

A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from the bar, containing the date.

3/26/2023

Internationalization under national restrictions

Data confidentiality in the case of the Dutch defense domain

Several thin, curved lines in shades of blue and grey originate from the bottom left and sweep upwards and to the right.

L.P.J. van Kan - Janson

EXECUTIVE MASTER IN CUSTOMS AND SUPPLY CHAIN COMPLIANCE

As ~~protected~~ as possible; as ~~open~~ as necessary.
open protected

Thesis for the executive Master in Customs and
Supply Chain Compliance (MCSCC)

Date:	March 26 th , 2023
Author:	Loes (L.P.J.) van Kan - Janson
Student nr:	477105
Academic supervisor:	Rob Zuidwijk
Co-reader:	Ruud Tusveld
Version:	Final version research report
University:	Rotterdam School of Management Erasmus University

NOTE

This document does not contain any classified information.

This document is not export controlled.

This document does not contain any confidential information on the protection of state secrets by industry participants.

This document does not describe any contact details, nor any agreements made by industry participants with the Dutch Ministry of Defense or any other Dutch government institutions.

This research was done independently of any company or government institution. This document solely represents the views and opinions of the author, and does not necessarily reflect the opinion of one specific company/industry participant, nor that of the Dutch government.

This document and parts thereof may not be copied, reproduced, distributed, published, modified, transmitted or in any way exploited, except with the expressed prior written permission of the author.

1. Executive summary

In a world where digitalization has become the norm rather than the exception, security threats can no longer be mitigated by physical measures only. In fact, the future of supply chains is dependent on technological developments of digitalization. Data security is central to the existence of supply chains as a whole, and it is thus essential to protect vital data. However, protection also has its downsides. Implement too many protective measures, and it hinders developments; companies would no longer be able to function.

This thesis describes the qualitative research done on an extreme case of the need for data protection: protecting the confidentiality of government classified information. Such information is occasionally shared with defense industry companies, who are held to protect it against unauthorized access by remaining compliant with pre-set national rules. As any cross-border interaction increases the threat to data security, defense companies particularly feel an impact on their operations of these data confidentiality rules when operating internationally.

By means of a single case study of the Dutch defense industry and making use of interviews held with industry companies as well as with Dutch government representatives, the following research question was investigated:

“How can the impact of the restrictive nature of government-imposed data confidentiality rules, on a defense firm’s sourcing of international knowledge and skill, be minimized?”

It must be stressed that this research does not pass judgement on the content and extent of the government-imposed data confidentiality rules. On the contrary: such rules are indispensable for the security of Dutch citizens and government, as well as for the protection of the defense companies themselves. However, actions can be proposed which may reduce the experienced impact without changing the rules and compromising data security.

This impact experienced by the defense industry, seems to be coming primarily from the time that is needed to obtain government authorizations on international sourcing, such as recruitment of-, or incidental assistance by non-Dutch nationals, and international outsourcing. Due to these time constraints, an impact is experienced on the quality delivered to the client, namely project delays, not being able to offer the latest available technologies, and a higher cost than would be the case in the non-defense industry. This by itself also leads to a loss of market opportunity for defense companies, and a potential loss of the knowledge position of the Netherlands on the international market with regard to defense technologies. Although time seems to be the main driver of the experienced impact, the amount of work that is needed to remain compliant with the rules may be self-evident, but does also have an impact on the industry due to the required capacity in staffing, costs for trainings and IT systems, and finding solutions for processes which are normal for other industries but restricted in the defense industry, such as teleworking or using cloud-based solutions.

One of the main causes of these difficulties is found in a complex organizational structure, both on the industry side as well as on the government side. When decisions are taken, multiple departments are involved which all have their own interests and motivations. The defense industry companies receive information from various government actors; the department responsible for supervision of compliance with the rules is different from the department deciding the required level of protection. From the organization chart of the government, as well as from the interviews, we can derive that these departments may not have short communication lines, and thus data may be overclassified. Furthermore, the interviewees indicate that there is often a lack of understanding of the rules. The complexity also adds to the compliance burden when multiple security regimes are applicable to the industry. Compliance with the rules is a “license to operate” for the defense business, which translates to a systematic risk, generally causing a behavior of risk aversion. There are indications that the abovementioned causes and the risk averse behavior are leading to overcompliance by the industry, which, according to literature, can be a reaction to extensive communication with the regulator, particularly if there are high volumes of information, or if the information is ambiguous.

Thus, the most feasible recommended action is for the industry to bring together experts from various departments and with different areas of responsibility, to review existing procedures and eliminate “Red Tape”; unnecessary and inefficient rules and procedures. Furthermore, it is proposed for the government to make bilateral agreements (General Security Agreements and Memoranda of Understanding) more accessible to the industry, for example by publishing lists or guidance. These agreements can facilitate internationalization, if the industry makes use of these agreements when rolling out recruitment strategies or when taking decisions with regard to outsourcing.

Other recommendations seem feasible only on the longer term, but also seem more likely to have a more permanent positive effect on reducing the impact for the industry. Such recommended actions include an efficiency improvement at the government side for security screenings, by moving away the screening operations from the intelligence agency and towards a department with more capacity and less expertise requirements in the area of intelligence services. For industry companies, a long-term action which is proposed is to implement “compliance by design”, for example by designing products in such a way that they are, in basis, not containing any classified information and are thus not subject to the restrictions. Compliance by design can also be implemented by firms which are relatively new, by taking into account the data confidentiality rules from the start in the design of their IT systems, so that the company is already compliant at the moment of considering a defense-related bid.

Overall, it can be said that both industry and government are advised to carefully assess which data needs protection, and protect only that portion of data which is necessary. In short: to operate in a way that is as open as possible, and as protected as necessary.

Table of Contents

NOTE	2
1. Executive summary	3
2. Preface	8
3. Introduction	9
3.1 A boy from India	9
3.2 Problem analysis: data security in a digital world	10
3.3 A fragmented approach.....	11
3.4 Research objective.....	11
4. Research design, structure and methodology.....	12
4.1 Conceptual model.....	12
4.2 Research questions.....	14
4.3 Methodology	14
a. Qualitative research	15
b. The case study	15
c. The interviews	16
d. The literature review	18
5. Defense data confidentiality and international sourcing.....	19
5.1 About (defense) data confidentiality rules.....	19
a. Unauthorized access.....	19
b. Standardization of defense security measures	20
c. Classification of data.....	20
5.2 About the (Dutch) defense industry.....	21
a. An uncertain market.....	21
b. The effects of sovereignty	22
c. State support	22
5.3 About sourcing international knowledge and skill	23
a. Need for internationalization	23
b. Outsourcing, increasing internal capacity, and insourcing.....	23
5.4 Conclusion literature review	24

6. The impact of data confidentiality rules.....	26
6.1 Experienced impact of government-imposed data confidentiality rules.....	26
a. Loss of quality for clients.....	28
b. Loss of market opportunity.....	31
c. Increased amount of work.....	31
d. Conclusion.....	32
6.2 Analysis of causes of the experienced difficulties.....	33
a. Governance.....	33
b. Confidentiality rules.....	37
c. Capacity and agreements.....	39
6.3 Conclusion: causes and effects.....	42
7. Overcoming the difficulties.....	44
7.1 Overcompliance and risk aversion.....	44
7.2 Skilled Dutch nationals.....	47
7.3 Complicated organizational structure.....	48
7.4 Politics.....	50
8. Conclusion and recommendations.....	52
8.1 Conclusion.....	52
8.2 Recommendations for minimizing the impact of data confidentiality rules.....	53
8.3 Limitations of the research.....	56
8.4 Contributions for research and practice.....	57
8.5 Recommendations for future research.....	58
9. References.....	59
Annex I: Interview protocols.....	62
Annex II: Thematic map.....	64
Annex III: ABDO rules related to foreign resources.....	65
Annex IV: World map of GSA's of the Netherlands.....	67

List of Tables and Figures

Figure no.	Description	Page number
1	Environment of the Conceptual Model	13
2	Conceptual Model	13
3	Number of ABDO Security Rules	27
4	ABDO Rules Related to Foreign Resources	27
5	Experienced Difficulties leading to Concerns on the Quality for Clients	30
6	Organization Chart of the Dutch Ministry of Defense	34
7	Causes and Effects of Data Confidentiality Rules	42

Table no.	Description	Page number
1	Interviewees	17
2	Comparison between GSA's of the Netherlands	41

2. Preface


This thesis is written for the executive master in customs and supply chain compliance. It is meant to give customs- and supply chain professionals an insight in the manner of protecting the world's most-wanted information: classified government information.

Writing this thesis has been an interesting journey, both personally as well as professionally. Although I have a background in export controls, sanctions and customs, I've only become more convinced that the topic of data security is essential to comprehend, particularly when working internationally. I believe that export control- and customs compliance is more effectively achieved when having knowledge of the security concerns that go hand in hand with cross-border transactions.

Throughout this research I have come across various recent quotes which assured me that the topic of this thesis is relevant today in various ways. These quotes I have added to the start of the chapters, and I hope they give you, the reader, the inspiration and deeper understanding as they did for me.

