). Such technologies are key in changes towards a future industry, an

\textsuperscript{18} Tacit knowledge becomes explicit knowledge.

\textsuperscript{19} Think of aspects such as global climate warming and environmental pollution. Wang et al. (2016) state that the consumption of non-renewable resources such as petroleum and coal increases and the industry suffers an ever-shrinking workforce supply because of population aging, complementing the issue. Therefore, industrial processes need to achieve high flexibility and efficiency as well as low energy consumption and cost (Wang et al., 2016).

\textsuperscript{20} The main idea is that firms manufacture ‘on demand’ and no longer create inventory. It will dynamically adapt itself to demand, will be more predictive and auto-corrective and will involve less trial and error (Blachet & Rinn, 2016).
industry that can withstand the changing economic playfield, deal with the changing market demands, and address social challenges (Smart Industry Workgroup, 2014). In Germany for instance, the Internet of Things, Data and Services plays a vital role in mastering the energy transformation, in developing a sustainable mobility and logistics sector, in providing enhanced health care and in securing a competitive position for the leading manufacturing industry (Kagermann, 2015).

By implementing Industry 4.0 economic, environmental and societal impacts on the manufacturing industry are to be expected. It aims for cost and risk reductions, performance improvements and flexibility (Leonard, 2015; Sommer, 2015), increased productivity (Chung, 2015; Schuh et al., 2014), virtualization of the process and supply-chain, mass customization (Brettel et al., 2014), individualization of demand or batch size one (Lasi et al., 2014), creating resilient industries (Kagermann, 2015; Wang et al., 2016), etc. From a social point of view, individual employees will benefit from Industry 4.0. They will manage their own working hours, being the center of the working environment, conceptualizing and designing new products and complex systems, determining their parameters, rules and requirements inherent to this type of complexity. The role of the human being as generator of creativity, planning and decision-maker will continue to exist. The most important task for employees is to develop skills\textsuperscript{21} that fit the new needs of Industry 4.0 (Brynjolfsson & McAfee, 2012; Kagermann, 2015).

Aspects of Industry 4.0

As was pointed out, Industry 4.0 could be defined as merging or converging the real and virtual world (Schlaepfer and Koch, 2015). Hermann et al. (2015) state that there are four enablers or concepts of Industry 4.0. These concepts are Internet of Things (IoT), Internet of Services (IoS), Cyber-Physical Systems (CPS), and Smart Factory. They also point on the main outcome, which is Interoperability\textsuperscript{22}, and therefore interconnectedness.

\textsuperscript{21} Besides that Industry 4.0 demands an enormous amount of financial resources (Russmann et al., 2015), it also demands a new and well-educated labor force which companies may not have employed yet. Davies (2015) estimates a shortage of almost a million ICT professionals in Europe by the end of 2020.
\textsuperscript{22} Allows the collaboration between different organizations (Mallek et al., 2012; Loos et al., 2011).
The term 'Internet of Things' or 'Industrial Internet of Things' reflects the growing number of smart and connected objects (think of products or machines) and emphasizes the new possibilities they can represent (Porter & Heppelmann, 2014). Within Industry 4.0 IoT technology provides each product with a unique identifier and makes its data available in real time through the web, and the IoT offers product traceability throughout the entire product lifecycle (Whitmore et al., 2015), and enables flexibility and operational efficiencies, reshaping the supply chain and manufacturing process (Chung, 2015), which could contribute for safety in dangerous environments, reduction of production losses and energy consumption with an efficient management, allowing new type of processes. These will create sustainability at all levels (Vermesan & Friess, 2013).

**IoS**

Internet of Services enables “service vendors to offer their services via the internet” (Buxmann et al., 2009, p. 341). The concept consists of participants, an infrastructure for services, business models and the services themselves. “Services are offered and combined into value-added services by various suppliers; they are communicated to users as well as consumers and are accessed by them via various channels.” (Buxmann et al., 2009, p. 341).

From a customers’ point of view, the shift to the servitization of the manufacturing industry is creating more value for them as the product can be monitored increasing the customer satisfaction offered by better customer service (Lightfoot et al., 2012). Manufacturers benefit from this change as well. By tracing the entire life cycle of the product, the probabilities of product malfunctioning are decreased and the source of the problem can be tracked down accurately to the starting point (Kang et al., 2016; Lightfoot et al., 2012). The servitization increases visibility of product performance and new trends (Lightfoot et al., 2012), and down time at the locations of production can be extremely reduced as the machine itself will be able to communicate when it needs maintenance in order to avoid a breakdown (Hermann et al., 2015).

**CPS**

Cyber-Physical Systems are engineered systems, built from and depend upon the seamless integration of software and physical components. It is characterized by a network of interacting elements with physical input and output resembling the structure of a sensor network (Chang...
et al., 2015). In Industry 4.0 CPS and humans are connected over the IoT and IoS (Hermann et al., 2015). These connected systems can interact with one another, analyse data to predict failure, configure themselves, and adapt to changes (Russman et al., 2015). Cyber-Physical Production Systems consist of smart machines, warehousing systems and production facilities that are digitally developed and benefit from end-to-end ICT-based integration, including everything from incoming logistics to production, marketing, outbound logistics and service (Kagermann, 2015). In their relationship, the IoT is seen as a network in which CPS cooperate with each other through unique addressing schemas (Hermann et al., 2015).

**Smart Factory**

The Smart Factory\(^{23}\) is the keystone of Industry 4.0 (Fornster & Dümmler, 2014) as it provides a common ground for humans, machines\(^{24}\), and resources\(^{25}\) to communicate with each other, increasing the interoperability of processes enabling to change or adapt processes dynamics (Loos et al., 2011). This changes the game of manufacturing completely: products are uniquely identifiable, may be tracked at all times and know their own history, current status and alternative routes to achieve their target state (Kagermann, 2015). In tomorrow’s smart factories, manufacturing structures will not be fixed and predefined (Kagermann et al., 2013, p.32). Within this smart factory, products can communicate with their environment and influence the arrangement of Reconfigurable Manufacturing Systems (RMS) (Brettel et al., 2014), and eventually become autonomous. Different is that concrete structures and specifications of production processes are now becoming configuration rules, from which case-specific topologies can be derived automatically (Kagermann et al., 2013). RMS make it possible for manufacturing companies to adapt to changing production requirements in a cost-efficient way. Machine components can now be added, removed or rearranged more easily, depending on their mechanical module interface (Brettel et al., 2014; Abele et al., 2007). One could think of 3D printing for instance.

---

\(^{23}\) Smart factories are vertically linked to the operational processes of individual factories and companies while being horizontally linked to value networks that stretch across the entire globe, incorporating everything from ordering to delivery (Kagermann, 2015).

\(^{24}\) Autonomous, distributed machines, robots, transport and warehousing systems that control and configure themselves in accordance with the needs of the current situation negotiate with each other to establish who has spare capacity at any given moment (Kagermann, 2015).

\(^{25}\) Smart products actively support the manufacturing process: the sheet of metal tells the machine how it should be processed (Kagermann, 2015).
3.4 Innovation processes

Innovating is about dealing with extending and rapidly advancing scientific frontiers, fragmenting markets all over the globe, political uncertainties, regulatory instabilities – and a set of competitors who are increasingly coming from unexpected directions (Tidd et al., 2005). Tidd et al. (2005) argue that a possible response could be “one of spreading the net wide and trying to pick up and make use of a wide set of knowledge signals – in other words, learning to manage innovation at the network level” – going towards a more open approach of innovation. This approach could be understood as a form of organizational innovation.

*Increasing interconnectedness – from Closed to Open Innovation*

Open innovation has gained increased attention the last decade both in academics as in business practitioners (Chesbrough & Brunswicker, 2013; Schroll & Mild, 2011; Chiaroni et al., 2011) due its huge potential in firm’s innovation practices. In the past, internal R&D was one of the main strategic assets, valuable, and even a great barrier to entry (Chesbrough, 2003). As a result, large firms with extended R&D capabilities and complementary assets could outperform smaller rivals (Teece, 1986).

This is known as the closed model, wherein companies generated, developed and commercialized its own ideas. It followed the philosophy of control and the approach called for self-reliance. High investments in R&D asked for high protection of intellectual property, ensuring that competitors could not exploit it. However this seems like a never ending way of innovating, a number of factors caused erosion to the underpinnings of this model. One important factor is the rise in number and mobility of knowledge workers, which makes it increasingly difficult for companies to protect their proprietary ideas and expertise (Chesbrough, 2003). This resulted in new thoughts regarding innovation processes, among which collaborating.

*Collaboration*

Interorganizational collaboration is seen as an important addition to the internal innovative activities of firms (Deeds and Rothaermel, 2003; Dodgson, 1993; Hagedoorn, 2002). Firms may choose for collaboration if they want to 1) acquire missing knowledge, 2) complementary resources or finance, 3) to spread risks, 4) to enlarge its social networks, 5) to reduce costs (Hoffman and Schlosser, 2001; Mohr and Spekman, 1994). It also might encourage the transfer of codified and tacit knowledge (Ahuja, 2000; Doz and Hamel, 1997; Eisenhardt and
Schoonhoven, 1996; Lambe and Spekman, 1997). To improve innovative capabilities, firms can try to make use of interorganizational collaborations with a variety of partners, for instance with existing suppliers and customers (Shaw, 1994; Von Hippel, 1988), potential lead users (Quinn, 1985; Von Hippel, Thomke, and Sonnack, 1999), universities and research centers (Gerwin, Kumar, and Pal, 1992; Santoro, 2000), and even potential or existing industry competitors (Doddston, 1993; Hamel, 1991).

Participating in innovation networks can help firms to encounter new ideas and creative combinations – also in mature businesses (Tidd et al., 2005), and can help innovation in providing support for shared learning. In extension, much process innovation is about configuring and adapting what has been developed elsewhere and applying it. Although firms can start this process on their own, an increasing number of firms acknowledge the value of using networks, giving them some extra traction on the learning process (Tidd et al., 2005).

Although, interorganizational collaboration and participating in networks have considerable potential to contribute to the innovation strategies of firms (Faems et al., 2005), not all are successful. This is due to unintended knowledge spillovers (Teece, 2002; Veugelers, 1998), learning races between the partners (Hamel, 1991; Larsson et al., 1998), diverging opinions on intended benefits (Larson, 1992; Lorange and Roos, 1992), and lack of flexibility and adaptability (Doz, 1996; Ring and Van de Ven, 1994). Therefore the resulting interconnectedness has also cons.

**Open Innovation**

Looking at innovation processes and increasing interconnectedness, the model of open innovation, at which firms commercialize external (and internal) ideas by deploying outside (as well as in-house) pathways to the market, is next. Studies by Chesbrough et al. (2006) and Chesbrough and Crowther (2006) differentiate purposive outflows\(^\text{26}\) and inflows\(^\text{27}\) of knowledge, to accelerate internal innovation processes and to better benefit from innovative efforts. In a perfect situation, firms combine both flows in order to create maximum value from their technological capabilities or other competencies (Chesbrough and Crowther, 2006; 2006;

\(^{26}\) Purposive outflows of knowledge, or technology exploitation, implies innovation activities to leverage existing technological capabilities outside the boundaries of the organization.

\(^{27}\) Purposive inflows, which are referred as technology exploration, relates to innovation activities to capture and benefit from external sources of knowledge to enhance current technological developments.
Lichtenthaler, 2008). This means that the boundary between a firm and its surrounding environment that existed before, becomes more porous, enabling innovation to move easily between the two (Chesbrough, 2003). And some dare to say that implementing open innovation is even an inevitable organizational adaptation to changes in the environment (Chesbrough, 2003). More concrete differences between closed- and open innovation models are shown in Appendix B.

Why should a firm adopt an open innovation approach? On one hand, Enkel et al. (2009) state that once the notion of inter-organizational innovation collaboration has entered an industry, every firm that does not join will cope with serious competitive disadvantages. Koschatzky (2001, p.6) discovered that it is even worse, “firms which do not cooperate and which do not exchange knowledge reduce their knowledge base on a long-term basis and lose the ability to enter into exchange relations with other organizations”. Also Vanhaverbeke (2006) admit that companies are increasingly forced to team up with other companies to develop or absorb new technologies, commercialize new products, or simply to stay in touch with the latest technological developments. On the other hand, there are also several benefits of a successful open innovation process, which are not forced, for instance: access to sources of knowledge outside the firm’s boundary, thereby expanding of the firm’s knowledge base, shortened time to market of new products and services, and maximization of intellectual property. Tomlinson (2010) discovered that vertical cooperation has a positive impact on innovative performance, though, it is the strength of such ties and not just their existence that is important.

In this research, the concept of Open Innovation is used as an indicator of a firm’s attractiveness concerning becoming a target of Industrial Espionage. To come to a more detailed approach of Open Innovation, the distinction of van de Vrande et al. (2009) is used. They divide two practices of open innovation, exploitation and exploration. Exploitation refers to activities such as improvement, refinement, efficiency, selection, and implementation. Exploration is best captured by notions like search, variation, experimentation, and discovery (March, 1991, p. 102). Practices of both are shown in the following table (table 2). These are used to capture the construct of open innovation.
Table 2.

*Surveyed open innovation practices. Based on Van de Vrande et al. (2009).*

<table>
<thead>
<tr>
<th>Practice</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technology exploitation</strong></td>
<td></td>
</tr>
<tr>
<td>Venturing</td>
<td>Starting up new organizations drawing on internal knowledge, and possibly also with finance, human capital and other support services from your enterprise.</td>
</tr>
<tr>
<td>Outward IP licensing</td>
<td>Selling or offering licenses or royalty agreements to other organizations to better profit from your intellectual property, such as patents, copyrights or trademarks.</td>
</tr>
<tr>
<td>Employee involvement</td>
<td>Leveraging the knowledge and initiatives of employees who are not involved in R&amp;D, for example by taking up suggestions, exempting them to implement ideas, or creating autonomous teams to realize innovations.</td>
</tr>
<tr>
<td><strong>Technology exploration</strong></td>
<td></td>
</tr>
<tr>
<td>Customer involvement</td>
<td>Directly involving customers in your innovation processes, for example by active market research to check their needs, or by developing products based on customers’ specifications or modifications of products similar like yours.</td>
</tr>
<tr>
<td>External networking</td>
<td>Drawing on or collaborating with external network partners to support innovation processes, for example for external knowledge or human capital.</td>
</tr>
<tr>
<td>External participation</td>
<td>Equity investments in new or established enterprises in order to gain access to their knowledge or to obtain others synergies.</td>
</tr>
<tr>
<td>Outsourcing R&amp;D</td>
<td>Buying R&amp;D services from other organizations, such as universities, public research organizations, commercial engineers or suppliers.</td>
</tr>
<tr>
<td>Inward IP licensing</td>
<td>Buying or using intellectual property, such as patents, copyrights or trademarks, of other organizations to benefit from external knowledge.</td>
</tr>
</tbody>
</table>

But there are risks and barriers looming. A study of Enkel et al. (2009) showed that there are frequent risks such as loss of knowledge, higher coordination costs, loss of control and higher complexity, which hinder firms from profiting of their initiatives, just like with collaboration.
On one hand, too much openness can detrimental impact firms’ long-term innovation success, caused by loss of control and core competences. Laursen and Salter (2006) found a curvilinear relationship between open innovation and performance, suggesting that too much open innovation hurts firm performance. On the other hand, a closed innovation approach does not cope with the increasing demands of shorter innovation cycles and reduced time to market (Enkel et al., 2009). Enkel et al. (2009) differentiate three core processes of open innovation: the outside-in process, the inside-out process, and the coupled process, each of which can be more or less open (Gassmann and Enkel, 2004).

Now Open Innovation is explained, one could assume two things. On one hand, open innovation could be a driver for performance, and therefore a firm using this approach is an attractive target of Industrial Espionage. On the other hand, precisely this openness could make sure that most of the interesting information is already out there, which causes that the firm is less an attractive target of Industrial Espionage. Also, a moderating effect of Open Innovation on the relation between Digitization and Industrial Espionage is expected. The assumption is that both aspects of a firm’s attractiveness, in terms of being vulnerable for espionage, will strengthen each other regarding the probability of becoming a target of Industrial Espionage.

3.5 Towards a conceptual model

In the previous paragraphs, the characteristics of product-, process-, and open innovation were described. The similarity between all described forms is that they influence the attractiveness of a firm concerning the risk of Industrial Espionage. To come to a conceptual model, the assumptions made must be translated in hypotheses. This is done in the section below. Product Innovation, incremental and radical, are expected to have a positive effect on the probability of becoming a target of Industrial Espionage. Also, Digitization of manufacturing processes is expected to have a positive effect on this probability. Open Innovation could have a positive or negative effect. It is interesting to investigate this effect. This research is about confirming these (or one of the conflicting) hypotheses. Another assumption is that there is a moderating effect of Open Innovation on the expected relationship between Digitization of manufacturing processes and the probability of becoming a target of Industrial Espionage (Figure 3). The innovation activities form together a self-named ‘attractiveness’ box.
Hypotheses

After describing the literature on Industrial Espionage and Innovation Management - Product Innovation, Digitization of manufacturing processes (Industry 4.0), and Open Innovation - the following hypothesis are formulated:

1A. *The Incremental Product Innovation of a firm will have a positive effect on the probability of becoming a target of Industrial Espionage.*

1B. *The Radical Product Innovation of a firm will have a positive effect on the probability of becoming a target of Industrial Espionage.*

2. *A higher degree of Digitization of manufacturing processes (Industry 4.0) will have a positive effect on the probability of becoming a target of Industrial Espionage.*

3. *The number of Open Innovation practices of a firm will have an effect on the probability of becoming a target of Industrial Espionage.*

4. *The number of Open Innovation practices will have a moderating effect on the relation between the degree of Digitization of manufacturing processes and the probability of becoming a target of Industrial Espionage.*

3.6 Summary

In this chapter the characteristics of Industry 4.0 are addressed and innovation activities are described. This is done to understand why innovation forms may contain aspects of attractiveness concerning Industrial Espionage. Now both the theory on and relationship
between Industrial Espionage and innovation have been discussed, taking into account what possible impacts these could have, the following chapter is about the methods used to test the formulated hypotheses. Also the operationalization of the concepts and the characteristics of the samples are described, and the choices concerning the methods are explained.
Chapter 4 – Research Methodology

In the previous chapters, the research problem to be investigated and the fitting concepts from literature were introduced. In this chapter the content of and the rationale for choosing the adopted research methodology is addressed. Furthermore, a detailed account of how the research was conducted, including sample, data collection, data analysis, and research ethics is described. The dependent and independent variables are explained, and a part of this chapter is dedicated to the control variables. The research is both quantitative as qualitative.

4.1 Research design/strategy
This research has the purpose to identify causal relationships between the included variables. The research question, the concepts and their underlying relationships are derived from theory, making it deductive research (Vennix, 2006). This resulted in the choice for a mixed methods study, consisting of interviews and a survey. The survey can be used to identify causal relations among variables and is normal practice for testing hypotheses (Hair et al., 2010). The interviews can be used to better understand possible causality and the process by which these relations get enacted in daily practice. An overview of the research design and the used variables is presented in Appendix C.

4.2 Research process/data collection
The data has been gathered in two ways. First, the relationship between the digitization of technological production processes and industrial espionage has been examined through quantitative data from European Manufacturing Survey (EMS), conducted in 2015. Also the relationship between Open Innovation and Industrial Espionage was examined this way. More in-depth information about the concepts of digitization, product innovation, open innovation and industrial espionage have been gathered by means of semi-structured interviews. In particular, the relationships between the concepts are in-depth examined.

Semi-structured interviews
The main purpose of the interviews conducted in this research, is to gain additional and more in-depth information about the relationship between digitization of production processes and risk of industrial espionage in manufacturing firms. In other words, why do firms become attractive targets for industrial espionage in terms of innovativeness and how do managers
experience this. The interview is semi-structured which means that it consists of a combination of predetermined and new questions. The interview script can be found in Appendix D.

The interview is structured by the following main topics: 1) Digitization of manufacturing processes; 2) Open Innovation practices; 3) Product Innovation; 4) Risks of Innovation; and 5) Industrial Espionage. Several manufacturing firms across different sectors in the Netherlands were contacted and their managers were invited to participate in the interview. First, they were contacted by means of an e-mail. The e-mail was about the information of the research, the researcher, anonymity and confidentiality. Each respondent was asked if audiotaping was okay for him/her. By audiotaping the interview the researcher can guarantee that the detailed transcript is a complete representation of the conversation.

The qualitative data used in this research are collected by interviewing employees (active in the departments: strategy, R&D or security, for preferably at least seven years) or owners of manufacturing firms with preferably at least *50* fulltime-equivalent employees. It is preferably that both employees and owners are active for more than 5 years to be sure that they have seen developments in their firms on topics as process innovation, open innovation and industrial espionage. The semi-structured interviews are used to get more in-depth information on these topics and, in particular, the relationships between those. The data is analyzed by means of theory-guided coding. Furthermore, it is important to collect the data from different industries, which is why the researcher tried to contact a balanced palette of respondents. In the end 8 employees/owners were interviewed (table 3).

<table>
<thead>
<tr>
<th>Firms interviewed</th>
<th>Company</th>
<th>Industry</th>
<th>Job description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 TC1 (TransformerC)</td>
<td>Energy</td>
<td>Program manager</td>
<td></td>
</tr>
<tr>
<td>2 PC1 (PlasticC)</td>
<td>Molding</td>
<td>Operations manager</td>
<td></td>
</tr>
<tr>
<td>3 CC1 (ConcreteC)</td>
<td>Construction</td>
<td>Managing director</td>
<td></td>
</tr>
<tr>
<td>4 MC1 (MachineryC)</td>
<td>Machinery</td>
<td>Operational director</td>
<td></td>
</tr>
<tr>
<td>5 LC1 (LoamC)</td>
<td>Pre-stage Food and others</td>
<td>Quality/application administrator</td>
<td></td>
</tr>
<tr>
<td>6 EC1 (ElectricalC)</td>
<td>Electrical equipment</td>
<td>Operational director</td>
<td></td>
</tr>
<tr>
<td>7 MC2 (MachineryC)</td>
<td>Machinery</td>
<td>Managing director</td>
<td></td>
</tr>
<tr>
<td>8 CC2 (ConcreteC)</td>
<td>Construction</td>
<td>Technical manager</td>
<td></td>
</tr>
</tbody>
</table>

28 The weighted relevance of answers is based on theoretical concepts.
European Manufacturing Survey

The quantitative data used in this research originates from a questionnaire (EMS) drafted and executed by, among other participating institutes, the Institute for Management Research of the Radboud University Nijmegen. The aim of the EMS (2015) used in this research is to investigate the efforts of manufacturing firms in modernization of production processes. The survey was sent to approximately 8000 manufacturing firms, and had a net valid response rate of 4.5%. Though indicator size is representative for the population, indicator industry deviates. It has therefore become a control variable. Only the data on Dutch manufacturing firms is used in the analysis. A logistic regression is chosen to conduct an analysis of the quantitative data. As a part of the regression techniques, it is an technique to identify and predict relationships given a dichotomous dependent variable of Industrial Espionage (Field, 2013).

4.3 Operationalization

It is important to make sure that the concepts from the literature become measurable in this stage of the research. The European Manufacturing Survey (EMS) covers a core of indicators on the innovation topics ‘Digitization of manufacturing processes’, ‘Open Innovation’, ‘Product Innovation’ and ‘Industrial Espionage’. For some of the topics it was needed to transform the questions to come to constructs. In the following paragraph the how and why questions of these transformations are addressed. The items/indicators that were used to measure the construct are presented in Appendix E. Both the validity and reliability of the used constructs are discussed later this chapter.

Dependent variable:

The probability of becoming a target of Industrial Espionage

The dependent variable of this thesis is the chance of becoming a target of industrial espionage. The indicator used to capture this variable is transformed in a dichotomous variable to make logistic regression possible, as it was categorical beforehand. The only values the variable can have are ‘0’ and ‘1’, which in this research represent the outcomes ‘target of industrial espionage’ and ‘not a target of industrial espionage’. Both a firm’s own experiences as firms heard of others’ experiences with Industrial Espionage are included. It is important to state that the data is from the questionnaire of 2015 and that it covers the past five years from that point.
Independent variables:

**Digitization of manufacturing processes**

To cover the concept of digitization of manufacturing processes in organization, 13 items were used to measure the construct. These are all applications of digitization and are smart industry practices as were described earlier, based on McKinsey Digital (2015). It is a proxy variable, counting the number of digitization activities, averaging it, to come to a firm-level value. It is based on this bridge assumption.

**Open innovation**

This construct is based on the distinction made by Van de Vrande et al. (2009) between technology- exploitation and exploration, both practices of open innovation. All eight items were used to build this construct. The scaling is based on the distinction user/non-user of the individual practices.

**Product innovation**

This concept is represented by the distinction between ‘no product innovation’, ‘incremental product innovation’, ‘radical product innovation’, and apart from that ‘product program’. This last item needs some explanation as it is about the product portfolio of an organization, were the organization is still offering a product which they already offer for at least 10 years. This last item could have an opposite effect compared with the other two items, as offering a product for that long might result in returning customers, brand loyalty, etcetera. This means that ‘product program’ would have a negative effect on the probability of becoming a target of Industrial Espionage.

**Control variables**

(*Firm size, industry, R&D investment and Suppliertype*)

Several organizational characteristics can influence strategic choices towards innovation practices as digitization and others. These characteristics or in this research control variables are usually variables that the researcher is not particularly interested in, but that are related to the dependent variable. Such control variables are widely used (Chen & Huang, 2009). For instance, previous studies has shown that there is a great deal of difference in the innovation strategies of small and large firms (e.g. Vossen, 1998; Acs and Audretsch,1990). Some even show a positive relationship between firm size and innovation (e.g. Rogers, 2004; Ayyagari et al., 2012). The purpose of controlling for firm size, industry, R&D investment and Suppliertype
is to remove their effects from the equation. In this research it could be that the probability of becoming a target of industrial espionage is different for firms looking at their size, R&D investments or that firms behave differently in innovation in different industries. It is therefore important to make sure that these relations are known to understand the conceptual relations even better. Characteristics of the control variables can be found in the descriptive statistics table 4 in chapter 5. The transformation of R&D investment and Suppliertype asks for extra explanation, which is given in the following section.

**R&D investment**

The control variable ‘R&D investment’ is split up in three categories. This is done to combine ‘yes/no’ outcomes of item 18.1 and 18.2 with the corresponding R&D percentages of item 18.1, without losing information.

**B2C versus B2B (Suppliertype)**

Kumar and Sareen (2012) state that because of a significant amount of information is exchanged between the trading partners over a fairly large period of time in B2B e-commerce, this information flow may be valuable to the present and potential competitors and can be used for industrial espionage. This is in contrast with the exchange of information in B2C e-commerce that is very limited for a short period of time.

Besides that, previous marketing research has found considerable differences between B2B and B2C markets (Edwards, Gut & Mavondo 2007). For instance the difference between end customers and business customers concerning relying on brands as quality signals. A reason for this is that business customers in B2B markets are often experts themselves and can judge product quality without having to rely on a product brand as a signal for product quality (De Vries, et al., 2017). In contrast, it could be that end customers need to be convinced by appearance, with consequences for product innovation considerations. In addition, business customers mostly engage in long-term customer relationships, reducing the need for signaling through brands. In other words, it is expected that there is a difference between B2B firms and B2C firms, concerning a firm’s attractiveness and therefore probability of becoming a target of Industrial Espionage.

This variable is originally categorical. As was mentioned earlier categorical variables cannot be included in the regression analysis. In addition, only the distinction between business-to-
consumer versus business-to-business is of importance in this research. Therefore the answer options of item 1.3: a) manufacturer of finished products for companies, b) supplier of systems / installations or semi-finished products / parts and c) provider of operations; are coded as B2B. By doing this the control variable the dummy ‘dSuppliertype’ was created.

Moderating effect
A moderating effect is a qualitative or quantitative variable that affects the direction and/or strength of the relationship between independent and dependent variable (Baron and Kenny, 1986). This is also called an interaction effect. As was assumed in the research, there is an interaction effect of Open Innovation on the relationship between Digitization and Industrial Espionage expected. Therefore both variables are mean-centered and multiplied by each other.

4.4.1 Data analysis
After collecting the data, a first analysis need to be done. This analysis includes data inspection and preparation, a reliability and validity analysis, and a check of the assumptions regarding to the form of analysis.

4.4.2 Data inspection and preparation
Sample size
After distilling the data, meaning taking only Dutch manufacturing firms out of the EMS data, who filled in the items chosen to represent the concepts, the usable sample is 177 (N=177). Calculating the sample size for a respective logistic regression is more complex than for ordinary linear regressions. There is however, based on the work of Peduzzi et al. (1996), a guideline for a minimum number of cases to include in the research: $N = 10k/p^{29}$.

In this research there are 3 covariates to include in the model and the proportion of positive cases in the population is 0.169 (16,9%). The minimum number of cases required is $N = 10 \times 3 / 0.169 = 177.5$. Therefore the sample size fits the model.

---

29 In this equation $p$ is the smallest of the proportions of negative or positive cases in the population and $k$ is the number of covariates (the number of independent variables).
**Missing data**

After analyzing the data, one could see that only item 7.3 has 5 missing values. Hair et al. (2010) state that missing data over 10% for an individual response should be studied. The idea is that the researcher should determine whether to delete certain responses when they have over 10% missing data in a compromise between sample size and potential problems with missing data. 5 missing values out of a sample of 177 falls within the margin of 10%, giving no reason to stop the analysis.

**Data transformation**

Based on the data analysis it turned out that the control variable ‘firm size’ did not meet the requirements of normality and therefore it was logarithmic transformed into lnSize, correcting the strong right skewed distribution. This was possible because the variable consists of only positive data.

**4.4.3 Reliability and validity**

**Reliability analysis**

Reliability is “...the degree to which the observed variables measures the ‘true’ value and is ‘error free’.” (Hair et al., 2010, p. 8), which means that a repeated data collection should show consistency with the initial data collection. The goal of the reliability analysis in this research was to identify the internal consistency between items related to a particular construct. This analysis was conducted in SPSS for the constructs (variables) Digitization and Open Innovation. The construct Digitization consists of 13 items, with a Cronbach’s Alpha of .662. This value is lower than the advised value of .8 (Field, 2013). The construct Open Innovation consists of 8 items, with a Cronbach’s Alpha of .689. Both values are not close to .8, indicating potential reliability problems. However, looking at both constructs and their reliability deleting of one of the items would not result in an noteworthy improvement of the reliability (Digitization = .659, Open Innovation = .690), so the decision was made to keep all items for both constructs. In addition, some researchers state that a .6 threshold can be used for few item reliability (Cortina, 1993). The SPSS output of the reliability analysis can be found in Appendix F.

---

30 Skewness= 12.731; after transforming: skewness= 1.490
Validity analysis

Validity is “the degree to which a measure accurately represents what is supposed to” (Hair et al., 2010, p. 8). Yin (2003, p. 18) divides three forms of validity that can be considered. These forms are:

*Construct validity* – the extent to which a set of measured variables actually represent a theoretical latent construct (Hair et al., 2010, p. 631). Except for Digitization and Open Innovation, the research variables are all measured by means of a single item (excluding sums of extra features within the item). The EMS survey does already assure that these constructs are accurate on an acceptable level as Digitization is based on McKinsey Digital (2015) and Open Innovation is based on Van de Vrande et al. (2009).

*Internal validity* – the extent to which an observed effect can be attributed to an independent variable and not to other factors. By controlling for the chosen control variables, the researcher tried to minimize systematic error or bias. In other words, effects from other factors are mapped to better understand the main conceptual relations.

*External validity* – the extent to which an observed effect can be generalized to particular populations and situations. One could question the external validity in means of only interviewing 8 respondents in different industries. It is therefore important to point on the fact that this data is used to get a more in-depth understanding on the conceptual. In that sense the quantitative analysis technique is better for generalizing.

The combination of both quantitative as qualitative techniques enhances the validity of the research as a result of triangulation. This means that the same constructs are measured in different ways, with different methods or techniques, enhancing their measurement of the same construct from different perspectives (Hesse-Biber, 2010).

**4.4.4 Assumptions of the (multiple) logistic regression analysis**

Logistic regression does not make many of the key assumptions of linear regression regarding linearity, normality, homoscedasticity, and measurement level. However, as Tabachnick and Fidell (2001, p. 521) note, satisfying these conditions among the independent variables for the whole sample may enhance power. Though, to use logistic regression analysis as a technique to investigate the hypotheses as formulated in chapter three, there are still some assumptions
regarding the data that should not be violated. The assumptions are: linearity of the logit, absence of multicollinearity\(^\text{31}\) and the independence of the dependent variable outcomes\(^\text{32}\) (Hair et al., 2010).

4.5 Research ethics

The principles of research ethics of the American Psychological Association and the instructions mentioned by Babbie (2007) were taken into account during all stages of the research. All respondents are approached by email, phone or via the network of the researcher, participated on a voluntary basis, and were asked to give an hour of their time. The researcher emphasized the importance of the confidentiality of the responses and the privacy of the respondents. All responses are made anonymous to guarantee the privacy and anonymity of the respondents and to encourage to answer honestly. The transcripts of the interviews are consulted with the respective respondents to prevent misunderstanding and misinterpretation of the results. All respondents were asked if they would like to receive the report of the research and, after approval, the contact information of respondents was collected for research purposes in near future. Finally, a research integrity form is signed by the researcher to ensure proper use of work and references, appropriate information provision to all relevant parties, transparency of data processing and representation and confidentiality of storage and use of data (Appendix K).

4.6 Summary

In this chapter the chosen research methods are addressed. A mixed methods study is chosen to investigate and test the formulated hypotheses statistically and more in-depth. It was necessary to operationalize the concepts to make them measurable. Now both the theory and methods have been discussed, the following chapter is about the results. This chapter is divided into two sections, a quantitative and a qualitative analysis, and later on combined to find an answer on the research question.