I would like to thank my employer for being so supportive, and for having given me the inspiration to choose a thesis topic in the security domain which is in so many ways complementary to the trade compliance domain.

This thesis would not have seen the light of day without the helpful and comforting suggestions made by my supervisors, Rob Zuidwijk and Ruud Tusveld. For the contents, I'm very grateful for the useful insights provided to me by all of the interviewees, who spent their precious time on answering all of my questions, both during the interview as well as the follow-up questions. A special thanks to Mr. Henk Schutte, for inspiring such an interesting topic, and to Mr. Pieter Cobelens, for going through the trouble of meeting me personally and providing me with some additional useful insights from the government point-of-view. Finally, I would like to thank my friends and colleagues for showing such an interest in the topic and in my progress of the research, and of course a big thanks my family – you have truly stimulated me throughout this whole course and I could never have completed it without you.



2-4-2023

3. Introduction

“Not least due to different national requirements, the security and defence industry in the EU still has a strong national focus and remains highly fragmented. “...” In many cases, this leads to considerable disadvantages in terms of expenses, international competitiveness and cooperation.” *Strategy Paper of the (German) Federal Government on Strengthening the Security and Defense Industry.*

3.1 A boy from India

It is the year 1952. A 16-year old boy named Abdul emigrates from India to Pakistan with his parents. A technical university study eventually brings him to Europe, where he studies for eleven years at universities in Berlin, Delft and Louvain. During these years, he also falls in love and marries a woman from South-Africa who is fluent in Dutch. In 1972, he is promoted and starts working for the Physical Dynamics Research Laboratory in the Netherlands, for which he easily passes the required government security screening due to his experience in Europe and his Dutch-speaking wife. The laboratory works for Urenco.

Urenco is a facility in the Netherlands where uranium is enriched for nuclear reactors. In such reactors, chain reactions of nuclear fissions (splittings) provide heat, which can be used for creating electricity. Only one element found in natural uranium can be split, namely U-235, but the amount of U-235 found in natural uranium is too small to sustain the chain reaction needed. Therefore, natural uranium is enriched using a special process. Not much U-235 is needed for the chain reaction to create electricity, but with enough U-235, the chain reaction can be so strong that nuclear weapons can be made with it.

In 1975, Abdul Khan does not return from a holiday in Pakistan. It is later found that he has spent several years taking confidential documentation from Urenco home, to make copies and to have his wife translate the documents from Dutch. This information was all forwarded to Pakistan, which used it to build its own copy of the Urenco factory, and by 1980, was able to produce highly enriched uranium for making their own nuclear weapons (Rosenkranz, 2017).

Some say the Netherlands purposely allowed the export of this sensitive data to Pakistan. Others say it was a grave mistake, and even worse, that Pakistan later forwarded the information to Iran and North-Korea. Whatever the case, this true story makes it painfully clear that sensitive information needs to be protected from threats on the outside, as well as on the inside.

3.2 Problem analysis: data security in a digital world

In the 1970's, physical data protection measures would suffice for keeping sensitive information safe. In the digital world of today, that is no longer the case. The future of manufacturing in Europe lies with several game-changing technologies (Eurofound, 2019), such as advanced industrial robotics, additive manufacturing and industrial internet of things. In these digital technological developments, use of data is a central aspect. Furthermore, Eurofound points out that these new technological developments will require new skills, as well as significantly deeper and advanced skills, mainly in the high-end technical areas such as engineers, data scientists and data security analysts.

Not just the manufacturers by themselves are subject to technological developments; digitalization is also growing in international supply chains as a whole (World Customs Organization, 2018). The WCO calls for countries to establish customs IT systems which allow the secure sharing of data, which is then timely available, of high quality and integer. By being able to use such trustworthy data, all parties in the supply chain could benefit from less impact by customs controls, and a stronger focus of the authorities on the most important security risks such as terrorism. According to the WCO, countries should co-operate with other countries in order to achieve such benefits.

We can thus conclude that data security is central to the existence of (high-tech) manufacturers, as well as to the supply chain as a whole, and that it is therefore essential to protect vital data.

However, there is also a flip-side to data protection. Protecting anything too much would hinder developments, it would mean a company can no longer function. Determining which level of protection is sufficient, but not too much, is essential for the continued existence of high-tech manufacturing companies.

In most circumstances, the extent of data protection measures is a choice of the company itself. However, in some cases, it is required by an external party. In the financial industry for example, it is the Dutch Central Bank which prescribes a framework for risk monitoring, called the Systematic Integrity Risk Analysis (DNB, 2015). Their motto is: "more where necessary, less where possible". Another good example is the defense industry, where classified government data, like the data stolen from Urenco in the 1970's, must be protected.

3.3 A fragmented approach

Similar to the reason for the WCO to call upon countries to co-operate in achieving “safe” IT systems for sharing data, the defense industry struggles with a fragmented approach to data security. Defense is a national competence, meaning that rules governing the protection of sensitive defense or military information is governed by national law. Even so, the need for protecting such data is extreme, as unauthorized disclosure can have catastrophic consequences to national safety. Data protection, for a defense firm, is a license to operate.

Although all firms must abide by national data protection laws, the multinational companies must remain competitive on an international level in order to keep making a profit. Competition in high-tech companies is on the level of technical advance, and price. In order to maintain a competitive strategy, these firms have a need for international co-operation. Furthermore, as mentioned by Eurofound, there is a rapidly increasing need for personnel skilled in IT. Such personnel is often found across country borders; in the Netherlands this trend has been very clear with a 45% increase between 2010 and 2020 of non-Dutch personnel in Dutch firms (CBS, 2022).

3.4 Research objective

The need for data security, especially data confidentiality, is topical for all entities in a supply chain. Some require it for protecting their intellectual property, some for participating in safe trade lanes, and others for protecting (financial) data of their clients. However, most of these companies also require some degree of internationalization. Whether it is through international co-operations, through hiring non-Dutch personnel, or by other means, any cross-border aspect increases the threat to data security as evidenced by sources such as the WCO guidelines, the Eurofound report, or even the case of Abdul Khan.

This research will look at the actions which can be taken to ensure data confidentiality of sensitive information, while making use of the much needed international knowledge and skill. It will point out which issues can be experienced when applying data confidentiality measures which are as strict as those required in the defense industry. It will also point out which causes are at the source of these issues, since the cause can also be found in the manner of implementation rather than in the legislation. Finally, it will suggest some actions that can be taken, either by the industry or by a rule-setting entity such as the government, in order to facilitate the industry without risking data confidentiality breaches.

The next chapter will describe how the research is designed in order to reach this research objective.

4. Research design, structure and methodology

“Foreign powers are, amongst others, trying to penetrate ministries, investigation- and safety agencies, political parties, international organizations and cultural-social organizations. “...” Various state actors are capable of, and possibly have the intention to harm the Dutch national security.” *Advice from Dutch intelligence agencies on the bill for extending the punishability of espionage, 16 december 2022, annex to explanatory memorandum no. 36280. Translated from Dutch*

In this research, as mentioned in the previous chapter, we will look at the impact of data confidentiality rules on the ability to use international knowledge and skill, and what is needed in order to reduce this impact without compromising the much-needed security of classified information. This chapter describes amongst others the design of the research, the chosen methodology, and the used data.

4.1 Conceptual model

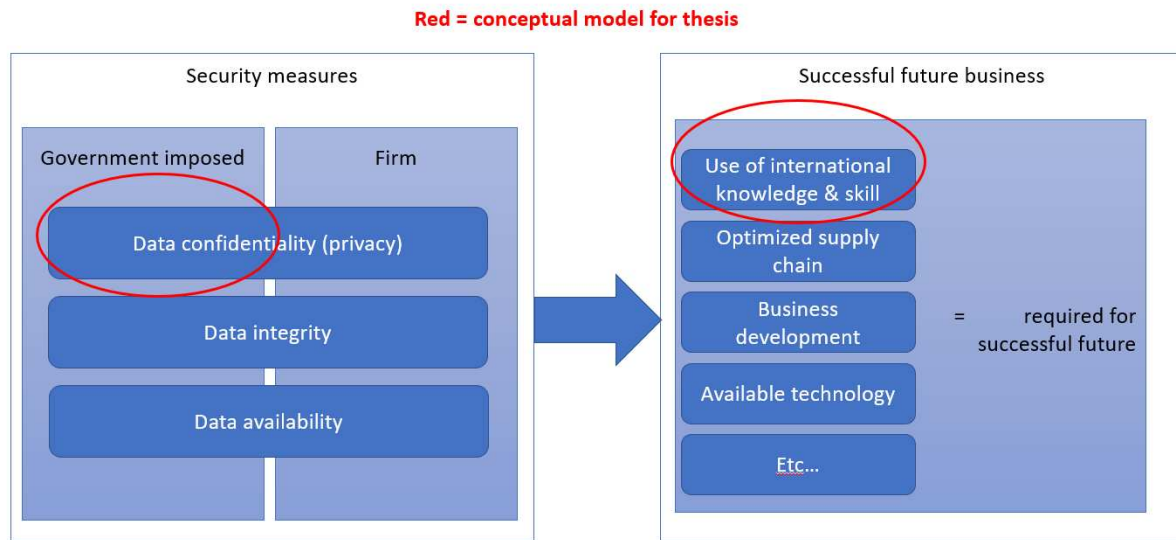
This research is done through a single case study. The case is confidentiality of classified data in the Dutch defense industry. From the choice of case study, it follows that the research design is based on the Dutch defense industry. Literature study is needed with the focus on the defense industry in Europe, since that provides more insights than just focussing on the Netherlands. The European Union has similar legislation on the topic of securing government classified data, therefore literature concerning the European Union can be applicable.