---

\(^{31}\) A common threshold to use is VIF<10 (Hair et al., 2010, p.201). Based on the analysis the assumption of multicollinearity is not violated (Appendix G).

\(^{32}\) There are no cases of repeated measurements or matched data.
Chapter 5 – Results

To find an answer to the research question quantitative and qualitative research techniques have been conducted. In this chapter the results of these quantitative, a multiple logistic regression analysis, and qualitative methods, semi-structured interviews, are presented. The first part of the chapter is dedicated to the quantitative data and the analysis. The second part of this chapter highlights the results from the conducted and theory-based coded interviews.

5.1 Quantitative analysis

As is explained in the previous chapter, a major limitation of a linear regression is that it requires that the dependent variable to be metrically scaled. In this research this is not the case. The type of model that is used to conduct the analysis is therefore a logistic regression. This choice is based on the fact that the dependent variable is a dichotomous variable, meaning that the appropriate statistical technique for analyzing the data is making use of logistic regression (Hair et al., 2010).

5.1.2 Sample statistics

Before presenting the empirical outcomes for the hypothesized relationships, a short overview of descriptive statistics of the quantitative EMS data are presented in table 4. Information on (inter-)correlations among variables can be found in Appendix H. The sample consists of 177 Dutch manufacturing firms in different industries. The distribution of these firms in the several industries is as follows: Metals and metal products (20,9%), Food, beverages and tobacco (10,2%), Textiles, leather, paper and board (12,4%), Construction, furniture (7,3%), Chemicals (energy and non-energy) (12,4%), Machinery, equipment transport (18,6%) and Electrical and optical equipment (18,1%). The firm sizes have a range of 7790, starting with a minimum of 10 employees and a mean of 104. Only 35,6% of the firms do invest in R&D and 84,2% of the firms are business-to-business focused.
Table 4.
Descriptive Statistics of the EMS (2015)

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Mean</th>
<th>S.D.</th>
<th>Median</th>
<th>Frequency (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial Espionage (dummy)</td>
<td>Industrial Espionage cases</td>
<td>0.1695</td>
<td>.37625</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firm Size</td>
<td>Number of employees in 2014</td>
<td>104.0</td>
<td>591.0</td>
<td>38.00</td>
<td></td>
</tr>
<tr>
<td>FirmSize_(log)</td>
<td>Metals and metal products</td>
<td></td>
<td></td>
<td></td>
<td>20.9</td>
</tr>
<tr>
<td></td>
<td>Food, beverages and tobacco</td>
<td></td>
<td></td>
<td></td>
<td>10.2</td>
</tr>
<tr>
<td>Firm Industry (dummy)</td>
<td>Metals and metal products</td>
<td></td>
<td></td>
<td></td>
<td>12.4</td>
</tr>
<tr>
<td>Catergory</td>
<td>Textiles, leather, paper and board</td>
<td></td>
<td></td>
<td></td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td>Construction, furniture</td>
<td></td>
<td></td>
<td></td>
<td>12.4</td>
</tr>
<tr>
<td></td>
<td>Machinery, equipment transport (reference category)</td>
<td></td>
<td></td>
<td></td>
<td>18.6</td>
</tr>
<tr>
<td></td>
<td>Electrical and optical equipment</td>
<td></td>
<td></td>
<td></td>
<td>18.1</td>
</tr>
<tr>
<td>R&amp;D investment (dummy)</td>
<td>0% R&amp;D Investment (reference category)</td>
<td></td>
<td></td>
<td></td>
<td>64.4</td>
</tr>
<tr>
<td></td>
<td>R&amp;D investment below median</td>
<td></td>
<td></td>
<td></td>
<td>18.1</td>
</tr>
<tr>
<td></td>
<td>R&amp;D investment above median</td>
<td></td>
<td></td>
<td></td>
<td>17.5</td>
</tr>
<tr>
<td>Suppiertype (dummy)</td>
<td>B2B relative to B2C</td>
<td></td>
<td></td>
<td></td>
<td>84.2</td>
</tr>
<tr>
<td>Digitization</td>
<td>Number of practices</td>
<td>3.6158</td>
<td>2.431</td>
<td>3.0000</td>
<td></td>
</tr>
<tr>
<td>Open Innovation</td>
<td>Number of practices</td>
<td>5.4859</td>
<td>1.828</td>
<td>5.0000</td>
<td></td>
</tr>
<tr>
<td>Product Innovation</td>
<td>No product innovation</td>
<td></td>
<td></td>
<td></td>
<td>38.4</td>
</tr>
<tr>
<td></td>
<td>Incremental</td>
<td></td>
<td></td>
<td></td>
<td>35.0</td>
</tr>
<tr>
<td></td>
<td>Radical</td>
<td></td>
<td></td>
<td></td>
<td>26.6</td>
</tr>
<tr>
<td>Product Program</td>
<td>Change in program relative to no change</td>
<td></td>
<td></td>
<td></td>
<td>9.0</td>
</tr>
</tbody>
</table>

Of the firms, the average number of digitization practices is between 3 and 4 (M=3.6158, SD=2.431). The use of Open Innovation practices is higher, with a mean of more than 5 practices (M=5.4859, SD=1.828). Regarding product innovation, 61.6% of the firms innovate on product-level, more incremental than radical. Concerning another aspect of innovation, the product program, a large group of firms still offers products they were offering the last ten years (91%). At last, almost 17% of the firms has dealt with some form of Industrial Espionage past five years.
Analysis of Industrial Espionage

As was mentioned in the introducing chapter, Industrial Espionage is a form of information gathering without obtaining approval by the holder of the information (Crane, 2005). The questionnaire specifically asked firms for their experiences with this phenomenon in terms of suspicious and demonstrable cases. As is presented in table 4, 16.95% of the firms experienced these cases. In line with thus, it could be interesting to know what forms of information are targeted by Industrial Espionage. The questionnaire offered several options of information as target of Industrial Espionage. These are information on products, on production, on customers and/or suppliers, and on the firm’s strategy. 28 of the 177 firms indicated that the targeted information was one or more of these options. The distribution can be found in table 5. Although this information is interesting and could result in direct managerial implications, it is beyond the scope of this research.

<table>
<thead>
<tr>
<th>Table 5.</th>
<th>Descriptive Statistics on targeted information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information on:</td>
<td>Frequency(%)</td>
</tr>
<tr>
<td>Products</td>
<td>43.4</td>
</tr>
<tr>
<td>Production</td>
<td>24.5</td>
</tr>
<tr>
<td>Customers/suppliers</td>
<td>20.8</td>
</tr>
<tr>
<td>Strategy</td>
<td>11.3</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
</tr>
</tbody>
</table>

In addition, the questionnaire offered several options as anti-measures to avert Industrial Espionage. These are anti-measures in terms of IT security measures, training courses for employees and increase of vigilance, physical security measures and security instructions on illegal information dissemination. From the questionnaire it became clear that 146 of the 177 firms indicated that they at least use one of these measures, also meaning that 31 firms did not used any anti-measure. The distribution of the anti-measures can be found in table 6. Again, this is interesting information, which could say something about the usefulness of these anti-measures, could be integrated in the conceptual model, but this is also beyond the scope of the research, as the researcher is in search of aspects that make firms an attractive target.
### Descriptive Statistics on Anti-Measures

<table>
<thead>
<tr>
<th>Anti-measures</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT security measures</td>
<td>53</td>
<td>36.3</td>
</tr>
<tr>
<td>Training courses for employees and increase of vigilance</td>
<td>40</td>
<td>27.4</td>
</tr>
<tr>
<td>Physical security measures</td>
<td>34</td>
<td>23.3</td>
</tr>
<tr>
<td>Security instructions on illegal information dissemination</td>
<td>19</td>
<td>13.0</td>
</tr>
<tr>
<td>Total</td>
<td>146</td>
<td>100</td>
</tr>
</tbody>
</table>

#### 5.2.1 The model
Logistic regression is used to study the relationship between the probability $p$ of the dependent variable $Y$ to take a certain value and the independent variable $X$. In the research design this means that the probability that a firm becomes a target of Industrial Espionage is influenced by the independent variables ‘Digitization’, ‘Open Innovation’ and ‘Product Innovation’. Also the moderating effect of Open Innovation on the relation between Digitization and Industrial Espionage is analyzed.

#### 5.2.2 Logistic regression
The first logistic regression that was conducted consisted of the dependent variable, independent variables and control variables, using a five steps enter-method. It turned out that the final model was not significantly better than the base model (chi-square= 21.391, df=16, $p>.05$). A quick look at the control variables indicated the reason. All control variables, excluding Suppliertype, were not significant and caused ‘noise’ in the model. That is why there was chosen to conduct the logistic regression again, but now without the non-significant control variables.

This logistic regression is conducted in a three steps enter-method. Model 0 shows only the dichotomized dependent variable. Model 1 includes the effects of the control variable Suppliertype and the independent variables. At last, model 2 contains all previously mentioned variables and the interaction term of Digitization and Open Innovation. This model shows the results of the full model containing the main effects and interaction effect of the control variable and independent variables. All steps can be found in table 7.
To check whether the new model (including more variables) is an improvement over the baseline model, chi-square tests can be used to see if there is a significant difference between the Log-likelihoods (specifically the -2LLs) of the baseline model and the new model. If the new model has a significantly reduced -2LL compared to the baseline then it suggests that the new model is explaining more of the variance in the outcome and is an improvement. Here the chi-square is significant (chi-square= 14.111, df=7, p<.05), so the final model is significantly better than the base model.

**Model fit**

In making an assessment of the overall fit of the logistic regression, there are three approaches: statistical measures of overall model fit, pseudo R² measures, and classification accuracy as expressed in the hit ratio (Hair et al., 2010, p. 429). In this research the first approach is used. The Hosmer and Lemeshow measure of overall fit (Hosmer and Lemeshow Chi-square) measures the correspondence of the actual and predicted values of the dependent variable. In this research the best outcome is to find no significant differences. This is the case in all successive steps to come to the final model as is shown in table 7.

<table>
<thead>
<tr>
<th>Table 7.</th>
<th>Model fit evaluation of binary logistic regression analysis (N=177).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exp. (B)</td>
</tr>
<tr>
<td>Model 0:</td>
<td>DV</td>
</tr>
<tr>
<td>Model 1:</td>
<td>DV+IVs+CV</td>
</tr>
<tr>
<td>Model 2:</td>
<td>DV+IVs+CV+ Interaction term</td>
</tr>
</tbody>
</table>

The presented R² values tell approximately how much variation in the outcome is explained by the model. In particular the step from model 0 to model 1 make the values increase. In the final model Nagelkerke’s R², which is a modification of Cox & Snell R², suggests that the model explains roughly 13% of the variation in the outcome. A value of 1.0 would indicate perfect model fit. Remarkable is that the interaction term of Digitization and Open Innovation is not adding anything in terms of an increase in pseudo R².
Statistical significance of the coefficients

For the logistic regression a statistical significance level of .05 was employed and the exponentiated coefficients are reported instead of the logistic coefficients. The advantage of reporting the odds ratios instead of the coefficients is because the exponentiated coefficients directly reflect the magnitude of change in the odds value instead of log of the odds (Hair et al., 2010). As the hypotheses were consciously formulated in the way they are, this results in one-tailed regression. In other words, the predicted relations are only tested in one direction of interest.

The expectation prior to the logistic regression analysis was that all independent variables would increase the probability of becoming a target of Industrial Espionage, except for Open Innovation from which the direction was uncertain. The researcher controlled for some variables to make sure that the effects to be found are solely from the independent variables. After concluding that non-significant control variables were causing ‘noise’, these were left out of the original model, as is explained earlier. The results are shown below (table 8) and summarized in table 9.

5.2.3 Hypotheses

The influence of Product Innovation was conceptualized. Product Innovation could have a positive effect on the probability of becoming a target of Industrial Espionage. This concept was split into incremental and radical Product Innovation, resulting in the following hypotheses:

H1A: The Incremental Product Innovation activities of a firm will have a positive effect on the probability of becoming a target of Industrial Espionage.

H1B: The Radical Product Innovation activities of a firm will have a positive effect on the probability of becoming a target of Industrial Espionage.

The results of the logistic regression (table 8) show that Incremental Product Innovation does have a significant positive effect on the probability of becoming a target of Industrial Espionage. The logistic exponentiated coefficients of Incremental Product Innovation (OR=3.194, p=.056) gives support for hypothesis 1A, meaning that the probability that a firm becomes a target of Industrial Espionage is more than three times higher if it is innovating its product(s) incrementally.
Looking at the results of the logistic regression (table 8), they show that Radical Product Innovation does have a significant positive effect on the probability of becoming a target of Industrial Espionage. The logistic exponentiated coefficients of Radical Product Innovation (OR=3.962, p=.024) gives support for hypothesis 1B, meaning that the probability that a firm becomes a target of Industrial Espionage is almost four times higher if it is innovating its product(s) radically. In other words, if a firm innovates its products radically the probability of becoming a target of industrial espionage almost quadruples.

As was conceptualized, the more a firm digitize its manufacturing processes, the more attractive it becomes concerning being a target of Industrial Espionage. This assumption is operationalized in the hypothesis:

\[
\text{H2: } \text{A higher degree of Digitization of manufacturing processes (Industry 4.0) will have a positive effect on the probability of becoming a target of Industrial Espionage.}
\]

Looking at the results of the logistic regression (table 8), they show that the construct Digitization does have a significant positive effect on the probability of becoming a target of Industrial Espionage. The logistic exponentiated coefficients of Digitization (OR=1.192, p=.068) gives support for hypothesis 2, meaning that the probability that a firm becomes a target of Industrial Espionage is 19.2% higher if it is digitizing its manufacturing processes.

The influence of the construct of Open Innovation on the probability of becoming a target of Industrial Espionage was also conceptualized. The number of Open Innovation practices could make a firm more or less attractive. This assumption is operationalized in the hypotheses:

\[
\text{H3: The number of Open Innovation practices of a firm will have an effect on the probability of becoming a target of Industrial Espionage.}
\]

Looking at the results of the logistic regression (table 8), they show that the construct Open Innovation does not have a significant positive or negative effect on the probability of becoming a target of Industrial Espionage. The logistic exponentiated coefficients of Open Innovation (OR=1.062, p=.654) gives no support for hypothesis 3, meaning that it not significantly influences the probability that a firm becomes a target of Industrial Espionage. This results in rejection of the hypothesis.
### Table 8. Results of binary logistic regression analysis

<table>
<thead>
<tr>
<th>Variables</th>
<th>Model 0</th>
<th>Model 1</th>
<th>Model 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exp(B)/OR</td>
<td>S.E.</td>
<td>Exp(B)/OR</td>
</tr>
<tr>
<td><strong>Dependent Variable</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability of becoming a target of Industrial Espionage</td>
<td><strong>.204</strong>*</td>
<td>.200</td>
<td></td>
</tr>
<tr>
<td><strong>Control Variables</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dSuppliertype</td>
<td>.430</td>
<td>.532</td>
<td>.430</td>
</tr>
<tr>
<td><strong>Independent Variables</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitization</td>
<td>1.195*</td>
<td>.094</td>
<td>1.192*</td>
</tr>
<tr>
<td>IncProduct Innovation</td>
<td>3.192*</td>
<td>.607</td>
<td>3.194*</td>
</tr>
<tr>
<td>RadProduct Innovation</td>
<td>3.946*</td>
<td>.608</td>
<td>3.962*</td>
</tr>
<tr>
<td>Product Program</td>
<td>.895</td>
<td>.870</td>
<td>.889</td>
</tr>
<tr>
<td>Number of Open Innovation practices</td>
<td>1.058</td>
<td>.128</td>
<td>.654</td>
</tr>
<tr>
<td><strong>Interaction</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I_DigitizationOpenInnovation</td>
<td>.995</td>
<td>.046</td>
<td></td>
</tr>
</tbody>
</table>

*** p<.001, **p<.01, *p<.05

At last, the influence of the interaction term between Digitization and Open Innovation was conceptualized. Open Innovation could have a moderating effect on the relation between Digitization and the probability of becoming a target of Industrial Espionage. This resulted in the following hypothesis:

**H4:** The number of Open Innovation practices will have a moderating effect on the relation between the degree of Digitization of manufacturing processes and the probability of becoming a target of Industrial Espionage.

The results of the logistic regression (table 8) show that the interaction term Digitization - Open Innovation does not have a significant positive or negative effect on the probability of becoming a target of Industrial Espionage. The logistic exponentiated coefficients of the interaction term (OR=.995, p=.916) gives no support for hypothesis 4, meaning that it not significantly influences the probability that a firm becomes a target of Industrial Espionage. This results in a rejection of this hypothesis.

In addition, the control variable dSuppliertype, which was significant in the first model has no significant influence on the probability of becoming a target of Industrial Espionage anymore. Also the variable Productprogram was not found significant, meaning it has no significant
influence on the dependent variable. In other words, a) the difference between Business-to-business and Business-to-consumers, and b) the fact that a firm offers the same products during the past ten years, have no significant influence on the probability to become a target of Industrial Espionage.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1A</td>
<td>The Incremental Product Innovation of a firm will have a positive effect on the probability of becoming a target of Industrial Espionage.</td>
</tr>
<tr>
<td>1B</td>
<td>The Radical Product Innovation of a firm will have a positive effect on the probability of becoming a target of Industrial Espionage.</td>
</tr>
<tr>
<td>2</td>
<td>A higher degree of Digitization of manufacturing processes (Industry 4.0) will have a positive effect on the probability of becoming a target of Industrial Espionage.</td>
</tr>
<tr>
<td>3</td>
<td>The number of Open Innovation practices of a firm will have an effect on the probability of becoming a target of industrial espionage.</td>
</tr>
<tr>
<td>4</td>
<td>The number of Open Innovation practices will have a moderating effect on the relation between the degree of Digitization of manufacturing processes and the probability of becoming a target of Industrial Espionage.</td>
</tr>
</tbody>
</table>

**5.2.4 Summary**

Based on quantitative analysis, the formulated hypotheses were tested. The construct of Digitization turned out to have a significant influence on the dependent variable, just like both forms of Product Innovation. The construct of Open Innovation turned out to be not significant, meaning that it does not affect the probability of becoming a target of Industrial Espionage. While the quantitative method gave insights about the existence, strength, and the direction of the relationships, the following section provides insights about the contents of the relations. In this qualitative analysis, quotes of eight different respondents are analyzed.
5.3.1 Qualitative analysis

To get insights on if, how and why strategic decisions are made regarding to the probability of becoming a target of Industrial Espionage, eight semi-structured interviews were conducted at firms meeting the same criteria as the EMS participants, Dutch manufacturing SMEs. The conversations were audio-taped and completely transcribed in order to make it possible to agree on the content and to facilitate the analysis. Using a theory-based coding approach the most relevant quotes on the concepts were selected and ascended. For each concept and their inter-concept relationships, the quotes were ranked on a point-point scale from (1) most relevant to (4) least relevant. The findings will be presented and discussed in the remaining of this chapter.

First, the results of the main concepts – Product Innovation, Digitization of manufacturing processes, Open Innovation, and Industrial Espionage are addressed. The second part of this section consists of an elaboration on the inter-concept relations. At last, this section is closed with a summary of the findings of the qualitative analysis, followed by concluding words on both analyses concerning the conceptual model.

5.3.2 Main concepts

To make the coding technique less biased, several subjects were introduced to serve as categories. These categories are for instance content, purpose, perspective and example. This distinction is necessary to structure the large amount of quotes. All subjects can be found in Appendix I.

Product Innovation

Dewar & Dutton (1986) define innovation “as an idea, practice, or material artifact perceived to be new by the relevant unit of adoption.” As was mentioned Dewar & Dutton (1986) divided two forms later on: radical and incremental innovations. Whereas product innovation in the quantitative section was based on the distinction between incremental and radical product innovation, complemented by the product program, the qualitative section is based on quotes that are most relevant in terms of considerations with regard to product innovation as a more broad strategy of a firm.

Looking at the firms, most of them are not focusing on product innovation to launch new products (fast). One respondent explains that “when you quickly launch something completely new it often comes at an expense, in this case our core values: reliability and dependability”.


Therefore they “have never been the most innovative in launching completely new products on the market (MC2)” (Appendix J).

The firms try to optimize their existing products (MC2), transform existing products to make them fit in other markets (MC1) (table 10), or only produce new products based on customer request, “a dedicated product for a dedicated customer, developed together (PC1)” (Appendix J). It is also that firms offer products in differing shape due to changing requirements and circumstances, “we just deliver a dry product, fully ready-made, completely prefab (CC2)”, and “one could see a development in the increase in the use of organic fertilizers, making more use of natural defense systems, and make less use of artificial fertilizers (LC1)” on retailer’s request (Appendix J). Some firms add value by assembling components, in those cases the product innovation is in the components (EC1) (table 10). Though, some firms do launch new products. These products are quite similar to the other products they already offer, and therefore incremental. As an example: “From now on we will enter the market with a new product that they do not yet know in the Netherlands, and that is that you can put elevator shafts and stairwells at once as a ready-made concrete tube (CC1) (Appendix J)” and “we have just started the production of a new floor, for a pilot project of two hundred homes (CC2)” (table 10).

<table>
<thead>
<tr>
<th>Quotes on product innovation as key-asset</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CC1</strong></td>
</tr>
<tr>
<td><strong>CC2</strong></td>
</tr>
<tr>
<td><strong>EC1</strong></td>
</tr>
<tr>
<td><strong>MC1</strong></td>
</tr>
<tr>
<td><strong>MC2</strong></td>
</tr>
<tr>
<td><strong>PC1</strong></td>
</tr>
</tbody>
</table>
The firms seem future oriented. One respondent mentioned that they “have been a bit early with the launch of certain products (MC1)” referring to the intelligent drives they are offering already. Another respondent was also future oriented but in a different way as “the product will become superfluous once, your innovation must be focused on what will be the solution after the product we offer and what our role will be in those developments (TC1)”. Though one firm is also awaiting, as it is not responding panicky to the fact that “you already can buy expensive and unreliable large electric forklift trucks” explaining that “it must be profitable for the customer first (MC2)” (Appendix J).

Remarkable is a quote of one respondent on product innovation, that there is a trend, “contrary to innovation”, replacing products with similar ones, with the advantage “that you do not have to comply to all new legislation (TC1)”, meaning that renovating dominates innovating in some cases. Also interesting is the quote that “in times that things are going well, they are only playing one game, just earning money, innovation ... is of later concern. The necessity is not there at the time (CC1)” (Appendix J). One could wonder whether lean times are better moments to innovate...

**Digitization**

According to McKinsey Digital (2015), Industry 4.0 can be defined as “digitization of the manufacturing sector, with embedded sensors in virtually all product components and manufacturing equipment, ubiquitous cyber-physical systems, and analysis of all relevant data”. This focus on analyzing these data is important as it is the means to get to cognitive manufacturing which is key in productivity improvements in quality, efficiency, and reliability of the manufacturing environment (Zhang, 2017). Whereas the degree of digitization in the quantitative section was based on the number of practices, the qualitative section is based on quotes that are most close to the definition of McKinsey Digital (2015) or in terms of productivity improvements in quality, efficiency, and reliability of the manufacturing environment.

Remarkable is that not one of the firms totally fitted the definition. As one of the respondents rightfully said: “I cannot buy a package of smart industry. You have to develop, do, sort out a

---

33 Big Data: Huge quantities of information are generated by systems and subsystems and it is stored and analyzed in the Cyber-Physical Systems (Wang et al., 2016).
lot yourself, there is no ready-made solution (PC1).” It is therefore a process to eventually fit the phenomenon of industry 4.0. Many firms are developing in the right way though, as they are using for example ERP-systems. One of the respondents even called it “a must”, certainly “if a company grows to a certain size, you cannot organize it efficiently enough in any other way (EC1)” and another said “without such an ERP-package you cannot produce anymore (PC1)” (Appendix J). According to the interviews quality (CC2), efficiency (PC1, MC2, LC1, CC1, EC1) and reliability (CC2) are the main reasons for implementing industry 4.0 and other digitization practices (table 11), as “it is an essential part of the reason for our existence (PC1)”, and even without adapting being “gone in the future (MC2)”. All respondents of the represented industries feel some kind of need to go along with the trend, with all different practices. One respondent mentioned that digitization “is changing the market, as everything is becoming a service... you are literally connected to your customer (MC2).”

### Table 11.

**Quotes on the purpose of Digitization**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>Op het moment dat de klant tevreden is, dan vindt er een nagenoeg vol geautomatiseerde engineering plaats. Dat wil zeggen dat wij online software beschikbaar hebben, die op basis van het model van de klant, de tekeningen automatisch genereerd op het grootste detail/productieniveau, berekeningen van producten op sterkte, dat dan automatisch wapeningstekeningen worden gegenereerd, en dat al die productiestukken binnen 24-uur weer terug zijn bij de klant. Dat proces duurt nu gemiddeld 4-6 weken. Dan gaat de opdracht de fabriek in, en daar staat een semi-robot-gestuurde productiestraat, waar digitale 3D-vormen ingaan en waarbij het eindproduct binnen vijf werkdagen van de band rolt. Nu duurt het hele traject tussen de 12 en 20 weken, afhankelijk van complexiteit, grootte en volume, en ik denk dat we straks terug kunnen naar twee weken.</td>
<td></td>
</tr>
<tr>
<td>CC2</td>
<td>Kwaliteit staat hoog, dat willen we ook, niet alleen esthetisch maar ook functionele kwaliteit, en dat kan eigenlijk alleen maar met een geautomatiseerde omgeving. Zodoende maken wij gebruik van robots. Onze digitalisering, in ons geautomatiseerd proces, helpt bij grote leverbetrouwbaarheid, omdat we kunnen monitoren, we kunnen sturen, versnellen, eventueel vertragen waar nodig.</td>
<td></td>
</tr>
<tr>
<td>EC1</td>
<td>Qua digitalisering, niet dat we de strategie daar volledig op geënt hebben, maar we zijn wel dit jaar begonnen met het nieuwe systeem om ons hele bedrijf en de bedrijfsvoering in een systeem te hebben staan, waardoor je beter kunt monitoren. Je krijgt je financiële gegevens er makkelijker uit maar ook hoe staat het met productieprocessen, met voorraad, daar willen we meer in gaan automatiseren, dat het systeem ook voorraad-waarschuwingen gaat geven.</td>
<td></td>
</tr>
<tr>
<td>LC1</td>
<td>Uiteindelijk doe je alles vanuit de druk van de markt, je wilt efficiënter gaan werken. Wij moesten twee nieuwe fabrieken bouwen want we gingen verhuizen, we moesten weg op de locatie waar we zaten, dat was de belangrijkste drijfveer, maar om het goed en efficiënt te doen was het nodig om het zo in te richten dat het gekoppeld was aan het ERP-systeem.</td>
<td></td>
</tr>
</tbody>
</table>
An additional aspect to the purpose of making use of the digitization practices is the appearance of these practices and the use of data. A number of respondents that were interviewed mentioned that they in some way use digital tools for their production, for instance “using touchscreens to run 3D models (TC1)”, “drawing digitally, preferably in the model (CC2)” and “using digital-torque-tooling throughout the production process (MC2)”. Not all practices are in all industries of use. For example, one firm had been working on 3D printing of concrete but has stopped, still believing “that there will be a specific market in the future, but that is not a market for the bulk (CC1)” (Appendix J).

The firms have different ways of processing and make use of data. For one firm it is about predicting nearby future service activities (MC2). Another firm mainly use data to trace their products (PC1) and a third firm use data to support their overall marketing strategy (EC1) (table 12).

An additional aspect to the purpose of making use of the digitization practices is the appearance of these practices and the use of data. A number of respondents that were interviewed mentioned that they in some way use digital tools for their production, for instance “using touchscreens to run 3D models (TC1)”, “drawing digitally, preferably in the model (CC2)” and “using digital-torque-tooling throughout the production process (MC2)”. Not all practices are in all industries of use. For example, one firm had been working on 3D printing of concrete but has stopped, still believing “that there will be a specific market in the future, but that is not a market for the bulk (CC1)” (Appendix J).

The firms have different ways of processing and make use of data. For one firm it is about predicting nearby future service activities (MC2). Another firm mainly use data to trace their products (PC1) and a third firm use data to support their overall marketing strategy (EC1) (table 12).

### Table 11

**Quotes on the purpose of Digitization**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MC2</td>
<td>Degene die het meeste data heeft, het meeste weet hoe die dingen worden ingezet, die het efficiëntst zijn service kan inplannen enzovoort, die gaat daar de beste deal neerleggen. Als je dus niet connected bent en al die data hebt, en daar efficiënt mee gaat leren werken, dan ben je in de toekomst weg.</td>
</tr>
<tr>
<td>PC1</td>
<td>De producten die wij maken zijn in hele grote volumes, en die kosten daardoor weinig, maar dat lukt alleen maar door vergaande mate van automatisering en digitalisering. Het is een wezenlijk onderdeel van de reden van ons bestaan. Zonder automatisering en digitalisering zouden we hier geen producten kunnen maken.</td>
</tr>
</tbody>
</table>
Digitization also involves obstacles in terms of transition. According to the interviews these are diverse. Firms mention that it depends on the product type (MC2), the not adequately trained employees due to the changing profile of the manufacturing activities (CC2) and in line with that lagging knowledge (MC1), plus in one situation it is even path dependent, namely, there was a plan to implement a new developed EAP-package but is was stopped by the former director (MC1) (table 13).

<table>
<thead>
<tr>
<th>Table 12</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quotes on the use of data</strong></td>
</tr>
<tr>
<td>bepaalde specificaties erachter. Dat wordt met name in de medische wereld steeds belangrijker, de traceability van producten.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 13.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quotes on obstacles in switching to digitization practices</strong></td>
</tr>
<tr>
<td>CC2</td>
</tr>
<tr>
<td>MC1</td>
</tr>
<tr>
<td>MC1</td>
</tr>
<tr>
<td>MC2</td>
</tr>
</tbody>
</table>
Open Innovation

According to studies by Chesbrough et al. (2006) and Chesbrough and Crowther (2006) a distinction between purposive outflows\(^{34}\) and inflows\(^{35}\) of knowledge can be made to accelerate internal innovation processes and to better benefit from innovative efforts. Whereas open innovation in the quantitative section was based on the number of practices, the qualitative section is based on quotes that are most relevant in terms of considerations with regard to collaborations/partnerships between firms for different purposes.

Looking at the different reasons of collaborating with other (non-competitive) firms (table 14), the main purpose is to make use of others’, “preferably known partners’ (EC1)”, know-how\(^{36}\)/knowledge, because “you cannot invent everything yourself (MC2)”, “nobody has knowledge of all the steps (PC1)” and “two know more than one (MC2)”. This is typical for small to medium sized organizations as large firms with extended R&D capabilities and complementary assets could outperform smaller rivals (Teece, 1986), also quoting a respondent: “being a large organization, you might be able to do it yourself, but as an SME you will have to work together (PC1)”. But it is not only about benefiting from each other’s knowledge. “Good partnerships should express themselves in that they, in the end, cost less (CC1)” or to make sure that “in the end you have more breath to be able to get it feasible (CC2)”. Therefore, it is definitely a financial consideration as well.

<table>
<thead>
<tr>
<th>Table 14. Quotes on the purpose of partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
</tr>
<tr>
<td>CC2</td>
</tr>
</tbody>
</table>

\(^{34}\) Purposive outflows of knowledge, or technology exploitation, implies innovation activities to leverage existing technological capabilities outside the boundaries of the organization (Chesbrough et al., 2006; Chesbrough & Crowther, 2006).

\(^{35}\) Purposive inflows, which are referred as technology exploration, relates to innovation activities to capture and benefit from external sources of knowledge to enhance current technological developments (Chesbrough et al., 2006; Chesbrough & Crowther, 2006).

\(^{36}\) Cognitive knowledge (Quinn et al., 1996).
None of the firms are innovating with direct competitors. There are collaborations between competitors though. These arise from issues concerning lacking back-up possibilities to compensate for unexpected events (MC1), and from avoiding investing in non-growing markets, making use of each other’s production capacity (LC1) (table 15).

More common are collaborations with firms that are not or only partly participating in the same markets. These are between suppliers (CC1, MC2), contractors (CC2), colleges (TC1), universities and the manufacturing firms. Also collaborations with governments are not uncommon, and then it is mainly about transcending topics that are wider than sector specific, such as the use of hydrogen as fuel (MC2) (table 15).

Firms try, preferably, to structurally collaborate with the same parties\(^{37}\), because of the believe that “if both parties structurally put in energy that you can work together more efficiently (CC1)” (table 15), and because “you do not build a relationship without purpose, they know us and we know what we can offer them (EC1)” (Appendix J). In some cases it is fused, as specific

\(^{37}\) Identified relationships.
Markets are characterized as very loyal, “It is a relationship market, you do not sell something for only 1/2/3 years, you are going to do whole development processes together, and then also, it is a very loyal market. You do not just join in, and you do not just lose your customers (MC1)” (Appendix J).