Governments benefit from having a national defense industry, and national defense manufacturers, just like they benefit from having multinational manufacturers from other types of industries. This is beneficial for employment possibilities, the national knowledge base and the possibility to develop and acquire defense products which are not already owned and known by other countries.

However, due to their nature, defense firms experience more nationally imposed restrictions in their entrepreneurship than most other types of business. Certain factors which are needed for the growth and development of the defense industry are complicated due to the confidential nature of the data and technologies. As mentioned earlier in this chapter, one of these factors in the Netherlands is the use of international knowledge and skill, for example through hiring non-Dutch employees or through multi-national co-operations.

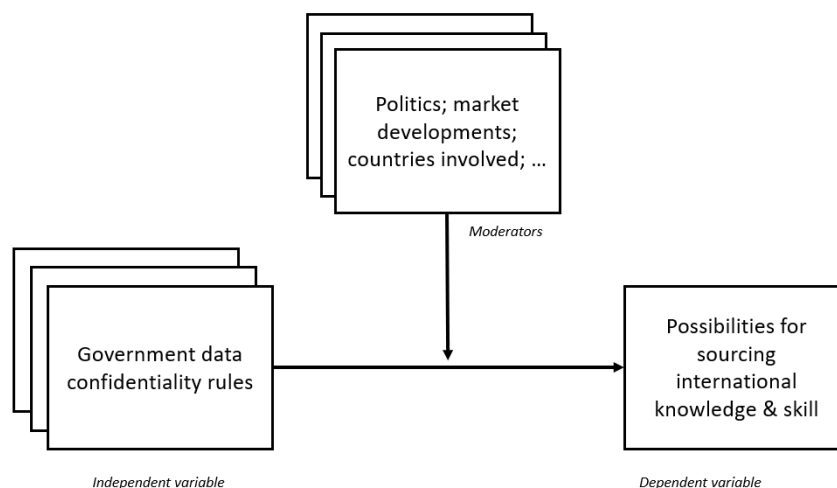
In this research, we look at the impact of nationally imposed security rules on the ability to use that international knowledge and skill. Security measures in the defense industry can be government-imposed or self-imposed, and can be aimed at data confidentiality, data integrity or data availability. As shown in the conceptual model displayed in figure 1, this research specifically looks at government-imposed data confidentiality security measures.

FIGURE 1
Environment of the Conceptual Model



The conceptual model is derived from this model, as shown in the below figure.

FIGURE 2
Conceptual Model



From the conceptual model, it follows that the main research question is:

“How can the impact of the restrictive nature of government-imposed data confidentiality rules, on a defense firm’s sourcing of international knowledge and skill, be minimized?”

4.2 Research questions

The main research question is comprised of various elements, some of which need clarification and some of which need a further deep-dive before being able to provide a full answer.

First, clarification is needed for the elements “government-imposed data confidentiality rules” and “sourcing of international knowledge and skill”. Once it is clear in which way these elements should be interpreted, we will be able to deep-dive into the restrictive nature, by finding out which restrictions are actually experienced. These restrictions do not necessarily have a significant impact on the operations of a defense firm, thus it is necessary to find out which impacts are experienced by the industry. Then, in order to provide an answer to the question how such impact can be minimized, we need to identify the source of the impact. The source could indeed be the factual government-imposed data confidentiality rules, but possibly also other sources can be indicated. Finally, using the outcomes of the previous answers, it will be possible to identify potential actions that can be taken to overcome the difficulties.

Therefore, the following subquestions are posed:

- What are the (government) data confidentiality rules?
- How do companies source international knowledge and skill?
- What impact of the data confidentiality rules is experienced by the defense industry?
- What are potential causes of this impact?
- What are potential recommendations for overcoming these difficulties?

4.3 Methodology

As mentioned earlier in this chapter, this research is done through a single case study of data confidentiality in the Dutch defense industry. This paragraph describes the steps taken in this research, and the methodology which was applied.

The research aims at assessing the impact of government data confidentiality rules on a defense company’s possibilities for sourcing international knowledge and skill. The research also will explore which attributes could indeed moderate the impact. For example: politics, market developments, countries involved, etcetera. From this knowledge, we will be able to understand better how the defense industry can be facilitated, without risking data confidentiality breaches.

a. Qualitative research

In 2020, a Dutch investigative journalist published the book: “There’s a war going on, but no one can see it”. The book describes how the Dutch national security agencies (NSA’s) have been fighting digital attacks on national security, and reconstructs several espionage operations by Dutch and other government authorities. The book reveals the enormous sensitivity of the topic; the writer continuously describes his difficulties in finding sources, and the unwillingness of these sources to disclose anything.

This is also a difficulty that is encountered during this research, as will also become clear from the literature review in chapter five. Not much literature is published on the protection of classified state secrets. After all, if the adversary knows exactly how information is protected, they can also find out how to access it.

This research is therefore a qualitative, exploratory research. Qualitative research is most appropriate when explaining “social events as experienced by individuals in their natural context” (Malterud et al., 2001). Exploratory research, as opposed to descriptive or explanatory research, is most appropriate to find out “what is happening”, to “seek new insights” or to “assess phenomena in new light” (Saunders et al., 2009). The outcome of exploratory research is dependent on the position and interest in the research of the researcher (Reiter, 2017).

In this light, it is important to acknowledge that this research is performed by an employee of a multinational defense manufacturing firm in the Netherlands. Due to this fact, there can be biases or shortcomings in understanding when only using data from within the firm itself. Triangulation is therefore necessary, as described in section c of this paragraph, by making use of data from various stakeholders. This includes the firm, the government supervising authority and the government policy maker.

b. The case study

The defense industry designs, produces and maintains products for the military (naval, land and air forces) of governments. In doing so, information about the products employed by the government military often needs to be shared with the industry. This information is in essence the intellectual property of the government, and must therefore be protected against unauthorized access. If such information ends up in the wrong hands it can cause political unrest, set military operations up for failure, harm governments, or even be a threat to society as a whole. Thus, maintaining data confidentiality is indispensable.

Although case studies are useful in exploratory research (Dul et al., 2008), accessibility to data is necessary in order to conduct a good case study. Case studies can help understand a topic when not much is known. Case study as a research approach is appropriate for practice-oriented, exploratory research, to describe or explain a phenomenon with possible recommendations (Nikulina, A., 2022). In particular, a case study is interesting here because it allows to study data confidentiality rules in a new empirical setting, namely the application of the rules to the defense industry. It is new, because very little literature exists on this specific topic. The case of data confidentiality in the defense industry is, compared to other industries, an extreme case for the need of data confidentiality.

This case study is performed at a macro level of analysis, namely at the industry level within one country. Within this case study, the meso level of analysis is also taken into account, looking at how companies within the industry have implemented certain government-imposed rules. The case study belongs to the broader class of data security phenomena. However, the research will be limited to the defense industry in the Netherlands.

Case studies rely on multiple sources of evidence. In this case study, the main source is data obtained from interviews as described in the next section. Furthermore, data was obtained from published government documents, such as transcripts from the House of Representatives ("*Tweede Kamer*") and General Security Agreements. Finally, data is obtained through personal observations of the researcher, employed at a defense firm and communicating with other defense firms. This observation regards the way in which confidentiality rules on classified data are being implemented in defense firms.

c. The interviews

A deeper understanding of the case can be reached by making use of interviews. Interviews are a good way of collecting in-depth data in an exploratory research setting (Jain, 2021). Interviews offer the chance to ask probing questions and to get into more depth on the topic, depending on the knowledge and experience of the interviewee. It allows the researcher to ask additional questions in order to better understand the context, and also allows the researcher to provide additional explanations during the research in order to ensure that the questions are well-understood by the interviewee. The interviewees are listed in table 1.

TABLE 1
Interviewees

Organization	Role	Interview type	Duration
Manufacturer	Security director	Face to face	40 min.
Manufacturer	Business development director	Online	41 min.
Manufacturer	Technical director	Online	52 min.
Manufacturer	Trade compliance director	Online	46 min.
Government	Intelligence services	Face to face	70 min.
Government	Security authority (policy maker)	Online	63 min.

Triangulation is achieved by interviewing persons with a different objective: the manufacturers wish to comply with the legislation while not missing out on (international) business opportunities; the intelligence services who are responsible for conducting the audits at the manufacturer's site wish to get a true impression on the level of security at the manufacturer's site, and the security authorities, who are responsible for the Dutch security policy, are solely concerned with ensuring the safety of government classified data, regardless of the cost. Persons from several large manufacturers with a Dutch presence were interviewed in order to reduce chance of bias from using only one company.