Table 15.
Quotes on forms of collaboration

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>Heb je het over partnerships, ja we gaan partnerships aan met automatiserders, er is een viertal bedrijven dat ons helpt te automatiseren, en partnerships met onze leveranciers. ~ We zijn daar best druk mee, om in ieder geval structureel met dezelfde partijen zaken te doen, ik geloof er ook in dat als beide partijen daar structureel energie instoppen dat je dan steeds efficiënter samen kunt gaan werken.</td>
</tr>
<tr>
<td>CC1</td>
<td>Ik ben 3-4 jaar bezig met een zoektocht naar dat proces. Ik heb op een gegeven moment op een seminar op de TU Eindhoven de zaal gevraagd: dit is mijn uitdaging, wie weet de oplossing? Twee weken daarna belde iemand met de oplossing. Sindsdien ontwikkelen we dit samen, omdat we weten dat het waarschijnlijk de hele industrie gaat veranderen.</td>
</tr>
<tr>
<td>CC2</td>
<td>Samenwerkingsverbanden waarmee we nu mee zitten zijn meerdere aannemers en meerdere installateurs. Onze toeleveranciers proberen we wel zoveel mogelijk hetzelfde te houden, omdat het de basis en het hart is van ons bedrijf is.</td>
</tr>
<tr>
<td>LC1</td>
<td>We hebben wel een uitzonderlijke samenwerking, wij hebben productiecapaciteit over, de machines kunnen veel meer aan dan dat ze eigenlijk doen. Maar andersom ook, we zouden allebei nog wel een fabriek kunnen bouwen, dan zouden we allebei investeren en kosten maken, voor een markt in Nederland met name die eigenlijk niet meer groeit. We hebben capaciteit genoeg, laten we dan voor elkaar gaan maken.</td>
</tr>
<tr>
<td>MC1</td>
<td>We zijn met een concurrent aan het praten, zij hebben dezelfde vraagstukken, als zij back-up voor ons zijn en andersom, kunnen we elkaar zo steunen, dan hoeven we niet die enorme investeringen te doen.</td>
</tr>
<tr>
<td>MC2</td>
<td>We werken veel met toeleveranciers, we hebben nu net een patent aangevraagd samen met een toeleverancier, dan doen we ieder de helft. Die toeleverancier maakt de components maar heeft niet de hele truck, wij hebben de hele truck maar niet de kennis en de volumes in die components, op dat snijvlak kun je samen mooi dingen ontwikkelen en dan moet je daar ook een soort partner-approach in hebben.</td>
</tr>
<tr>
<td>MC2</td>
<td>Daarnaast zijn we bezig met waterstof, daar werken we samen met een zusterbedrijf, maar ook weer met andere partijen. Daarin moeten we ook gaan samenwerken met overheden, semi-overheden, subsidieinstanties, noem maar op.</td>
</tr>
<tr>
<td>TC1</td>
<td>Het wordt nog niet optimaal gebruikt. Het is met name uit de standaardkennis bedrijfjes (hoge scholen) en minder met bedrijven die in dezelfde tak van sport zitten en concurrent zijn.</td>
</tr>
</tbody>
</table>
According to the interviews, specific collaborations in R&D on a structural basis are scarce. One can conclude that R&D collaborations arise from specific issues, in search of a groundbreaking process innovation, “Since then we have been developing this together, because we know that it is likely to change the entire industry (CC1)” (table 15) or to develop “a new method for a better silver-gold alloy, for in our cables (EC1)” (Appendix J). There is a focus in advance.

There are also firms that are only internally focused concerning innovation, ranging from being “not in the genes of this company (MC1)” to being “a company where customers were always standing in line to purchase their products”, resulting in “less need to develop on certain aspects (TC1)” (Appendix J). Nevertheless they are collaborating in other business aspects.

Industrial Espionage
Industrial espionage is a form of information gathering. Espionage could be defined as the access to sensitive information without obtaining approval by the holder of the information (Crane, 2005). Whereas Industrial Espionage was captured as the probability of becoming a target in the quantitative section, the qualitative section is based on quotes that are most relevant in terms of how respondents experience the phenomenon and how they deal with it.

“How bad can it really be (CC1)”? Looking at the findings, there is a varying degree of awareness of the threat among the firms, from “it is seen as a risk (PC1)” to “we have experienced the craziest things, simply opening drawers and photographing the contents... (MC1)”. The results reveal that all respondents acknowledge the threat in one way or another (table 16), resulting in different counter policies (table 17 and 18). One respondent reflected on why espionage is not that great of a threat: “Perhaps we are fortunate that the construction industry is more traditional in that respect, being beneficial for digital developments, as well as espionage (CC2)”. Another respondent stated that “it is a timeless phenomenon (MC2)”, while he shifted his attention to a different approach to the threat, that of being digitally sabotaged as a firm (table 20). Overall, one could say that the threat of Industrial Espionage has not yet become a main topic in strategy.
Table 16.  
Quotes on Industrial Espionage as a threat

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>Ik weeg altijd risico’s af, stel de informatie ligt op straat, hoe erg is dat nou echt?</td>
</tr>
<tr>
<td>CC2</td>
<td>Misschien hebben we het geluk dat de bouw wat dat betreft wat traditioneler is, wat eenduidiger misschien ook wel, qua processen, dertien in een dozijn zeg maar, en misschien is dat voor deze digitale ontwikkeling, alsmede spionage een gunstige uitwerking.</td>
</tr>
<tr>
<td>LC1</td>
<td>Met betrekking tot de automatisering in de fabriek, we laten maar beperkt mensen toe, maar wat blijkt, als iemand een onderdeel denkt te weten, dan lukt het vaak alsnog niet om het bij hunzelf te implementeren, dan missen ze in de productieketen andere onderdelen, en dan lukt het niet.</td>
</tr>
<tr>
<td>MC1</td>
<td>We hebben daarmee de gekste dingen meegemaakt. Die trekken gewoon laden open en fotograferen de inhoud van de laden.</td>
</tr>
<tr>
<td>MC2</td>
<td>We hebben ook een tijd gehad dat iemand tien Chinese stagiaires in dienst had, en die hadden de hele harde schijf leeggeplukt van de onderneming, dat is van alle tijden.</td>
</tr>
<tr>
<td>PC1</td>
<td>We hebben afgelopen jaren geen aanleiding om te denken dat er dingen oneerbaars zijn gebeurd of het stelen van gegevens, of dat gegevens op de verkeerde manier zijn gebruikt. Maar het wordt wel gezien als een risico.</td>
</tr>
<tr>
<td>TC1</td>
<td>Met betrekking tot bepaalde middelen ben je soms een beetje op elkaar aangewezen. We testen nu een product van een concurrent omdat zij niet de capaciteit hebben. Theoretisch kun je dan alles spioneren wat je wilt…</td>
</tr>
</tbody>
</table>

As firms acknowledge the threat of Industrial Espionage, they execute counter measures. During the interviews the researcher divided two forms of espionage, namely, physical and cyber. This distinction is also used in characterizing the counter measures.

The results reveal that an important ‘soft’ counter measure regarding industrial espionage is keeping your (scarce) employees pleased: “preventing them from doing harmful things due to dissatisfaction (PC1)” (table 17) and “making them participate (CC1)” (Appendix J), responding to the insider threat. In addition, respondents mentioned the use of the ‘harder’ measure of non-competition- and confidentiality agreements (CC1, CC2, MC1). Though, to be realistic: “there only needs to be one dissatisfied employee (MC1)” and “if someone wants to do harm, then it will happen anyway (CC1)” (table 17).

Countering the outsider threat firms try to restrict physical access. They make well-considered choices as they “look closely at who we show the extended and who the limited tour (LC1)” and “check on arrival... to create barriers (PC1)”, though, realizing that things as camera surveillance, daunting as it is, sort in that you are always too late (PC1). In addition, firms try
to protect trade secrets and intellectual property by “being reserved with mentioning suppliers (EC1)” (table 17) and by banning photography out of the factory (MC1) (Appendix J).

Table 17.
Quotes on Physical/Human Counter Measures

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>Men heeft natuurlijk wel in het contract een bepaalde geheimhoudingsclausule, als is dat geen enorm zware clausule, als iemand kwaad wilt dan lukt dat toch wel.</td>
</tr>
<tr>
<td>CC2</td>
<td>Het risico dat ze weglopen is er altijd, dan is er een concurrentiebeding, dat is een juridische kwestie. Voorkomen kun je het nooit, maar je probeert een optimale omgeving te creëren waardoor je de kansen tot nihil terugbrengt.</td>
</tr>
<tr>
<td>EC1</td>
<td>We zijn wel heel voorzichtig met het noemen van leveranciers, bepaalde formules en onze bedrijfsgeheimen zijn natuurlijk vertrouwelijk, dat zal een leverancier niet zomaar vrijgeven, maar je wilt dat risico zover mogelijk indammen.</td>
</tr>
<tr>
<td>LC1</td>
<td>We hebben over het algemeen, in vergelijking met het verleden, geen open deur beleid meer. We kijken goed wie we wel en niet mee rond nemen en als we iemand meenemen hebben we de uitgebreide tour en de beperkte tour. Daar hebben we wel van geleerd, de dingen waar we mee voorop liepen, die wilden anderen graag kopiëren.</td>
</tr>
<tr>
<td>MC1</td>
<td>Er hoeft er maar één ontevreden te zijn en met de map onder de arm ergens naar toe te gaan. Die kans bestaat altijd. Het enige wat je kunt doen is concurrentiebeding, in contracten opnemen dat het voor mensen verboden is.</td>
</tr>
<tr>
<td>PC1</td>
<td>Het hebben van goede mensen is belangrijk, techneuten zijn erg schaars, dus je moet goed zorgen voor je mensen, dat ze niet weg willen gaan, dat ze tevreden zijn, dat ze niet uit onvrede bepaalde dingen gaan doen. Uit onvrede zou je dingen kunnen saboteren, hoe houd je dat in de gaten, sommige dingen zie je en andere dingen niet.</td>
</tr>
<tr>
<td>PC1</td>
<td>Als iemand eenmaal binnen is.. wat moet je daar tegen doen? We hebben wel controle bij de ingang, of ze een pasje hebben gekregen. De rest komt alleen binnen met een tag, dus zo proberen we daar wel een aantal barrières in op te werpen.</td>
</tr>
<tr>
<td>PC1</td>
<td>Met camerabewaking ben je altijd te laat maar het is wel in een bepaalde mate afschrikwekkend en je kunt er achteraf iets mee achterhalen.</td>
</tr>
</tbody>
</table>

With regard to digital counter measures concerning Industrial Espionage, firms understand that they are never fully secure. An attempt is made to create a certain layering, “authorizing the use of data (LC1)”, “using a passwords regime, and splitting networks (PC1)”, and “assigning all IT services to one party (CC1)” (table 18). One respondent even mentioned that he had heard that other firms use policies regarding USB-free PCs, but he had “never seen it in practice (PC1)”.

---

69
Now all individual concepts are addressed, the relationships between these are being looked at. Comparing the conceptual and empirical causality is the main goal of the qualitative section. By doing that, possible similarities and discrepancies come to light, giving the results of the quantitative additional meaning.

### 5.3.3 Inter-concept relations

**Relation Product Innovation and Industrial Espionage**

As was conceptualized, Product Innovation could have a positive effect on the probability of becoming a target of Industrial Espionage. New and successful products are interesting for outsiders and in some cases easy to copy. Whereas this relation was calculated quantitatively in the previous section, the qualitative section is based on quotes that are most relevant in terms of how (if) respondents experience the conceived causal relationship and how they deal with this.
The results (table 19) shed some light on the acknowledgement of the relation between Product Innovation and Industrial Espionage by the firms. All the firms are product-focused, although there is a shift towards more integration of service as “it is increasingly becoming a digital service story (MC2)” (Appendix J). Some firms see their products being copied in the country of residence and abroad. Respondents stated that “products are really well copied, and are hard to distinguish from real (EC1)”, “we now see the first copies from China appear (MC1)”, and “you just think that's one of us (MC2)”, to pinpoint that seize does not have to be an obstacle for copying. But it is not only the product itself which is valuable to others. In some cases it is even more harmful if “exact specifications of a product, and why38 we did certain things, end up at a competitor (PC1)”, because that is where the knowledge is. In other cases product-level espionage is less expected as “the market is characterized as old, with little innovation, everything is already known (TC1)”. In perspective this respondent stated that he thinks that espionage in fact did play in the 80s-90s, but not anymore. This aspect of ‘everything is already known’ can be found in other industries as well, due to the degree of innovativeness and openness. For example, they “know practically how others produce, there is not much secrecy about that (CC2)” (Appendix J). One firm tries to protect their recipes “by using fancy names for the ingredients we put into it (LC1)”. Concluding, Product Innovation could be seen as an important factor of being attractive as a target of Industrial Espionage and firms are trying to keep their products, especially the specifications, for themselves, to reduce the risks, though it is also seen as “a compliment (EC1)” (Appendix J).

<table>
<thead>
<tr>
<th>Table 19.</th>
<th>Quotes on the relation between Product Innovation and Industrial Espionage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EC1</strong></td>
<td>De producten zijn echt goed nagemaakt, op foto’s op Ebay zijn ze door onze medewerkers moeilijk van echt te onderscheiden.</td>
</tr>
<tr>
<td><strong>LC1</strong></td>
<td>Het is bekend bij de klant, en daardoor ook wel bekend bij concurrenten. De klant kan het recept ook wel eens bij een collega neerleggen, dat gebeurt, niet vaak, maar het gebeurt, en dan heeft de collega het recept ook. We proberen dat zoveel mogelijk te voorkomen door een beetje fancy namen te gebruiken voor de spullen die we erin stoppen, maar in onze sector is het heel gebruikelijk om dingen open te communiceren.</td>
</tr>
<tr>
<td><strong>MC1</strong></td>
<td>We hebben een aandrijflijn ontwikkeld voor de foliekas, dat is een kas met een veel lagere investering. Dat is een andere markt met een andere behoefte. Dat is een enorme innovatie geweest en we zien nu de eerste kopieën uit China verschijnen.</td>
</tr>
</tbody>
</table>

38 System understandings (Quinn et al., 1996).
Table 19.
*Quotes on the relation between Product Innovation and Industrial Espionage*

<table>
<thead>
<tr>
<th>Company</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC2</td>
<td>We hebben een concurrent, die hebben gewoon letterlijk onze 16tons heftruck gekopieerd, dezelfde kleurstelling, je denkt gewoon dat is er één van ons.</td>
</tr>
<tr>
<td>PC1</td>
<td>Op internet kun je veel vinden, maar wat ik heel vervelend zou vinden als de exacte specs. van dit product, en waarom we bepaalde dingen gedaan hebben, als die bij een concurrent terecht zouden komen.</td>
</tr>
<tr>
<td>TC1</td>
<td>Omdat de markt zo oud is en er weinig innovatie is, is alles al bekend. Ik denk dat spionage in de jaren 80-90 wel echt gespeeld heeft, maar nu niet meer.</td>
</tr>
</tbody>
</table>

*Relation Digitization and Industrial Espionage*

As was conceptualized, Digitization could have a positive effect on the probability of becoming a target of Industrial Espionage. For instance, because tacit knowledge has become explicit, or that an increasing degree of digitization offers a larger palette of possibilities to spy. Whereas this relation was calculated quantitatively in the previous section, the qualitative section is based on quotes that are most relevant in terms of how (if) respondents experience the conceived causal relationship and how they deal with this.

The results shed some light on the experiences of the respondents with this inter-concept relation. Most of the firms acknowledge, and therefore supporting, the conceptualized relationship as “*anything you convert digitally can be stolen* (PC1)”, but not all firms experience this already. On one hand, respondents explain that this is because “*we still do a lot in the old-fashioned way* (TC1)”, or because their products are not that high-tech (CC1). One reason could be that it is firm-specific, or at least industry-specific. On the other hand, one respondent even called his competitor “*a vulture*”, as it tried to copy and own his process knowledge by speaking with the same suppliers (MC1). Another respondent is convinced that, as has already been mentioned, “*it is less about stealing information and more about sabotaging firms*”, because “*if you cannot do anything digitally anymore, then you are screwed* (MC2)”(table 20).

Table 20.
*Quotes on the relation between Digitization and Industrial Espionage*

<table>
<thead>
<tr>
<th>Company</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>Bij elk gebouw tekenen we weer die nieuwe betontrap uit, en het is ook zo’n niet hightech product, als we er allemaal sensoren in gaan stoppen die allemaal data gaan verzamelen, dan</td>
</tr>
</tbody>
</table>
Table 20.
Quotes on the relation between Digitization and Industrial Espionage

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wordt het gaande weg steeds interessanter, en dan ga je ook kijken naar databeveiliging. Maar dat gebeurt voorlopig nog niet.</td>
</tr>
<tr>
<td>MC1</td>
<td>De concurrent in het Westland, die kopieert alles wat wij hebben. Hij praat met dezelfde leveranciers, op het moment dat wij investeren in machines, borgen we dat met een NDA en willen wij zeker weten dat die kennis, proceskennis van ons niet bij hem terecht komt. Het zijn aasgieren.</td>
</tr>
<tr>
<td>MC2</td>
<td>Het is minder het jatten van informatie en meer het platleggen. Als er ergens in de keten iets verkeerd gaat, dat heel het bedrijf stilligt. Als je digitaal niets meer kunt, dan ben je de klos.</td>
</tr>
<tr>
<td>PC1</td>
<td>Maar dat houdt ook verband met de digitale wereld, alles wat je digitaal maakt kan worden gejat. Je kunt het stelen uit de computer, en of het gaat over privacy of over proprietary information, van beiden wil je niet dat het op straat komt te liggen.</td>
</tr>
<tr>
<td>TC1</td>
<td>Omdat we nog heel veel op de ouderwetse manier doen zie ik de risico’s van cyber espionage ook niet.</td>
</tr>
</tbody>
</table>

Relation Open Innovation and Industrial Espionage

As was conceptualized, Open Innovation could have either a positive or negative effect on the probability of becoming a target of Industrial Espionage. For instance, a large number of partnerships could show that a firm is a good partner and therefore good performer. But a large number of open innovations practices could also indicate that firms have nothing left to hide. Whereas this relation was calculated quantitatively in the previous section, the qualitative section is based on quotes that are most relevant in terms of how (if) respondents experience the conceived causal relationship and how they deal with this.

The qualitative approach of this relationship shows that firms recognize the risks, “It would be bothering me to find out that our developments would become known (CC1)”, often resulting in non-disclosure agreements as a legal means to curb possible risks (PC1, MC1, MC2). “Almost with everyone, nowadays more than ten years ago (MC2)”. Nevertheless, the results are not fully supporting the conceptualized relationship in one direction. It is in fact remarkable that the results show that there can be also aspects of collaboration which reduce potential consequences of Industrial Espionage. Loyalty and trust are key. For instance, “the partners we share secrets with, are known partners for a long time (EC1)”, and partners are even protecting the firms as a supplier called to inform that a competitor was asking for product according the firm’s specifications (MC1). Though, as soon as a firm starts collaborating, the firm becomes
dependent on the risk-awareness of the partner, “becoming as strong as the weakest link (MC2)” (table 21).

**Table 21. Quotes on the relation between Open Innovation and Industrial Espionage**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CC1</strong></td>
<td>We zijn, in samenwerking, met een redelijk revolutionaire ontwikkeling bezig, ik zou het wel vervelend vinden als die op straat zou komen te liggen, maar ik denk dat velen in de industrie zo arrogant zijn om de ontwikkeling niet te omarmen als iets dat gaat werken, omdat het zo al goed gaat.</td>
</tr>
<tr>
<td><strong>EC1</strong></td>
<td>Wij gaan er niet vanuit dat onze leveranciers kwaad willen met informatie, maar je kunt het maar beter afdekken want dan heb je in ieder geval niet het risico dat het kan gebeuren. De partners waar de geheimen liggen, daar zijn we al lang partners mee. Dus er is wel sprake van loyaliteit en vertrouwen.</td>
</tr>
<tr>
<td><strong>MC1</strong></td>
<td>Maar je hebt ook loyale leveranciers, die light aandrijving voor de foliekas, die maken we in plaats van in een gietijzeren behuizing in een aluminium behuizing. Die laten we in Nederland spuitgieten, en die leverancier belde ons op, de concurrent van jullie vraagt een kopieproduct, volgens de specificaties van ons bedrijf, ik ga het niet maken maar weet wel dat zij op zo’n manier de markt aan het benaderen zijn. En die loyaliteit is wederzijds want als een leverancier zo met je omgaat, ga je ook zo met je leverancier om. Dan ga je niet voor 2% kostenverlaging naar een ander. Daar ligt de basis voor een goede verstandhouding.</td>
</tr>
<tr>
<td><strong>MC2</strong></td>
<td>Op het moment dat wij IP gaan delen, dan komt er een NDA. Bijna met iedereen, dat was tien jaar geleden een stuk minder.</td>
</tr>
<tr>
<td><strong>MC2</strong></td>
<td>Bedrijven zoals wij gaan in zee met partijen die zorgen dat de cybersecurity goed werkt, maar als je gaat samenwerken met andere partijen en data gaat delen, zoals hoge scholen, dan hoop je dat die partijen dat net zo goed doen. Zo sterk als de zwakste schakel. Maar goed, ik denk dat dat niet veel anders gaat worden dan dat het al is.</td>
</tr>
<tr>
<td><strong>PC1</strong></td>
<td>Het beïnvloedt niet de keuze voor innovatievormen maar het zit wel in samenwerkingsovereenkomsten. We zullen dus geen details delen totdat er zo’n geheimhoudingsplicht is getekend. Van die geheimhoudingsovereenkomst zijn verschillende vormen, en we zorgen dat als we een samenwerking aangaan, bij een nieuw groundbreaking product of technologie, of met het specificeren van machines er geen data wordt uitgewisseld voordat er een overeenkomst is getekend. Dus belemmert het, nee, maar soms moet je een paar dagen wachten totdat iemand een krabbel heeft gezet onder zijn NDA. Das praktisch maar is geen belemmering voor de samenwerking.</td>
</tr>
</tbody>
</table>

**Interaction Digitization and Open Innovation**

As was conceptualized, Open Innovation could have a moderating effect on the relation between Digitization and the probability of becoming a target of Industrial Espionage. One way
to explain this thought is that digitizing firms are more attractive to spy on, and if they are seen as good partners and are connected to the other, become even more attractive to spy on in terms of more and more interesting information and more possibilities to spy. An opposite way to look at it is to see digitizing firms as attractive targets but because they are innovating more open, most of the information is already available and not secret. Whereas this relation was calculated quantitatively in the previous section, the qualitative section is based on quotes that are most relevant in terms of how (if) respondents experience the conceived causal relationship and how they deal with this.

There are no direct results on this specific moderating effect in the conceptualized relationship. There is, however, an interesting topic introduced during one of the interviews. A combination of the three mentioned concepts yields a new subject, namely that of liability. One respondent rightly pointed out that if “our product is connected to a network and to the network of the customer, and someone breaks into our machine via the network and thus enters the customer’s network and lays down the entire warehouse management system of the customer”, then “you have to make sure that it is your liability piece is properly mapped out (MC2)” (Appendix J).

5.3.4 Other memorable quotes
Several solutions and measures to reduce the impact of Industrial Espionage were mentioned during this chapter. But the ‘best’ strategies, all with the same scope, are saved for this section as respondents state that “you just have to make sure that you are faster and more efficient in your entire process, which is often more difficult to copy than a product or software (MC2)”, “the best protection is to stay ahead in your industry, keep innovating, and make sure that you are known as an innovator, then you keep the leading position automatically (CC1)”, and “due to espionage you could lose bits, but it is the total package that makes us successful in the market and that cannot be copied (MC1)” (Appendix J). This can be seen in the light of the Resource-based View, as firms combine unique competences and resources to be successful. In addition, firms acknowledge that competitive advantage is generally temporary.

Difference can be seen between more incremental innovation practices (CC1) and more radical developments as firms were building new factories with new manufacturing processes (CC2, LC1). Important subjects in this are the culture of the organization (MC2), the quality of relationships (loyalty and trust) with customers, and the dealer or distribution network (MC1).
In other words, as information is seen as a target of espionage, the content of the value chain could be seen as a protective measure because not all can be copied.

5.3.5 Summary
Based on qualitative analysis, insights on if, how and why strategic decisions are made regarding to the probability of becoming a target of Industrial Espionage were analyzed. The contents of the relations earlier mentioned have been researched. This was done by interviewing eight respondents.

First, the main concepts were introduced. All firms to a greater or lesser extent fit these concepts. No single firm has fully integrated Industry 4.0 yet but they are heading in the right direction, also because they see the potential. Second, the inter-concept relations were investigated. The respondents understand and acknowledge the conceptualized relations, see the threats of Industrial Espionage, although they are not valuing it as the highest risk to their businesses. Furthermore, respondents think it is not only about stealing trade secrets or proprietary information but also about shutting down business systems, with company-transcending consequences.

5.4 Concluding words
Complementing quantitative analyses by a qualitative method, a mixed methods study was created and conducted to obtain a more holistic view on the several forms of innovation and their relation with Industrial Espionage. By combining the results it becomes clear whether the analyses confirm, oppose, or amplify each other.

The quantitative analysis gave support for three hypotheses (1A, 1B and 2), as is presented in figure 4 by means of black arrows. This support could also be found in the qualitative analysis, as the respondents acknowledge the existence of these relationships (figure 4, black interrupted arrows). Based on the quantitative approach, there was no support for any influence of Open Innovation on the probability of becoming a target of Industrial Espionage, presented by a red arrow. Remarkable is that the qualitative results shed a new light on the assumed relationship, though not in terms of supporting (figure 4, red interrupted arrow). The importance of the content of this relation, for instance trust and loyalty, provides helpful insights and lessons in how to make use of collaborations in a possible protective way. The interaction effect between
Digitization and Open Innovation was not found in both qualitative as quantitative analysis (figure 4, red- and red interrupted arrow).

Figure 4. Conceptual model.

- Supported by quantitative analysis
- Supported by qualitative analysis
- Not supported by quantitative analysis
- Not supported by qualitative analysis
Chapter 6 Conclusions, implications and limitations

6.1 Summary

In this chapter the conclusions, implications and limitations are addressed. After a short introduction of the topics, Industrial Espionage and forms of Innovation, the following research question was formulated:

What is the impact of digitization of manufacturing processes, product innovation, and open innovation, on the probability of becoming a target of industrial espionage for firms in the Dutch manufacturing industry?

In search of an answer to this question, a literature study was conducted first. Consequently, the main concepts were defined and operationalized. Several adjustments were needed in order to come to measurable constructs. The European Manufacturing Survey of 2015 provided usable data to conduct a quantitative analysis. Concerning Product Innovation, a distinction was made between incremental and radical product innovation, supplemented with a product portfolio aspect. Both constructs of Digitization and Open Innovation were built based on theory of McKinsey Digital (2015) and Van de Vrande et al. (2009), and the dependent variable was made dichotomous to make a logistic regression possible. In addition, eight interviews were conducted after the literature study was finished. The interviews are transcribed and theoretical coded in order to get grip on the large number of quotes. All this was done to better understand what is going on in the quantitatively tested relationships. After all, it is important after figuring out there are inter-concept relationships, to understand why these relations exist and if the significantly tested relations are also of practical relevance.

Based on the extensive literature study it was expected that Product Innovation and Digitization would have a positive influence on the probability of becoming a target of Industrial Espionage. In other words, those aspects would make a firm vulnerable and/or attractive. The direction of the expected relationship between Open Innovation and the probability of becoming a target of Industrial Espionage was less clear, resulting in a hypothesis without a chosen direction. This had also as consequence that the direction of the possible moderating effect was uncertain. In other words, if there was a moderating effect to be found, the direction would be difficult to predict.
The (empirical) results from the EMS (2015) showed that Product Innovation and Digitization, referring to hypotheses 1A, 1B and 2, in fact do influence the probability to become a target of Industrial Espionage. Based on the analysis a higher degree of Digitization results in 19.2% increase of the probability. For incremental and radical Product Innovation it is much more, respectively an increase by a factor three and almost four of the probability. In other words, if a firm innovates its products radically, the probability almost quadruples.

The (empirical) results showed however that not all formulated hypotheses are supported. After conducting the logistic regression, it became clear that the construct of Open Innovation had no significant positive nor negative effect on the probability of becoming a target of Industrial Espionage. Also the interaction term of Open Innovation on the relation between Digitization and Industrial Espionage was not found significant.

The qualitative analysis sheds new light on the described concepts and quantitatively tested hypotheses. All firms fit the concepts to a certain degree in terms of that they are digitizing their manufacturing processes, innovating their products or that they are collaborating with others for, among others, innovative purposes. All respondents are familiar with and acknowledge the threat of Industrial Espionage as outlined, but also notice that it is not the only or biggest threat they face. Compared to the quantitative analysis, the results of the interviews do suggest that Open Innovation can be used as a protective means in countering the impact of Industrial Espionage. Trust and loyalty are key and firms have to make sure that their value-adding capabilities are through the whole value chain.

Overall the answer on the research question is that there is support, quantitative and qualitative, for positive relationships of Product Innovation and Digitization on the probability of becoming a target of Industrial Espionage. On the other hand, Open Innovation is not found to be statistically affecting this probability but the qualitative analysis revealed that if trust and loyalty are present in the interpretation of the concept of Open Innovation, it could decrease the probability. At last, there is no support for the conceptualized interaction term of Open Innovation on the relation between Digitization and the probability of becoming a target of Industrial Espionage.

Looking back on the entire study, one can conclude that the answer to the title of the research is ‘yes’. Yes, further digitization of manufacturing processes is a must to stay competitive, and
yes, firms will face new and unknown threats, similar to the mythical story of the Trojan horse. Time and further research will tell what impact this will have.

### 6.2 Implications

#### 6.2.1 Theoretical implications

By conducting this research is tried to contribute to the existing literature on Industrial Espionage. However Industrial Espionage is an interesting topic, it is also a sensitive issue and not everything is known yet as it is a developing subject. The what, who, how and why questions of Industrial Espionage are addressed in earlier research, but the mutual relations as conceptualized and found in this research have never been investigated in this way before. In addition, the comparison between the impacts of knowledge leakage and Industrial Espionage is one to highlight, as it elucidates the phenomenon. Also the link between Industrial Espionage and Innovation practices, originating from common sense, could be an important contribution to theory, as it maps a shadow side of innovating. Theory on innovation is often about strategic choices in order to increase performance and less about possible consequences in terms of becoming an attractive target. This is an underexposed issue that could use some attention, especially with new threats of cybercrime and such.

Also, this research acknowledges that the competitive advantage originating from innovations alone, is usually only temporary, seen from a Resource-based perspective. A higher degree of digitization of manufacturing processes, and its features, is seen as an advantage relative to competitors, though it is momentary. An extensive research on informant reports of East and West Germany investigated by Glitz and Meyersson (2017) suggests something similar, but from an espionage perspective. They found that, on the one hand, espionage programs paid off in significant technological growth, even as it crowded out domestic Research and Development (R&D). But, on the other hand, not paying enough attention to original research and development resulted in a collapse of the industry, meaning that in the long run, industrial espionage actually hurt the economy. Therefore, the competitive advantage originating from Industrial Espionage is also temporary, and the final profit is questionable.

#### 6.2.2 Practical implications

The results and conclusions of the mixed-methods design lead to some practical implications. First, although it is reasonably logical, Product Innovation is a strategy-aspect that makes a firm highly attractive for espionage. Nevertheless, it is now shown, creating awareness, and could
be taken into consideration by firms, when choosing innovating strategies and in particular for prioritizing the anti-measures.

The most important take home message of this research is that firms that digitize their manufacturing processes become more attractive targets of Industrial Espionage. The same applies to Product Innovation. Of course there are lots of advantages of digitization but it is important to be aware of the downsides. If Industry 4.0 takes it course as predicted, kind of forcing firms to go along with it, and the predicted benefits in terms of sustainable competitive advantage become reality, then the impact of the downsides might become equivalent.

According to the results of the research, it is important to value partnerships. As was mentioned, partnerships characterized by trust and loyalty could become protective measures of intellectual property if managed correctly. What can be learned from this research is that if a firm is innovating or collaborating with other firms, that it should look closely at cooperation criteria other than fast results. Though a lot can be captured in NDAs, trust and loyalty should be base in business-critical activities.

Also worth mentioning is the additional risk of connectivity. Firms should be aware of the fact that their security is as weak as weakest security of their partners. Firms can try to optimize their own security but this is worthless if they are fixated on that. In addition, liability becomes an important issue. Firms should make sure that they contractually define this very precisely.

At last, and that is nothing new, firms should try to create value-adding aspects in the whole value chain. This is the best security measure of all. Only by pursuing this, firms can ensure that someone copying products, processes, or parts of their competitive advantage, becomes not business threatening. It is the sum of product, process, and partnerships which makes survival plausible.

6.3 Limitations
This research contains a number of boundaries and limitations. A first limitation is the fact that the conceptual model only consist of a limited number of variables. One could understand that the reality is much more complex. There might be several more independent variables that can explain the dependent variable, for instance the use anti-measures. A more specific point to highlight is that both constructs have relative low values for Cronbach’s alpha. On one hand,
this could mean that there might be more items to build the construct. On the other hand, the values show that both concepts are complex phenomena, which was also reflected in the literature. In addition, the concept of Industrial Espionage as is presented in this research is doubtful. The combination of experiences of firms with industrial espionage and firms heard of industrial espionage cases is necessary because of the sensitivity of the issue. But, it can also be bothering not knowing if all firms have heard of the same case. However, it is very unlikely, it could result in an extreme form of double counting of data.

Furthermore, only a small number of respondents is interviewed. Despite that the outcomes shed a light on the content of the inter-concept relations and are of practical use, the sample size is considered quite small. Therefore the degree to which these firms represent the manufacturing sector as a whole is questionable, which makes the generalizability of the qualitative results limited. In addition, the research is focused on only Dutch manufacturing firms, in both quantitative and qualitative analysis, making it less generalizable worldwide.

To deal with some of the limitations, current research made use of a mixed-methods research design in which qualitative analyses of eight interviews supplemented the quantitative analysis of the data from the EMS (2015). The method provides strengths that offset the weaknesses of both quantitative and qualitative research. Only using one of two techniques would not have provide full information on the conceptualized relations. The use of the chosen design allows to investigate the concepts and their inter-concept relationships more in-depth, examining if and why relations exist. This has several advantages. First, by making use of mixed-methods, it was possible to gather information on the conceptualized relationships but also on the awareness and acknowledgement of those. Furthermore, the used method makes it possible to understand possible causality. For instance, the interpretation of Open Innovation would not have come to light if only a quantitative analysis was conducted.