The interviews are semi-structured, however, different interview protocols are used based on the interviewee's position, knowledge and interests. The interview questions are aimed at collecting data about:

- Determining the purpose of the data confidentiality restrictions, and
- Translating the restrictions to safety measures taken by the organization.

The generic interview protocols are included in annex I.

The interviews are all recorded. Because of the exploratory nature, the answers provided by the interviewees often contain elements which are interesting in multiple ways. Therefore, recording was essential in order to capture all these elements. In some of the interviews, sensitive data has been shared that the interviewee requested would not be published. Therefore, as a safety precaution, the recordings have been transcribed by hand, without the use of any software. Those parts which should remain confidential, have not been transcribed, but do add globally to the understanding of the researcher.

The interviews were subsequently analyzed.

Thematic analysis is an appropriate method for identifying, analyzing and reporting patterns within data (Braun & Clarke, 2006). Thematic analysis is a useful method for this research study which is exploratory, because it interprets the various aspects of the topic allowing the possibility to discover new information from the data. The six steps suggested by Braun & Clarke were used in order to perform the thematic analysis.

The purpose of the analysis in this research is to provide a rich description of the entire data set, which is useful because the Dutch defense industry can be considered an under-researched area as the literature review will point out. Themes were first identified in an inductive manner, in order to allow new aspects to be discovered. All interviews were divided into quotes by hand, in excel, without the use of software in order to preserve confidentiality. Each quote was assigned with a code which was not necessarily linked to the initial research question. Some quotes needed multiple codes, in this case the quote was copied and the copy identified with a number to indicate to the researcher that they were assigned multiple codes. Initially, a total of 362 quotes from 6 interviews were coded with a total of 40 different codes. Then, a combination of induction and deduction was used in order to identify the final themes. Additional codes were added to provide a basis for answering the research questions.

The themes and (primary) codes were converted into a thematic map. The thematic map is included in Annex II.

d. The literature review

This research starts with a review of the research literature, which is described in the following chapter.

This review will already provide an answer to the first two subquestions. The natural start of this review is to focus on the independent variable, being the data confidentiality rules. This is useful, since this research question is a case that can be generalized in compliance with data confidentiality rules which can be a struggle for companies and institutions regardless of their sector. Furthermore, the research literature has been explored on the topic of the defense industry, in order to gain a better understanding of the nature of the defense-industry related restrictions and difficulties. In the literature regarding the defense industry, we can also find indications for potential moderators. Finally, the literature needed to be explored on the topic of the dependent variable, being the sourcing international knowledge and skill. This is necessary in order to formulate useful interview questions and to understand the extent of the possible impact on this variable.

5. Defense data confidentiality and international sourcing

"I must be brutally honest with you, Europe isn't strong enough right now. We would be in trouble without the United States "... We have to make sure that we are building [those] capabilities when it comes to European defence, European defence industry." Sanna Marin, Prime Minister of Finland, Dec. 2nd 2022, speech at the Lowy Institute, Australia.

In this chapter, we will explore the three main subjects of the research question: the meaning and extent of data confidentiality rules (independent variable), the particularities of the defense industry as opposed to other types of industry (moderators), and the various ways in which international knowledge and skills can be applied to the operations in the defense industry (dependent variable). We will explore the way in which the conceptual model, as described above, is positioned with respect to the existing body of knowledge by exploring three streams of literature, namely data confidentiality in paragraph 5.1, the Dutch defense industry in paragraph 5.2, and the sourcing of international knowledge and skills in paragraph 5.3.

5.1 About (defense) data confidentiality rules

First and foremost, the research question looks at data confidentiality rules as they are applied in a particular circumstance. What are data confidentiality rules and what is their role in the defense industry domain?

a. Unauthorized access

As international trade increases, trade controls today mostly rely on administration by IT systems. Such systems must be reliable in order to be a useful data source for trade controls. According to Romney and Steinbart (2019), systems reliability is based on five principles: confidentiality, privacy, processing integrity, availability and (overall) security.

One of these principles, confidentiality, assures that sensitive organizational information is secured against unauthorized access. The Dutch General Security Requirements for Defence Contracts define confidentiality as: "The safeguard that information is only accessible to those authorized". Whereas assuring the confidentiality of (trade related) data can already be a difficult task when the data remains within the company, the difficulty only increases when exporting such data across borders. As indicated by Eichler (2018), an "export" not only includes shipments of hardware, but can also include sharing of information.

b. Standardization of defense security measures

In their research, van der Linden, Kalra, Hasman and Talmon conclude that when sharing information across organizations and borders, a global standardization of security measures, as opposed to organizational measures, is required. In the area of data security, international agreements and treaties are established. For example, the EU has an agreement with the UK concerning security procedures for exchanging and protecting classified information. Such agreements also exist bilaterally, in the form of General Security Agreements (GSA's) or Memoranda of Understanding (MoU's). When looking at which countries are likely to be a part of such treaties or agreements, we find that civil-law countries are more likely to ratify treaties than common-law countries (Klomp & Beeres, 2021). However, Klomp and Beeres do point out that this does not take into account the actual national implementation of the treaties, which in some cases might not be adequate. Thus, civil-law countries are more likely to agree with setting common measures.

From the fact that such agreements are necessary, it follows that countries do not handle data confidentiality in the same way. A practical example of this can be found in the General Data Protection Regulation (GDPR), which went into effect on May 25, 2018. Although the GDPR applies to all (legal) persons in the EU, the protections of personal data in the United States are in general not compliant with European rules (Draghia et al., 2018), despite the failed efforts by the US Commerce Department and the European Commission of creating a EU-U.S. Privacy Shield. Thus, even NATO countries have different confidentiality standards.

For the Dutch defense industry, this standardization is realized through the ABDO, the general security requirements for defense contracts. These requirements are set, maintained and updated every few years by the BA, one of the two Dutch security agencies (*beveiligingsautoriteit*), and implemented through the MIVD, the Dutch military intelligence agency, which is a part of the ministry of Defense. They are based on the VIRBI, the Civil Service Data Security – Special Information Regulation, where the rules for security of special information for the government are laid down. The VIRBI itself is further detailed in separate security policies for each Dutch ministry. The government itself is thus not held to the ABDO, which is only made applicable to legal persons when they enter into a contract involving special information with the ministry of defense.

c. Classification of data

In order to assure data confidentiality, various authors have indicated the importance of classifying data by importance, and limiting access to sensitive data (amongst others: Louwers & VanDenBurgh, 2003). Classification of government sensitive data is, in most countries, achieved by markings in three or more importance levels. Council decision no. 2013/488/EU acknowledges the following levels:

- EU Top Secret: information and material *the unauthorized disclosure of which* could cause exceptionally grave prejudice to the essential interests *of the European Union or of one of the Member States*;
- EU Secret: information and material (...) could seriously harm the essential interests (...)
- EU Confidential: information and material (...) could harm the essential interests (...)
- EU Restricted: information and material (...) could be disadvantageous to the interests (...)

The Netherlands makes use of the same levels, as laid down in the VIRBI:

- Stg. ZG/Staatsgeheim Zeer Geheim/TBB1 : *when unauthorized disclosure* could cause exceptionally serious harm to one of the vital interests of the State or its allies;
- Stg. G/Staatsgeheim Geheim/TBB2: (...) could cause serious harm to one of the vital interests of the State or its allies;
- Stg. C /Staatsgeheim Confidentieel/TBB3: (...) could cause harm to one of the vital interests of the State or its allies;
- Dep.V/Departementaal Vertrouwelijk/TBB4; (...) could cause harm to the interests of one or more ministries.

In the Netherlands, ABDO directs the defense industry for each of the four levels of confidentiality the extent of security measures required in specific areas. A distinction is made between measures for physical and for digital security.

5.2 About the (Dutch) defense industry

This chapter started with a statement by the Prime Minister of Finland just last year, stressing that Europe invest in its own defense industry. She is certainly not alone in these ideas. In January 2023, the Dutch Financial Times published an article in which it becomes clear that the Dutch government requests the Dutch defense industry to scale up, but the industry is unable to do so due to inefficient procedures, lack of government investments, and lack of government support (Conijn & de Lange, 2023).

This leads to conclude that there is a desire to grow the European and Dutch defense industry, yet defense industry companies are experiencing more than average restrictions with regard to their operations. What is the nature of these restrictions?

a. An uncertain market

As mentioned in the recent financial times article, the defense industry claims it cannot scale up easily, partly due to a lack of government investments. The defense industry is a unique kind of industry, the uncommon aspect of it in comparison to other industries is that the products are, for the most part, only available for sale to governments. Arms and war products can only be sold to governments, but the European Defense Ministries have a preference for cost-effective procurement as they need to balance security, industrial and economic considerations (Calcara, 2017). Thus, this limitation of the sales market brings uncertainty for the defense manufacturers. As described by Butler, Kenny and Anchor (2000) defense manufacturers are mostly suffering from declining defense budgets as well as a growing global competition.

b. The effects of sovereignty

The defense industry operations are, to a considerable extent, “sovereign” (Butler et al., 2000). Article 223 of the Treaty Establishing the European Community, having its foundations in the Amsterdam Treaty of 1997, states that an EU member state may, individually, “*take such measures it considers necessary for the protection of essential interests of its security which connected with the production of or trade in arms, munitions and war material (...)*”. This is an important obstacle of having a well-functioning European defense industry market (Britz, 2010), as it means that the Netherlands can legally ignore the procurement laws of the common market when procuring arms. Britz argues that in the EU, competition between defense industry companies is the normal state of affairs, and that defense companies which do not have a close collaboration with the government (e.g. state owned companies) have become more like any other company. Thus, the European defense industry policy is becoming more market-oriented rather than state-oriented.

c. State support

Some EU member states, such as France, have significant shareholdings within their defense industry, leading to a close relationship between state and defense industry (Calcara, 2017, and Carrincazeaux & Frigant, 2007). In the Netherlands, the state has diminished its share in the defense industry since they sold the only state-owned defense company, *Hollandse Signaal-Apparaten* in 1989. Since then, the Dutch state has only retained 1% ownership of the company which is now named Thales, and has not invested in any other companies in the defense industry (Jaarverslag Dutch government). Like the Netherlands, Germany also has shares in only one defense company, namely Airbus/EADS, together with France and Spain. Unlike the Netherlands, however, Germany has recently published guidelines for the Federal Government’s policy regarding the defense industry which explicitly expresses protection and promotion of Germany’s key security and defense technology companies, including through procurement, export promotion and export control.

5.3 About sourcing international knowledge and skill

The Netherlands is a key country in the European Union for trade. The Dutch government promotes trade and investment in the Netherlands, and the Port of Rotterdam ranks first in the busiest ports of Europe, and tenth worldwide (World Shipping Council). With such international activity in a relatively small country, it is clear that international knowledge and skill is often required by various companies.

What is the extent of sourcing international knowledge and skill in the Netherlands, and in which ways can such sourcing be done by companies?

a. Need for internationalization

The Dutch ministry of Defense has, in its report over 2021, stated that the relationship with the defense industry was under pressure due to delivery delays by the industry and its suppliers, at the expense of flexibility in execution schedule of projects (Yearly report defense material budget, 2021).

These delivery delays can be explained by the global shortage of semiconductors and other parts, due to the closing of factories during the Covid pandemic (Gulf Business, 2021). Furthermore, there has been a persistent shortage of available workers in the market in the past few years (CBS, 2022). The Dutch Central Bureau of Statistics reports that this shortage of staff causes a higher work pressure for personnel in nearly all sectors, as well as a clear increase in cost of staff. Thus, a capacity increase is needed.

While the shortage of semiconductors (and parts) is a global issue, the shortage of personnel is not. There are various ways of gaining personnel capacity, such as outsourcing, increasing internal capacity, and insourcing.

b. Outsourcing, increasing internal capacity, and insourcing

Outsourcing can be defined as (Chase, Jacobs & Aquilano, 2004) an “act of moving some of a firm’s internal activities and decision responsibilities to outside providers.” When classified data is involved, outsourcing will also require the downflow of security measure requirements. Villena (2018) describes that such cascading of requirements often fails, and indicates that there is a strategic role for the procurement department in building a supply chain network which is reliable. However, in the defense domain when classified information is concerned, the government does not rely on the procurement department of their industry contractors. The ABDO requires contractors to report to the government any proposed outsourcing of work pertaining to classified information, and to await government approval. Such approval is based on the confidence of the Dutch government in the security measures taken by the potential subcontractor, and approval is often dependent on the existence of (bilateral) general security agreements.

While outsourcing of certain activities can reduce the pressure on internal sources, internal means of gaining capacity are also possible. Literature, such as Jadayil, Khraisat and Shakoor (2017) points out various ways, such as optimizing effectivity of machines, or improving productivity of workers. Such manners of internal capacity increase are especially effective for production intensive environments. However, such measures do not mitigate today's issues of semiconductor- and staff shortage. In the defense industry, which is generally a high-tech sector, capacity increase can therefore also be sought in recruitment of new highly skilled staff. Such staff would need to come for the most part from abroad, since the shortage of staff is a broad national problem.

Finally, there is the possibility of insourcing. Insourcing can be defined as (Schniederjans & Schniederjans, 2005) "an allocation or reallocation of resources internally within the same organization, even if the allocation is in differing geographic locations". Large corporations may have multiple global sites, with various areas of expertise. In some cases, such expertise can overlap, making it time- and cost efficient to share production or development. This can be done, for example, in the form of shared competence centers. Furthermore, expert personnel may be exchanged between companies within the same corporation, thus assuring that knowledge remains within the corporation and making optimal use of personnel where they are needed.

5.4 Conclusion literature review

The questions that can be answered based on the review, are: what are the (government) data confidentiality rules? And: How do companies source international knowledge and skill?

Based on the review, we can conclude that limited literature is available on the topic of the defense industry and the protection of classified information. The literature available concerning the defense industry, is generally about the position of the industry within the European Union, and legal research studies on the working of the EU legislation. However, as we have seen, the defense domain is a national competence, and is governed by national law. No research literature was found on the implications of Dutch national law regulating protection of classified information, nor the impact of such law on the industry.

This lack of research can be a problem, because without knowledge of the impact the government rules have on the internationalization of the industry, there could be unnecessary negative impacts on both the government as well as the industry side.

This research therefore aims to add to the existing literature in terms of the issues of working internationally which arise from the national restrictions, and the way in which both industry and government could mitigate such issues without compromising the security of state secrets.

Although the literature review cannot answer questions regarding the impact of government data confidentiality rules on the industry's international aspirations, the review has provided a good grasp of answers to the first two sub-questions. These questions are: "What are the (government) data confidentiality rules" and "How do companies source international knowledge and skill" thereby clarifying the independent and dependent variable. Furthermore, it has set a framework for the particular challenges and restrictions which are valid for the defense industry in general.

Data confidentiality rules

We have seen that data confidentiality regards the security against unauthorized access to the sensitive data concerned. Standardization of rules is necessary for success, but when looking at the government confidentiality rules, standardization is limited to national practice. While there are differences between EU member states, there are even differences in standards between the Dutch defense and civil domains. The data confidentiality rules on classified information from the defense domain are contained within the ABDO framework, which is the handbook of general security requirements for defense contracts in the Netherlands.

Research (amongst others: Feddersen, 1995, and Latham & Hooper, 1995) points out that when pursuing a national manufacturing- and procurement strategy, defense firms are today at a competitive disadvantage in the global market. Therefore, just like other industries, the defense manufacturer must market its goods internationally, even globally. This need for globalization is in contrast with the determination by the government to retain national control over defense supplies. Such control forms restrictions, which the defense industry is experiencing. Control is exerted by, amongst others, export licensing restrictions and restrictions on sharing classified data. As we have seen, these restrictions can be somewhat moderated by state support, such as share-ownership by the State (France) or public announcement of support (Germany).

Sourcing international knowledge and skill

Dutch companies, which includes defense related companies, are facing capacity problems. These problems currently occur mostly in the form of semiconductor-, parts- and personnel shortage. Personnel shortage can be solved through outsourcing, recruitment of new (highly skilled) staff, or internal exchange within the multinational of personnel resources between companies within the same corporation, which is known as "insourcing". All these solutions to the capacity problem involve some type of internationalization, for which defense companies must acquire the permission of the government before implementing.

6. The impact of data confidentiality rules

“The digital transformation of the Dutch defense is not an “IT problem”, rather it has a broad impact. It will take guts, risks must be accepted. The classical, control-oriented way of working obstructs the realization of ambitions.” *Ambition document on IT by the Dutch Association for the Defense & Security Industry, Oct. 1st 2021. Summary of Dutch Parliament vision on IT investments of the government Defesnse department. Freely translated from Dutch.*

Now that the first two sub-questions have been answered, the case study and interviews methodologies are applied in this chapter in order to answer the sub-questions:

- What impact of the data confidentiality rules is experienced by the defense industry?
- What are potential causes of this impact?

Although it could be argued that it is normally more logical to start with the causes than with the effects, the research question: **“How can the impact of the restrictive nature of government-imposed data confidentiality rules, on a defense firm’s sourcing of international knowledge and skill, be minimized?”** requires first and foremost an answer to the question what the impact of the government-imposed data confidentiality rules actually is. Therefore, paragraph 6.1 will provide an analysis of the impact which is experienced by defense firms. Thereafter, paragraph 6.2 will provide an analysis of the perceived causes of this impact.

6.1 Experienced impact of government-imposed data confidentiality rules

The sub question to be answered in this paragraph is: what impact of the data confidentiality rules is experienced by the defense industry?

This question can be answered through the interviews conducted with industry stakeholders, as well as by analysis of the actual restrictions which are in force. First, it is necessary to identify which data confidentiality rules are actually applicable to defense firms handling classified data. As we have seen in the literature review, data confidentiality rules imposed on the defense industry are enforced through the “ABDO”. The latest version of the ABDO was published in 2019. The ABDO contains a total of 432 rules in different areas of control as shown in the following figure:

FIGURE 3
Number of ABDO Security Rules

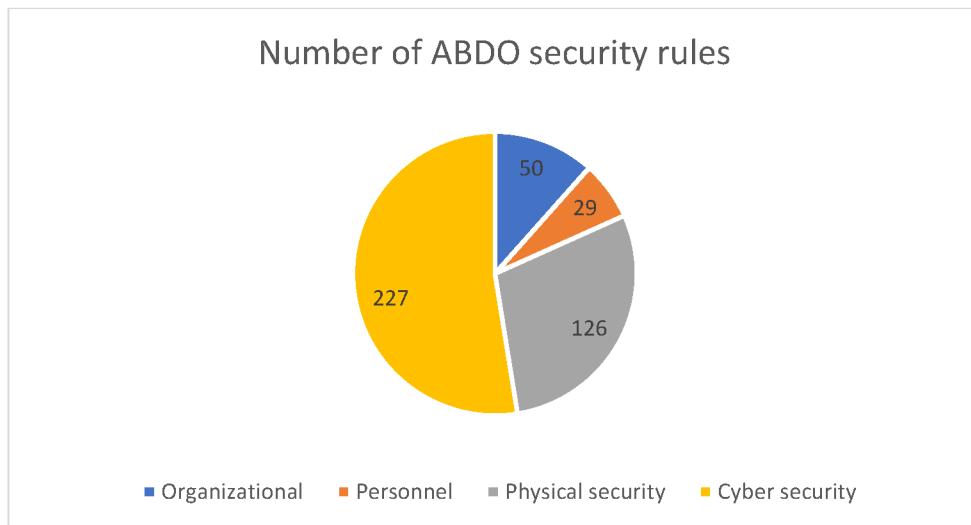
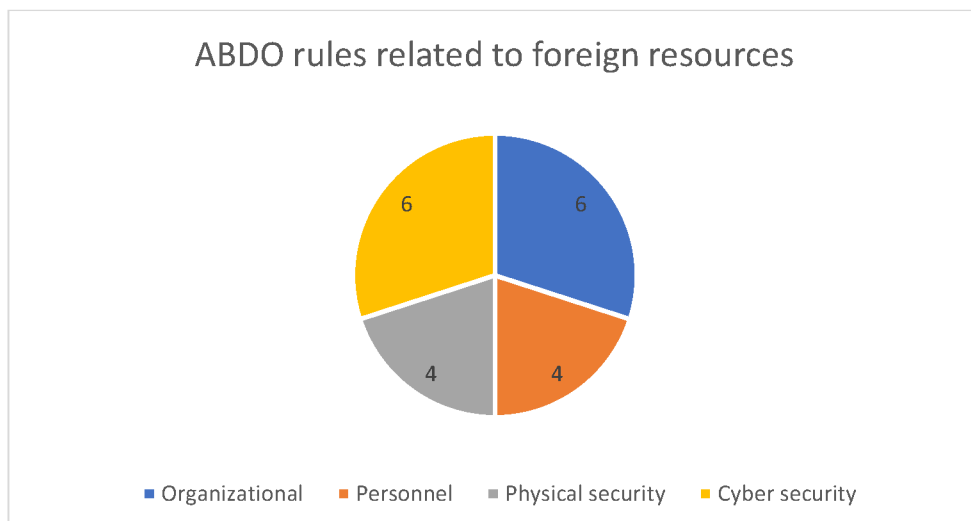


Figure 3 makes it clear that the most rules are in the domain of cyber security. However, we need to look at the content of the rules to understand the type of restrictions the rules post the industry. In addition, some rules only count for specific levels of confidentiality. When focusing on the rules which have a direct effect on the possibilities of the firm to make use of foreign resources, only twenty rules can be identified, as shown below:

FIGURE 4
ABDO Rules Related to Foreign Resources



These twenty rules can also be assigned to themes similar to the thematic analysis of the interviews. The rules and their assigned themes are specified in Annex III. These themes can subsequently be matched to the thematic map related to the problems and restrictions identified by the interviewees.

What difficulties do the restrictions pose, in general, for a commercial company in the defense industry? Three major themes can be identified, namely:

- a. Loss of quality for clients;
- b. Loss of market opportunity;
- c. Increased amount of work.

a. Loss of quality for clients

The thematic analysis of the interviews indicate three main areas of quality loss for clients, namely time, cost, and old technology.

Time

With regard to time, interviewees mention that time loss in projects occurs due to the processing time needed by the intelligence agencies for security screenings of partner companies, client companies, or employees. As we can see from the rules, several indeed require an upfront authorization provided by the intelligence agency. For example, rule number 2.1.11 states that “the appointment of a member of staff without Dutch nationality to a Confidential Position must be approved by BIV/MIVD prior to the application for a Security Screening”.

For staff involved with classified information, normal circumstances (Dutch nationals) require an upfront security screening to be completed. Such screening involves verifying the background of the individual, where the intelligence agency requests multiple pieces of evidence regarding the identity of the individual with various institutions. As explained by the security agency in an interview, the more information is obtained, the more certain it is that this person is who (s)he says (s)he is. However, gathering such information takes time, and there is also a shortage of staff at the intelligence agency, which means it generally takes weeks before the results are received. According to the rules, renewed security screenings are required at least once every four or five years, and in addition every time a person’s personal circumstances change. If a person does not have Dutch nationality, a permission from the intelligence agency is even required prior to starting the security screening as evidenced in the example shown above, and the intelligence agency itself must then request information from foreign government agencies, which can significantly increase the lead time depending on the country concerned.

For outsourcing, the rules also specify required prior permission from the intelligence agency. Interviewees indicate to experience more time constraints with security screening of staff than of partner/outsourcing companies, because the decision to outsource is usually taken at an earlier stage while staff is often needed on short notice (e.g. due to turnover). However, one interviewee indicated to experience delays in projects when certain changes occur in the company they outsource to, such as name changes, or ownership changes.

Old technology

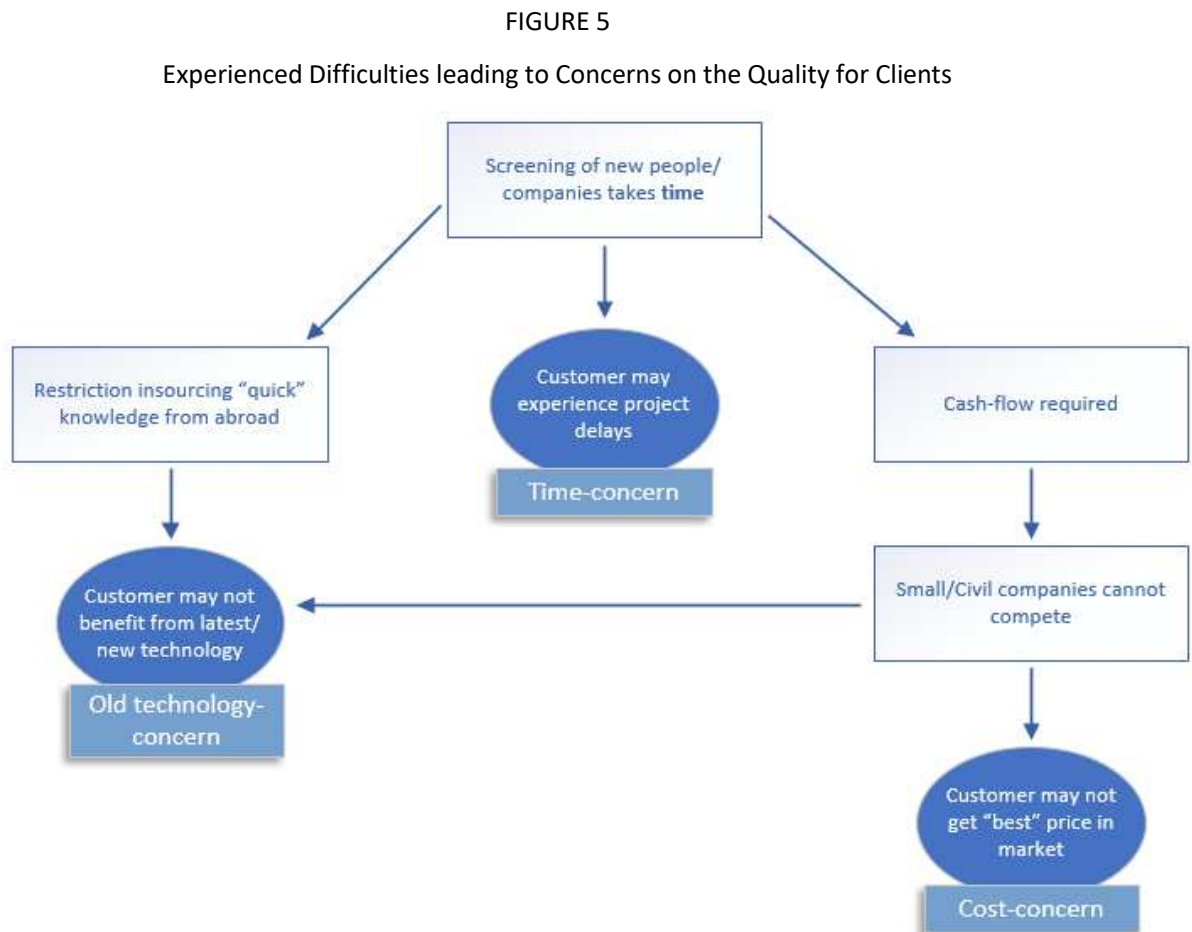
Another concern which leads to loss of quality for clients, is that due to the restrictions on use of non-Dutch nationality staff, it becomes more difficult to insource, so that larger companies cannot make full use of their potential in expertise. One interviewee from a company provided the example that experts in a certain area from foreign entities of the same company sometimes come together to share experiences and brainstorm for solutions to common problems encountered in different projects. Such experts, who already have a security screening clearance in their home country, may only have access to Dutch classified information after the Dutch intelligence agency has performed the security screening. Because such a screening process is too time- and work-intensive for ad-hoc meetings, expert meetings do not go into depth, and the best solutions for the customer may not be found due to this lack of depth. Thus, the customer may receive old technology, instead of the newest technology available.

Cost

Finally, a concern which leads to loss of quality for clients, is cost. In the opinion of both the larger manufacturers as well as the government agencies provided in the interviews, it seems likely that smaller companies do not have the cash-flow, nor the flexibility to go through the processes which are required for using foreign sources. This means small companies which remain local and which use only local resources are most likely to be prepared to invest in a cooperation with the Ministry of Defense regarding classified projects.

Naturally, there are also remarks from the interviewees regarding the cost of compliance. Examples were provided of a company which is normally active in the civil industry, but was involved in one defense contract. This involvement would have required implementation of ABDO rules, which was too costly. In this example, the civil company cooperated with a large defense company and the defense company was able to take over all activities related to confidential data under their existing security compliance framework. However, this example does show that there are likely certain experts in the civil market which are well-equipped to take on defense assignments, but are not able to due to the cost of implementing ABDO rules.

In summary, we can say that the amount of time needed for security screenings is a prime difficulty that is experienced by the industry, and this difficulty influences the concerns with regard to an increased project-time, old technology, and increased cost. A visual representation of this is provided in the figure below.



The time needed to have (repeated) security screening on staff, as well as the time needed to perform security screening on foreign partner/outsource companies in case of changes, cause a longer lead time in projects for clients of the industry. Furthermore, quality may be lost for clients of large manufacturers because the potential for insourced experts cannot be fully benefited from. Finally, small companies may not be able or willing to bid on (classified) projects from the Ministry of Defense. Thus, in the experience of the industry, these three difficulties (time, old technology and cost) are leading to a loss of quality for clients.

b. Loss of market opportunity

The problems regarding loss of market opportunity as mentioned by the interviewees, are mainly due to the high cost of maintaining the measures needed to comply with the security rules as a whole. Therefore, in the thematic map, the experienced difficulty with regard to cost has a relationship with both the loss of quality for clients, as well as the loss of market opportunity.

Although cost does not immediately have a relation with foreign sourcing, it was indicated that in the end, the client in the end is the one paying for the necessary security measures in the firm. However, there is a complication here, since the clients (government) do not pay companies beforehand. Therefore, investment in designing and implementing the security measures must be done up front by the companies themselves. Some of the interviewees are of the opinion that only larger companies, which have capacity for multiple projects at once, have the cash flow to invest in sufficient security measures. Smaller companies may not be able to make this investment, which is gradually leading to a choice of suppliers for the client (government) of several larger companies in various countries. It is possible then that more orders would be placed abroad rather than at smaller companies within the Netherlands, thus risking the loss of the knowledge position of the Netherlands within the defense market.

c. Increased amount of work

It is clear, from the number of rules posed in ABDO, that a large amount of work is needed by the industry in order to comply. It is nevertheless acknowledged by the defense industry that such compliance is a necessity in order to maintain the security of government confidential information. However, interviewees also do indicate that this work increases in certain circumstances when involving foreign cooperation or sourcing. One of the difficulties mentioned is that the more projects and co-operations, and the more involvement of foreign persons or entities, the higher the burden of maintaining control. This burden translates into higher cost, as discussed under “loss of market opportunity”, as well as to the need for additional staff.

Other than the lead times for having staff screened, there are also other restrictions related to staffing and the burden of maintaining increased compliance measures. One example is that when classified information is involved, teleworking is not permitted. This means all such staff must be physically present at the site. In current times, it is an employment benefit for staff to be able to work from home or from another location. Thus, it is increasingly difficult to recruit and maintain staff under the teleworking restrictions. The literature review has pointed out that the Dutch market recruits many more foreign employees than in previous years, this is no different for the defense manufacturers.

One interviewee indicated that it is increasingly difficult to find competent staff, even across borders, due to the fact that the rules also restrict use of the newest online available technologies. This means that the technology available to engineers is often somewhat outdated, and thus not as interesting for highly educated engineers as what might be offered by other employers not active in the defense domain. This translates to increased work in the recruitment and HR functions of the defense firm, as well as the amount of time needed for screening as described under section (a) of this paragraph.

d. Conclusion

The question to be answered in this paragraph was: what impact of the data confidentiality rules is experienced by the defense industry?

In conclusion, it is found that the difficulties experienced by the Dutch defense industry are primarily caused by the time needed for having staff screened, which leads to decisions not to make use of certain knowledge available through insourcing, and which also leads to an increased amount of work for the recruitment- and HR functions of the company. Companies are forced to incorporate the costs incurred for security measures in their price calculations for clients (government), as well as additional lead times both due to screening as well as due to the difficulty of finding competent staff willing to work for the company, which subsequently can cause foreign competition to win bids in favor of the Dutch defense manufacturers. Interviewees find that this may finally lead to a loss of the knowledge position regarding defense systems in the Netherlands.

The fact that these difficulties are experienced, does not mean that there is an opinion that the data confidentiality rules need to change. It was acknowledged during the interviews that security measures are necessary for the protection of the classified information, as well as for the continued existence of the companies themselves. This is because when foreign actors get a hold of this information, the products will be replicated abroad as also evidenced by the case of Urenco described in the introduction of this thesis.

Although there is truth in that statement and it can be acknowledged that security measures are indispensable, the same measures still seem to be causing difficulties for the Dutch defense market as described. It is clear that these difficulties are an effect of the security rules by itself, but the interviews indicate that they could also have different causes. The following paragraph will deep-dive into the causes of these effects, in order to find out which other moderators, besides the factual rules as stated by the ABDO, also have an influence on this.

6.2 Analysis of causes of the experienced difficulties

The sub question to be answered in this section is: what are the potential causes of this impact?

From the interviews, various causes for the experience of difficulties with the data confidentiality rules can be derived. In the thematic analysis of the interviews, the approach has been chosen not to make a direct link of the causes to the effects. The consequence of this is that a broad analysis of the data is possible with regard to causes, even though it may not provide a direct answer to the question what exactly causes each effect. This paragraph will describe the various causes which are indicated by the experts. In the conclusion, an attempt will be made to indicate a link between the causes mentioned hereunder, and the effects mentioned in the previous paragraph.

a. Governance

The most important cause which is mentioned, can be referred to as “governance”, meaning the way in which compliance is managed. Here, we can see that there causes lie on both sides of the line: potential causes related to government governance are mentioned, as well as potential causes related to the governance at industry companies. On the topic of governance, two main causes can be identified: a complicated organizational structure, and a volatile political opinion due to the interest of the general public. As will be motivated in this section, the way in which the organization is structured can also bring about a lack of understanding of the rules, which in itself can be considered another cause.

Complicated organizational structure – industry side

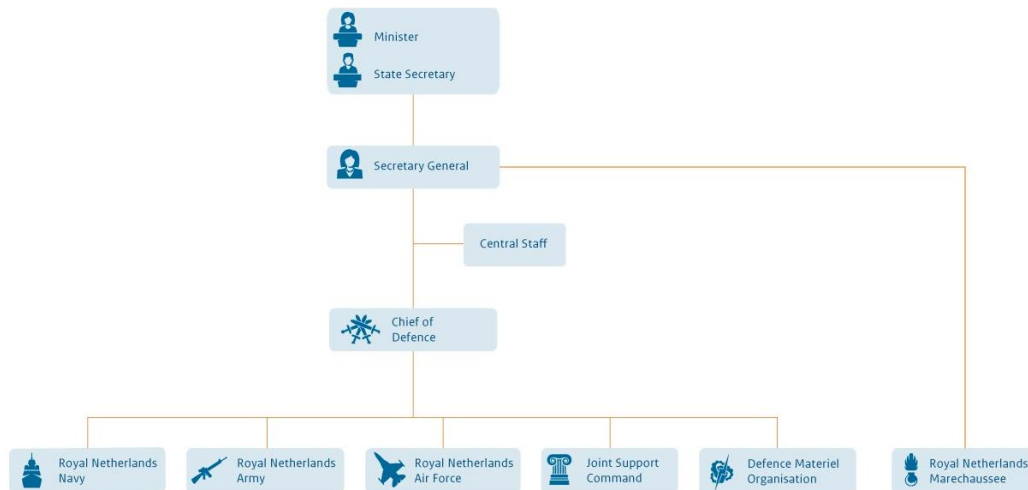
On both sides, administrative and procedural themes are mentioned. One interviewee from the government side explained that decision-making processes in general take too long, both from the side of defense companies as well as from the side of the government/ministry of defense. There are simply too many layers within the organizations, thus complicating communication. One interviewee from the industry side explained that indeed, the company has arranged the sales process in such a way that the opinion of various departments is required, which slows down their decision-making process. It is necessary to involve the expertise of many departments, but procedures do lengthen the decision-making time needed.

Complicated organizational structure – government side

On the government side, the organization chart of the ministry of defense, as shown below, reveals how some misunderstandings with regard to the organization can occur.

FIGURE 6

Organization Chart of the Dutch Ministry of Defense



Source: Website Dutch Ministry of Defense, accessed February 2023

As can be seen in the chart, the intelligence agency (MIVD) nor the policy making agency (national security agency, NSA) are mentioned in this organization chart, even though they do form an important part of the ministry of defense and are the important players when it comes to securing classified data.

Further desk research shows that the intelligence- and security agency is a part of the “Central Staff”. This agency has two main tasks, one is to provide military intelligence for the armed forces, and the other is to ensure defense industry security. For the execution of its tasks, the MIVD works together with the general intelligence- and security agency, which takes care of the “civil” intelligence and security, called the AIVD. The MIVD’s task of ensuring defense industry security, is what brings the government closest to the defense industry companies. These tasks are performed by the BIV, the *Bureau Industrieveiligheid* (Bureau Industry Security), which is a part of the MIVD. The BIV performs audits at industry companies, and interacts with them for ensuring a continued compliance with the security rules.

The defense security policy making agency, called the NSA (National Security Agency, or in Dutch: BA, *Beveiligings-Autoriteit*) also reports directly to the Secretary General. This agency however is more independent than the MIVD; it has a supervisory task on integral security. It is a member of the Defense Supervisory Board, and supervises compliance with the Defense Security Policy at all defense units. Industry security is one of its tasks, and in this position it maintains and regularly updates the ABDO, which is subsequently enforced at the industry companies by the MIVD. Besides the BA, various government ministries do also have a role in determining the level of security rules and the development thereof. Examples mentioned in the interviews include the ministry of Economic Affairs (“EZK”), the Commissariat Military Productions (“CMP”), the Netherlands Enterprise Agency (“RVO”), and the General Intelligence and Security Agency (“AIVD”).

This indeed is another cause of experienced difficulties mentioned by the interviewees, namely the multitude of political positions involved in the decision-making. One interviewee mentioned that the decision of whether a company is allowed to share classified data with a company in another country, is taken by the ministry of Economic Affairs, or by the ministry of Defense, but not by the NSA. In this decision making process, the NSA only has an advisory role.

Volatile political opinion

The fact that it is a ministry -and not the NSA- taking the decision also causes difficulties, according to the interviewees. The issue with this is that the ministries work to prevent political unrest, and thus decisions on data sharing taken by the ministry of Economic Affairs or even the ministry of Defense are probably influenced by the feelings and emotions of the general public. According to one interviewee, the defense industry “has not exactly been popular in the Netherlands”. This interviewee furthermore mentions that “We have politicians who are much more logically inspired, and are blinded because of that. They take much more unilateral decisions. They say: too bad, for the industry. “...” The defense industry in other countries, such as France, America and Italy also, has a much more important position, and therefore, much more is possible there”¹. When asking other interviewees about this, it was mentioned that there is often a misunderstanding in politics when talking about defense companies. Contrary to the general thought, one interviewee mentioned, most defense companies do not manufacture weapons. In fact, defense companies in the Netherlands mostly produce defense systems, designed for defending or surveillance, and do not produce any weapons at all. Although it is safe to assume that the NSA is aware of this fact, the various ministries may be inclined to take decisions partially based on the opinion of the general public.

¹ Translated from Dutch: “Nou en wij hebben natuurlijk politici die veel meer logisch bevlogen zijn, en daardoor worden verblind. Die maken daar gewoon een veel meer eenzijdige afweging. En die vinden het jammer dan, voor de industrie. “...” in andere landen zoals Frankrijk, Amerika, Italië ook, daar heeft de defensie industrie een veel belangrijkere positie en daardoor kan er meer.”

Lack of understanding of the rules

Finally, on the topic of the ministry of defense's organization chart in relation to this research it is important to mention that the classification, meaning the decision on the confidentiality levels of classified information shared with the industry, is decided upon by the purchasing department of each separate armed force. One of the interviewees commented that the purchasing officer sometimes just seems to "check the security box" without taking into account the consequences of using certain classification levels. Other interviewees commented that the way the purchasers in some cases indicate the classification levels, can be very crude, in the sense that their guidance does not indicate exactly which type of information shared is assigned with which classification level. This forces the industry company to take their own, more specified decisions on the classification level of various pieces of information, based on their own judgement. Regardless of this, the industry also indicates that they do not often go into a discussion with the purchaser on the topic of the level of classification. This is due to time restrictions; the belief that government- and company interests are opposites and are rarely compatible; and the uncertainty whether the two contract negotiators – often the government purchaser and the company contract manager – are sufficiently able to discuss classification level in the technical details which would be required. This can lead to overcompliance by the industry, as compliance measures may be organized for higher classification levels than necessary.

We can therefore conclude that the statements made by the interviewees regarding the decision-making difficulties are likely correct. Companies do use expertise from various internal departments, including but not limited to purchasing, engineering, legal, and trade compliance, in order to come to a decision. Within the ministry of defense, it is likely that there are no "short lines" between the policy makers, the enforcers, and the purchasers. Therefore, the purchasers may not realize the burden placed upon the industry, because they are not fully aware of the consequences of using certain classification levels. The enforcers may not have a full view of the extent of the burden, because they are not fully aware of the way in which the purchasers communicate the classification levels. This conclusion is endorsed by one of the government interviewees, who made the following statement regarding the data confidentiality rules during the interview: "I know that that [the rulebook] is also a maze for the user, also sometimes within the ministry of defense. Also within the ministry of defense, I get that same question, these same questions which you pose I also get them from defense, from employees. Why does it have to be so complicated²".

² Translated from Dutch: "En ik weet dat dat ook een wirwar voor de gebruiker is, ook bij defensie soms. Ook bij defensie loop ik tegen diezelfde vraag aan, dezelfde vragen die jij stelt krijg ik van defensie ook, van medewerkers. Waarom moet dat nou zo lastig"

b. Confidentiality rules

With regard to the rules imposed by government, we can be clear to say that compliance with such rules is a necessity in order to keep the country safe. This fact is not disputed by any of the interviewees.

Thus, the remarks made by the interviewees with regard to the rules, are in general more about the implementation of such rules than about the rules themselves. Various comments are related to a lack of understanding of the rules, and discrepancies between the interpretation of rules by government and industry. Finally, the way in which the rules are interpreted and implemented are influenced by an overlap in various control regimes, which will be described in this section.

Lack of understanding of the rules

A lack of understanding of the rules, as also indicated in the previous section, is not only perceived by the industry but also by government employees. The confusion from government can for example be noticed, as one interviewee remarked, by their reluctance to work together with the industry in development of new technologies. The reason for this, according to the interviewee, is a fear that the industry would use the government input in their commercial products to be sold abroad, but this is of course not possible when using the correct classification level.

Lack of understanding of the rules – discrepancies

Furthermore, the industry seems, on some occasions, to have a different interpretation of the rules than the government. One example is the use of online meeting tools. One industry company does not allow the use of Microsoft Teams at all, and does not allow sharing of desktop or even the use of the camera function while using online meeting tools with any external person. Their reason is that this could unintentionally reveal classified data, such as data written on whiteboards in the background. The government itself, however, does use Microsoft Teams and even allows sharing of the lowest classification level (Restricted/ *departementaal vertrouwelijk*) via this tool.

Another example is the use of cloud technology. Classified information cannot be stored in any cloud solution, with the exception of the lowest classification level (Restricted/ *departementaal vertrouwelijk*), which may in certain cases and only after specific permission from the defense department, be stored in private cloud environments which are hosted in the Netherlands. Cloud computing can, in accordance with ISO standard 17788:2014, be defined as a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. According to the same ISO standard, a private cloud is a cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer, whereas in a public cloud, services are potentially available to any cloud service customer and resources are controlled by the cloud service provider.

The Dutch government, in their 2011 cloud strategy, anticipated to develop a self-managed (thus, private) cloud environment for the Dutch federal government. This was based on a report by KPMG, concluding that cloud providers were at that time not sufficiently mature to meet the specific demands and responsibilities required by the government (House of Representatives document no. 26643.179, 2011). This private cloud strategy has been applauded by government data security experts (for example: Cobelens, 2021), but in 2022 the Dutch government published a renewed cloud policy (House of Representatives document no. 2022-0000478290, 2022) stating that public clouds should be used by the government under certain conditions. Although this public cloud strategy does not apply to the ministry of defense nor to storing of information in the three highest classified information of levels (TBB1, 2 and 3), the lowest classification level (Restricted) may be shared in public cloud by non-defense government services based on their risk assessment. Experts have warned the government that many of the parties involved still lack the expertise and capacity to properly secure data in the public cloud, and that the government renders itself dependent on the cloud providers which creates a risk of loss of control over its data (Rathenau Instituut, 2022). Even so, the government in