In order to prevent that this research would harm the participating firms, all interviews are made anonymous. The added value of participating consist of receiving the report and to take note of the results. The ideal scenario is that the information in this research supports firms’ future strategic decisions regarding innovation forms and threats.

Reflecting on this research, some recommendations regarding further research are to be mentioned. As the topic of Industrial Espionage is developing, the cyber aspect will take an
increasing part. Though this topic is mentioned in the research, it is still underexposed and needs further investigation as it is a serious threat to intellectual property and daily functioning of firms. Furthermore, a suggestion is to include anti-measures in the model in search of a degree of effectiveness of those measures. This could result in very specific managerial implications on security-level, making further research of more practical relevance.
References


Blachet, M. & Rinn, T. (2016). *The Industrie 4.0 transition quantified. How the fourth industrial revolution is reshuffling the economic, social and industrial model*. München: Roland Berger


## Appendices

### Appendix A

<table>
<thead>
<tr>
<th>Activity</th>
<th>Method</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dumpster diving</td>
<td>Spies pick through corporate garbage for information</td>
<td>Many corporate technical secrets can be obtained</td>
</tr>
<tr>
<td>Elicitation</td>
<td>Scientific seminars, trade shows, unsolicited telephone calls</td>
<td>Bits of information about new developments</td>
</tr>
<tr>
<td>Electronic interception</td>
<td>Telecommunication interception or computer intrusions</td>
<td>Detailed information and secret plans can be obtained</td>
</tr>
<tr>
<td>Insider treason</td>
<td>Espionage acts performed by company personnel</td>
<td>Detailed information and secret plans can be obtained</td>
</tr>
<tr>
<td>Product announcement and preannouncements</td>
<td>Detecting technical features and availability of new developments</td>
<td>Counteracting the competitor’s innovations and keeping ahead in product development</td>
</tr>
<tr>
<td>Industrial theft</td>
<td>Copying corporate files by breaking in or stealing executive luggage or laptop computer</td>
<td>Much information can be obtained regarding all aspects of the company’s business</td>
</tr>
<tr>
<td>Reversed engineering</td>
<td>Obtaining a sample of the product, taking it apart and putting it back together</td>
<td>Determining product features and production procedures for replication</td>
</tr>
<tr>
<td>Business intelligence</td>
<td>Using information such as company job openings, suppliers, subcontractors, prices, mergers and financial results</td>
<td>Understanding where the competition is going and competitor’s strengths and weaknesses</td>
</tr>
<tr>
<td>Hiring away key information employees</td>
<td>A company hires a key executive away from the competitor</td>
<td>Learning first-hand how the competitor is managing its business</td>
</tr>
<tr>
<td>Lawsuits</td>
<td>Lawsuits relating to products and patents</td>
<td>Much information is received about technical products and their developments</td>
</tr>
<tr>
<td>Government-supported espionage</td>
<td>Using government organizations such as CIA and FBI for industrial spying</td>
<td>Valuable secret information can be obtained by specially trained people</td>
</tr>
</tbody>
</table>
Appendix B

Table B.  
*Contrasting Principles of Closed and Open Innovations.* From Chesbrough (2003). The era of open innovation. p. 38

<table>
<thead>
<tr>
<th>Closed Innovations Principles</th>
<th>Open Innovations Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>The smart people in our field work for us.</td>
<td>Not all of the smart people work for us, so we must find and tap into the knowledge and expertise of bright individuals outside our company</td>
</tr>
<tr>
<td>To profit from R&amp;D, we must discover, develop and ship it ourselves.</td>
<td>External R&amp;D can create significant value; internal R&amp;D is needed to claim some portion of that value.</td>
</tr>
<tr>
<td>If we discover it ourselves, we will get it to market first.</td>
<td>We don’t have to originate the research in order to profit from it.</td>
</tr>
<tr>
<td>If we are the first to commercialize an innovation, we will win.</td>
<td>Building a better business is better than getting to market first.</td>
</tr>
<tr>
<td>If we create the most and best ideas in the industry, we will win.</td>
<td>If we make the best use of internal and external ideas, we will win.</td>
</tr>
<tr>
<td>We should control our intellectual property so that our competitors don’t profit from our ideas.</td>
<td>We should profit from other’s use of our intellectual property, and we should buy other’s intellectual property whenever it advances our own business model.</td>
</tr>
</tbody>
</table>
Appendix C

Table C. Overview Research design and variables

<table>
<thead>
<tr>
<th></th>
<th>Quantitative method</th>
<th>Scale</th>
<th>Dummy</th>
<th>Qualitative method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependent Variable</td>
<td>Chance/probability/odds of becoming a target of Industrial Espionage</td>
<td>Dichotomous</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
| Independent Variables    | 1. Digitization of production processes  
2. Open innovation  
3. Product innovation | Ratio  
Ratio  
Categorical |       | Yes   |
| Control Variables        | Firm size  
Firm industry  
R&D investment  
Supplier type | Ratio  
Categorical  
Categorical  
Dichotomous |       | Yes   |
| Interaction term         | cDigitization x cOpenInnovation | Ratio   |       |                   |
| Research concepts        | 1. Digitization (of manufacturing processes)  
2. Open Innovation  
3. Product Innovation  
4. Risks of Innovation activities, such as Industrial Espionage |                   |       |                   |
| Type of Analysis         | Logistic regression |        |       | Theory-guided coding |
Appendix D

Table D.

Interview script

Intro; 5 minuten

Goedendag, mijn naam is Jasper Haen, masterstudent bedrijfskunde aan de Radboud Universiteit Nijmegen. Allereerst hartelijk dank dat ik hier mag komen en dat u mij te woord wilt staan. Dit interview is in het kader van mijn afstudeeronderzoek dat ik doe naar digitalisering en andere innovatie activiteiten in de Nederlandse maakindustrie en de risico’s die daar mee gepaard gaan. Het interview is gestructureerd aan de hand van een aantal vragen en mocht er onduidelijkheid zijn dan kunt u om verheldering vragen.

In verband met het transcriberen van het interview wil ik u vragen of dit gesprek mag worden opgenomen. Dit komt ten goede aan de verwerking van de resultaten en draagt bij aan een precieze verslaglegging. Het transcript is geheel anoniem en niet terug te herleiden naar u of het bedrijf. Ik zal het transcript eveneens met u overleggen voorafgaand aan de analyse. Al met al zal het interview circa een uur in beslag nemen.

1. Oriënterende vragen ; 5 minuten

a. Wie bent u en wat is uw rol binnen het bedrijf?
   Grootte arbeidsduur bedrijfstak

b. Op welke manieren bent u betrokken bij digitalisering en andere innovatie activiteiten?
   (focus op werkzaamheden/ activiteiten)

c. Binnen welke specifieke industrie opereert uw bedrijf met name?
   Welke activiteiten worden uitgevoerd?

d. Wat is uw bedrijfsstrategie?
   Hoe verkrijgt u competitief voordeel ten opzichte van concurrenten?

e. Ondernemingsstrategie: Wat probeert uw bedrijf op het gebied van digitalisering en innovatie te bereiken in de komende 5 jaar?

2. Digitalisering; 10 minuten

Steeds meer industrieën digitaliseren hun processen. Een trend, het zogenaamde industry 4.0, waarbij automatisering en gegevensuitwisseling steeds verder doorgevoerd wordt is hier een voorbeeld van. Dit maakt processen efficiënter, optimaliseert voorraadbeheer en maakt logistiek zichtbaarder.

a. Wat betekent digitalisering als proces innovatie voor uw bedrijf?
   (productie, marketing/verkoop, O&O, imago, design)?

b. Welke activiteiten met betrekking tot digitalisering (m.n. in de productie) ontwikkelt/voert uw bedrijf (uit)?
(in welke fase(n) van adoptieproces: kennis van, concrete plannen, beslissingen, implementeren, monitoren, resultaten, effecten)
(afhankelijk van specifieke fase: wat/hoe orienteren; afwegingen ; welke prioriteiten; manier implementatie; monitoren, resultaten, uitwerking (voor wie)..)
(activiteitsgericht, bijv. beleid, rapporten, bespreking in (werk), overleggen, acties, trainingen e.d)

c. In hoeverre voelt uw organisatie druk om mee te gaan in deze ontwikkelingen in de markt? (Kijken naar concurrenten, subsidie vanuit de overheid, …) Waaromvraag. Wat zijn uw ervaringen?

d. Op welke manier betrekt het bedrijf mensen van verschillende afdelingen/funcities/disciplines bij deze digitalisering?
(event. doorvragen over een nieuwsbrief/ Workshops / Bedrijfsplan)

| 3. Open Innovatie; 10 minuten | Het idee van open innovatie is dat bedrijven niet langer volledig afhankelijk kunnen zijn van eigen innovatie, door uiteenlopende ontwikkelingen (mobilitieit van werknemers, scholing, externe kennis en toegankelijkheid) en dus op zoek gaan naar samenwerkingen in verscheidene vormen?
| a. In welke mate heeft uw organisatie samenwerkingsverbanden op het gebied van Research and Development?
| (kennis van, concrete plannen, beslissingen, implementeren, monitoren, resultaten, effecten)
| b. Waarom heeft u deze samenwerkingsverbanden? (Wilt u naar een andere situatie?) Wat zijn uw ervaringen?
| (Soorten, prijs, leveranciers)
| c. Op welke manier is er gedurende de afgelopen drie jaar een verschuiving zichtbaar met betrekking tot de innovatiestrategie?
| d. Wat heeft dit het bedrijf opgeleverd?

Resultaten innovatie activiteiten

| 4. Product Innovatie; 10 minuten | Bij productinnovatie gaan het over de verbeteringen van het product zelf of de lancering van nieuw ontwikkelde producten. Dit kan competitief veel voordelen opleveren maar kan ook duur zijn en het succes is niet altijd gegarandeerd.
| a. Welke vernieuwingen zijn er de afgelopen 3 jaar doorgevoerd in de producten en/of portfolio van het bedrijf?
| b. In welke mate is uw bedrijfsstrategie gebaseerd op product innovatie? Staat uw bedrijf hierom bekend? (Imago)
5. **Risico’s**

Met digitalisering en andere innovatie activiteiten kunnen risico’s gepaard gaan. Zo kan de innovatie niet het gewenste effect opleveren, kunnen bedrijven door vergaande digitalisering kwetsbaar worden en kan open innovatie scheve voordelen resulteren.

   a. Welke risico’s en impact gaan er gepaard met de innovatie die uw bedrijf hanteert? Wat zijn uw ervaringen? Voorbeelden?
      - Financieel, weglekken van kennis, kopiëren van producten?

   b. Hoe worden deze risico’s beperkt?

6. **Industriële Spionage**

Een risico waar de hedendaags steeds meer aandacht voor is, is industriële spionage, zowel fysiek als cyber.

   a. Wat verstaat u onder industriële spionage?
      (Wat is het? Welke vormen kent het? Wie spioneert?)

   b. Hoe gaat uw bedrijf om met dit fenomeen? (trainingen, specifieke aanwijzingen, policies met betrekking tot geheimhouding, beperkte toegang tot locaties?)

   c. In hoeverre komen deze activiteiten voort uit situaties in de praktijk?

   d. Hoe worden bedreigingen gesignaleerd?

   e. Balansvraag: In welke mate beïnvloedt het risico van industriële spionage de keuze voor innovatievormen (proces, product, open innovatie)?

**Outro**

Hartelijk dank voor dit interview. Zoals ik al zei zal ik het interview volledig anonimiseren en als transcript nog aan u voorleggen voorafgaand aan de analyse. Zodra het gehele onderzoek afgerond is kan ik het u digitaal toesturen als u daar interesse in heeft.

Dan nog een laatste vraag namens mijn begeleider: Zou u later einmalig een vragenlijst willen invullen? (Emailadres)
### Appendix E

**Table E. Operationalization: items used from EMS (2015)**

<table>
<thead>
<tr>
<th>Type variable</th>
<th>Construct</th>
<th>Items used from European Manufacturing Survey (2015)</th>
</tr>
</thead>
</table>
| IV | Digitization of manufacturing processes | 8.1:Welke van de volgende technologieën worden momenteel in uw bedrijfsvestiging toegepast?  
- Industriële robots voor bewerking en fabricage  
- Industriële robots voor hanteren van gereedschap  
- Additieve productietechnologie voor maken van prototypes  
- Productie met additieve productietechnologie  
- Systemen voor Machine2Machine communicatie, Multi-agent systemen  
- Systemen voor Cyber-Physical systems, cloud-computing  
- Digitale productieplanning en roosteringsysteem  
- Bijna real-time productiebeheersingssystemen  
- Digitale uitwisseling van productieplanningsgegevens met toeleveranciers en/of klanten  
- Systemen voor geautomatiseerd management van interne logistiek en orderverzameling  
- Mobiele/draadloze apparaten voor programmering en bediening installaties en machines  
- Technologieën voor veilige mens-machine interactie  
- Digitale oplossingen voor het direct beschikbaar maken van tekeningen, werkschema’s en –instructies op de werkvloer |
| IV | Open Innovation | 11: Hoe vaak heeft uw organisatie vanaf 2012 de volgende activiteiten verricht (Van der Vrande et al., 2009)? |
| IV | Product Innovation | 9.1: Heeft uw bedrijf sinds 2012 producten geïntroduceerd die nieuw waren voor uw bedrijf of die technisch ingrijpend zijn vernieuwd?  
9.3: Bevonden zich bij deze nieuwe producten (nieuw sinds 2012) ook producten, die nieuw-voor-de-markt waren en die uw bedrijfsvestiging als eerste op de markt introduceerde?  
9.4: Heeft uw bedrijfsvestiging producten in het programma die u al langer dan 10 jaar aanbiedt? |
| DV | Industrial Espionage | 7.1: Welke van de volgende maatregelen zijn genomen om het risico van industriële spionage te vermijden in uw bedrijfsvestiging?  
7.2: Heeft uw bedrijfsvestiging te maken gehad met spionage door andere bedrijven, buitenlandse overheidsorganisaties of met verdachte gevallen in de laatste vijf jaar? |
<table>
<thead>
<tr>
<th>Type variable</th>
<th>Construct</th>
<th>Items used from European Manufacturing Survey (2015)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CV</td>
<td>Firm Size</td>
<td>21: Aantal werknemers in 2014?</td>
</tr>
<tr>
<td>CV</td>
<td>Industry</td>
<td>1.2 Bedrijfstak (bijvoorbeeld textiel, chemische industrie, machinebouw etc.)</td>
</tr>
<tr>
<td>CV</td>
<td>R&amp;D investment</td>
<td>18.1: Heeft uw bedrijfsvestiging onderzoek en ontwikkelingsactiviteiten (O&amp;O) uitgevoerd of laten uitvoeren door externe partners in 2014?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18.2: Heeft uw bedrijfsvestiging sinds 2012 continu O&amp;O uitgevoerd of laten uitvoeren door externe partners?</td>
</tr>
<tr>
<td>CV</td>
<td>B2C vs. B2B</td>
<td>1.3: Is uw bedrijfsvestiging gelet op uw hoofdproduct(groep) leverancier van eindfabrinen of een toeleverancier van onderdelen/materialen of bewerkingen?</td>
</tr>
</tbody>
</table>
### Appendix F

**Table F1a.**

*Reliability Statistics construct Digitization*

<table>
<thead>
<tr>
<th>Cronbach’s Alpha</th>
<th>Cronbach’s Alpha Based on Standardized Items</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>.662</td>
<td>.658</td>
<td>13</td>
</tr>
</tbody>
</table>

**Table F1b.**

*Item-Total Statistics construct Digitization*

<table>
<thead>
<tr>
<th>Item</th>
<th>Cronbach’s Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industriële robots voor bewerking en fabricage</td>
<td>.635</td>
</tr>
<tr>
<td>Industriële robots voor hanteren van gereedschap</td>
<td>.641</td>
</tr>
<tr>
<td>Additieve productietechnologie voor maken van prototypes</td>
<td>.649</td>
</tr>
<tr>
<td>Productie met additieve productietechnologie</td>
<td>.659</td>
</tr>
<tr>
<td>Systemen voor Machine2Machine communicatie, Multi-agent systemen</td>
<td>.639</td>
</tr>
<tr>
<td>Systemen voor Cyber-Physical systems, cloud-computing</td>
<td>.655</td>
</tr>
<tr>
<td>Digitale productieplanning en roostering</td>
<td>.648</td>
</tr>
<tr>
<td>Bijna real-time productiebeheersingssystemen</td>
<td>.621</td>
</tr>
<tr>
<td>Digitale uitwisseling van productieplanningsgegevens met toeleveranciers en/of klanten</td>
<td>.632</td>
</tr>
<tr>
<td>Systemen voor geautomatiseerd management van interne logistiek en orderverzameling</td>
<td>.650</td>
</tr>
<tr>
<td>Mobiele/draadloze apparaten voor programmering en bediening installaties en machines</td>
<td>.656</td>
</tr>
<tr>
<td>Technologieën voor veilige mens-machine interactie</td>
<td>.645</td>
</tr>
<tr>
<td>Digitale oplossingen voor het direct beschikbaar maken van tekeningen, werkschema’s en –instructies op de werkvloer</td>
<td>.630</td>
</tr>
</tbody>
</table>

**Table F2a.**

*Reliability Statistics construct Open Innovation*

<table>
<thead>
<tr>
<th>Cronbach’s Alpha</th>
<th>Cronbach’s Alpha Based on Standardized Items</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>.689</td>
<td>.686</td>
<td>8</td>
</tr>
</tbody>
</table>
Table F2b.  
*Item-Total Statistics construct Open Innovation*

<table>
<thead>
<tr>
<th>Item</th>
<th>Cronbach’s Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spin-offs</td>
<td>.690</td>
</tr>
<tr>
<td>Uitgaand intellectueel eigendom</td>
<td>.684</td>
</tr>
<tr>
<td>Werknemersbetrokkenheid</td>
<td>.655</td>
</tr>
<tr>
<td>Klantbetrokkenheid</td>
<td>.656</td>
</tr>
<tr>
<td>Externe netwerken</td>
<td>.628</td>
</tr>
<tr>
<td>Externe participatie</td>
<td>.647</td>
</tr>
<tr>
<td>Uitbesteden O&amp;O</td>
<td>.630</td>
</tr>
<tr>
<td>Inkomend intellectueel eigendom</td>
<td>.667</td>
</tr>
</tbody>
</table>

Appendix G

Table G.  
*Multicollinearity assessment*

<table>
<thead>
<tr>
<th>Variable</th>
<th>VIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>dSuppliertype</td>
<td>1.037</td>
</tr>
<tr>
<td>Digitization</td>
<td>1.265</td>
</tr>
<tr>
<td>IncProductinnovation</td>
<td>1.402</td>
</tr>
<tr>
<td>RadProductinnovation</td>
<td>1.450</td>
</tr>
<tr>
<td>ProductProgram_10yr</td>
<td>1.093</td>
</tr>
<tr>
<td>Number of Open innovation practices</td>
<td>1.221</td>
</tr>
<tr>
<td>I_OpenDig</td>
<td>1.058</td>
</tr>
</tbody>
</table>

Appendix H

Table H.  
*Correlations variables*

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Industrial Espionage</td>
<td>1.000</td>
<td>-.093</td>
<td>.177</td>
<td>.047</td>
<td>.172</td>
<td>.037</td>
</tr>
<tr>
<td>2</td>
<td>Suppliertype</td>
<td>1.000</td>
<td>.123</td>
<td>.059</td>
<td>-.055</td>
<td>-.083</td>
<td>-.003</td>
</tr>
<tr>
<td>3</td>
<td>Digitization</td>
<td>1.000</td>
<td>-.016</td>
<td>.269</td>
<td>.007</td>
<td>-.362</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Inc Product Innovation</td>
<td>1.000</td>
<td>-.441</td>
<td>.190</td>
<td>-.111</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Rad Product Innovation</td>
<td>1.000</td>
<td>.056</td>
<td>-.181</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Product Program</td>
<td>1.000</td>
<td>-.002</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Open Innovation</td>
<td>1.000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Appendix I

<table>
<thead>
<tr>
<th>Subjects theoretical coding</th>
<th>Alternative</th>
<th>Content</th>
<th>Counter aspect</th>
<th>Definition</th>
<th>Deliberation</th>
<th>Evolution</th>
<th>Example</th>
<th>Forms</th>
<th>Future</th>
<th>Improvement</th>
<th>Obstacle</th>
<th>Opinion</th>
<th>Others</th>
<th>Perspective</th>
<th>Position</th>
<th>Purpose</th>
<th>Risk</th>
<th>Tools</th>
</tr>
</thead>
</table>

## Appendix J

### Table x

<table>
<thead>
<tr>
<th>Quotes used in the qualitative analysis</th>
<th>p.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product innovation</strong></td>
<td></td>
</tr>
<tr>
<td>MC2</td>
<td>We zijn nooit de meest innovatieve geweest in helemaal nieuwe, rare dingen op de markt brengen, want we zijn voor de zware inzet, reliable en dependable en vaak als je snel iets helemaal nieuw doet gaat het vaak ten koste van die twee waarden. Als je het snel wilt doen ga je toch ergens kortere dingen doen met je validaties, dat is wel een punt.</td>
</tr>
<tr>
<td>PC1</td>
<td>Dus een dedicated product voor een dedicated klant, samen ontwikkeld. Daar zit de automatisering en digitalisering in de keten.</td>
</tr>
<tr>
<td>CC2</td>
<td>Feitelijk is de hele visie, en ik denk dat de rest van de markt daar ook mee bezig, dat we gewoon een droog product leveren, volledig kant-en-klar, volledig prefab.</td>
</tr>
<tr>
<td>LC1</td>
<td>Je ziet een ontwikkeling in de toename van het gebruik van organische meststoffen, ook in het kader van, niet biologisch kweken maar plantweerbaar, meer gebruik maken van natuurlijk afweersystemen, en minder gebruik maken van kunstmeststoffen.</td>
</tr>
<tr>
<td>CC1</td>
<td>Vanaf nu gaan we de markt op met een nieuw product wat ze in Nederland nog niet kennen, en dat is dat je liftschachten en trappenhuizen in een keer als kant en klare koker neer kunt zetten.</td>
</tr>
<tr>
<td>MC1</td>
<td>Ik denk dat er niet veel ingrijpend verandert, maar wel dat het volume van de meer intelligente aandrijvingen toe gaat nemen. We hebben ze ontwikkeld en op dit moment hebben we ze op de markt en we denken dat de vraag daar naar wel zal gaan toenemen. We zijn wel wat vroeg geweest met het lanceren van die producten.</td>
</tr>
<tr>
<td>TC1</td>
<td>Het product zal niet veel gaan veranderen qua innovatie, maar hij wordt wel een keer overbodig, en dus moet je bezig zijn met de volgende stap, je innovatie moet gericht zijn op wat wordt de oplossing na ons product en wat wordt onze rol daarin.</td>
</tr>
<tr>
<td>MC2</td>
<td>We hebben gezegd dat die innovaties wel moeten leiden tot een lagere total-cost-of-ownership en met die elektrificisering en dat soort dingen, je kunt nu al een grote elektrische heftruck kopen maar die zijn zo duur en unreliable en de kosten van het opereren van zo’n ding liggen zo hoog dat het financieel eigenlijk niet uitkomt.</td>
</tr>
<tr>
<td>TC1</td>
<td>Een trend die je ook ziet, en dat is tegengesteld aan innovatie, een product heeft een gemiddelde levensduur van ongeveer 30-40 jaar afhankelijk van de intensiteit, het makkelijkste is als je hem wilt vervangen dat je hem vervangt met een gelijkssoortige, dan hoef je niet te voldoen aan alle nieuwe wetgeving.</td>
</tr>
<tr>
<td>CC1</td>
<td>Zeker in tijden dat het goed gaat zijn ze maar met één wedstrijd bezig, gewoon geld verdienen, innovatie., dat zal wel. De noodzaak is er dan bijna niet.</td>
</tr>
<tr>
<td><strong>Process innovation</strong></td>
<td></td>
</tr>
<tr>
<td>PC1</td>
<td>Het is niet iets kant en klaars, ik koop niet ergens een pakketje smart industry. Je moet daarin heel veel zelf ontwikkelen, doen, uitzoeken, er is geen kant-en-klare oplossing.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>EC1</strong></td>
<td>Ik denk dat het uiteindelijk voor alle bedrijven wel iets is waar je naartoe moet, als een bedrijf tot een bepaalde grootte groeit kun je het op een andere manier niet efficiënt genoeg inrichten.</td>
</tr>
<tr>
<td><strong>PC1</strong></td>
<td>We werken met ERP systemen, waarin je de hele productieadministratie, je financiële boekhouding, je hele logistieke administratie in bijhoudt. Daarin bewaak je middels het instellen van bestelparameters hoe dat je moet gaan produceren of inkopen. Zonder zo’n ERP-pakket kun je niet produceren.</td>
</tr>
<tr>
<td><strong>MC2</strong></td>
<td>Dat is een heel deel wat sterk in ontwikkeling is, waarbij je steeds meer ziet dat de klant, we hebben een portal waar die data vanaf te halen zijn, klanten willen die data zien in hun systeem, je ziet dat het steeds meer een digitaal service verhaal wordt. Vroeger was het traditioneel sell-and-service, je verkocht iets en iemand anders ging het servicen, nu wordt je letterlijk geconnect met je klant, dat gaat nu heel hard.</td>
</tr>
<tr>
<td><strong>TC1</strong></td>
<td>Waar we bij het productieproces naartoe gaan, nu zie je vaak dat we met tekeningen werken, maar we willen overal touchscreen hebben, waarbij we omdat we zulke specifieke units bouwen, 3D-modellen kunnen draaien, onderdelen wegklikken, maar ook daar de controles in te bouwen, dat die in het systeem worden geadministreerd.</td>
</tr>
<tr>
<td><strong>CC2</strong></td>
<td>Ons hele proces, de backoffice, dat is allemaal gedigitaliseerd, niets gaat meer op papier, hoogstens voor de beeldvorming soms nog wat tekeningen. We tekenen digitaal, het liefst in het model, of tekenen onze schijf en leveren het aan opdrachtgevers zodat die het in het model kunnen clashen en kunnen inpassen.</td>
</tr>
<tr>
<td><strong>MC2</strong></td>
<td>We hebben bijvoorbeeld digital-torque-tooling in het hele productieproces ingebracht, waarbij je precies kunt zien welke bout op welke tork is gezet, en dat kun je altijd weer terug vinden.</td>
</tr>
<tr>
<td><strong>CC1</strong></td>
<td>Er zijn wel diverse bedrijven die met innovatieve activiteiten bezig zijn, bijvoorbeeld 3D printen van beton, daar zijn wij ook een tijd mee bezig geweest maar daar zijn we mee gestopt, we geloven wel dat daar in de toekomst een markt voor is, maar dat is niet de markt voor de bulk.</td>
</tr>
<tr>
<td><strong>Innovation processes</strong></td>
<td></td>
</tr>
<tr>
<td><strong>EC1</strong></td>
<td>We proberen altijd op gebieden waar we de kennis niet hebben geschikte partners te vinden, bij voorkeur de partners die ons al kennen want je bouwt natuurlijk niet voor niets een relatie op, zij kennen ons en wij weten wat wij aan hen kunnen hebben. Waar mogelijk proberen we wel een samenwerking aan te gaan als dat voordelen oplevert.</td>
</tr>
<tr>
<td><strong>MC1</strong></td>
<td>Het is een enorme relatiemarkt, het is niet dat je in 1/2/3 jaar even wat verkoopt, je gaat hele ontwikkeltrajecten samen doen, en daarna ook, de kassenbouw, dat is een hele loyale markt. Je komt er niet zomaar tussen, je raakt ze ook niet zomaar kwijt, je moet gewoon goed met elkaar in gesprek blijven.</td>
</tr>
<tr>
<td><strong>EC1</strong></td>
<td>Een tijd geleden hebben we een nieuwe methodologie ontwikkelt, samen met een smeltbedrijf, daar halen we het zilver en goud voor onze kabels vandaan, voor in onze modellen kabels.</td>
</tr>
</tbody>
</table>
### Qua ontwikkelingen, daar zijn we niet echt op zoek naar externe partijen, dat zit niet in de genen van dit bedrijf.

#### Het is een bedrijf wat erg naar binnen gericht is, en minder naar buiten. Je moet het bedrijf een beetje zien als een bedrijf waar mensen altijd voor de toonbank stonden, als er altijd een rij klanten staat, dan is er minder de behoefte om je op bepaalde aspecten te ontwikkelen.

### Industrial Espionage

#### Ik geloof ook wel in de goedheid van de mens, natuurlijk de rotte appels daargelaten, maar als je mensen deelgenoot maakt van die informatie, en je zorgt dat je het daar met ze over hebt, misschien zelfs belonen bij goed gedrag, dat je veel slimmere werknemers krijgt.

#### De stickers ‘niet fotograferen’ zijn vooral, we hebben een Chinese vestiging, als die overkomen zijn ze vaak met een vliegtuig vol, die lopen allemaal door de fabriek heen, en ze zijn zo hondsbrutaal, ze lopen de werkplekken binnen en fotograferen alle werktekeningen. Ze leggen alles vast, en wat ze er mee doen, en bij wie het terecht komt…

### Relation Product Innovation and Industrial Espionage

#### Dat is een heel deel wat sterk in ontwikkeling is, waarbij je steeds meer ziet dat de klant, we hebben een portal waar die data vanaf te halen zijn, klanten willen die data zien in hun systeem, je ziet dat het steeds meer een digitaal service verhaal wordt.

#### We weten ook praktisch van elkaar hoe we produceren, daar doen we ook niet heel geheimzinnig over, ik nodig ze niet uit, niet van kom eens bij mij kijken hoe het bij mij gaat, zo is het niet, maar ik weet van al mijn concurrenten vanuit de analyse wel wat ze kunnen, hoe ze het doen en wat de zwakkere punten zijn, als ook de sterke punten.

### Interaction Digitization and Open Innovation

#### Stel de machine hangt aan het netwerk, en aan het netwerk van de klant, en iemand breekt in onze machine via het netwerk en komt zo binnen in het netwerk van de klant en legt het hele warehousemanagementsysteem van de klant plat…

### Other memorbale quotes

#### Correct, je moet gewoon zorgen dat je sneller en efficiënter bent in je hele proces, dat is vaak moeilijker te kopiëren dan een product of software. De cultuur van de organisatie, je dealernetwerk, dat soort dingen (MC2).

#### De beste bescherming is dat je voorop blijft lopen in je branche, blijf innoveren, blijf voorop lopen, en zorg dat je als innovator bekend staat, dan houd je de koploperspositie vanzelf. Natuurlijk loop je risico.
| MC1 | Door spionage kun je een stukje kwijtraken, maar het is het totale pakket wat ons succesvol maakt in de markt en dat is niet te kopiëren. | 75 |
| MC1 | Spionage hebben wij nooit meegenomen als besluitcriterium voor innovatietrajecten. Wel dat we proberen kennis in huis te houden, dus af te schermen, dat het niet lekt, maar echt spionage nee… Het is ook niet zomaar te kopiëren en de relatie met je klant, de markt, het product, een product kun je kopiëren, we hebben een Turkse concurrent die een gelijkwaardig product maakt, echt een geweldig product, maar hij heeft niet de relatie die wij hebben met onze klanten, heeft niet de marktkennis, heeft niet het distributienetwerk wat wij hebben, en dat is essentieel om succesvol te zijn in de wereldmarkt. | 75 |
Appendix K

Research Integrity Form – Master Thesis

<table>
<thead>
<tr>
<th>Name:</th>
<th>Student number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jasper Haen</td>
<td>s4147596</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RU e-mail address:</th>
<th>Master specialization:</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:j.haen@student.ru.nl">j.haen@student.ru.nl</a></td>
<td>Strategic Management</td>
</tr>
</tbody>
</table>

Thesis title: Digitization of manufacturing processes, a must, but also a Trojan horse?

Brief description of the study:
Stories of industrial espionage are as old as the industries themselves. The different stories arise from changes in technological developments, societal happenings, and from products to manufacturing processes. A recent development, the ongoing digitization of manufacturing processes, Industry 4.0, is an example of a series of technological developments that might result in new stories of industrial espionage, as it might increase firms’ attractiveness (to be spied on) and vulnerability. This, and other forms of innovation added together, could give insights regarding why firms become targets of industrial espionage, with all the associated consequences.

To find insights regarding these aspects, this research focused on the relationships between innovation forms and the probability of becoming a target of industrial espionage. A mixed-methods study was conducted, using data of the European Manufacturing Survey 2015 to conduct a logistic regression, combined with semi-structured interviews to investigate the content of the assumed relationships. A distinction was made between several forms of innovation, namely: product innovation, digitization of manufacturing processes (process innovation), and open innovation (innovation process). One finding is that if firms innovate their product incrementally or radically, the probability of becoming a target of industrial espionage respectively triples or almost quadruples. Also, the digitizing of manufacturing processes increases this probability. The results of this research not only have theoretical implications, but are also useful for firms facing strategical considerations regarding innovation forms. The findings together with the suggestions for future research will help to understand and extent the body of literature about industrial espionage and its relation to innovation.

It is my responsibility to follow the university’s code of academic integrity and any relevant academic or professional guidelines in the conduct of my study. This includes:

- providing original work or proper use of references;
- providing appropriate information to all involved in my study;
- requesting informed consent from participants;
- transparency in the way data is processed and represented;
- ensuring confidentiality in the storage and use of data;

If there is any significant change in the question, design or conduct over the course of the research, I will complete another Research Integrity Form.

Breaches of the code of conduct with respect to academic integrity (as described / referred to in the thesis handbook) should and will be forwarded to the examination board. Acting contrary to the code of conduct can result in declaring the thesis invalid.

Student’s Signature: Date: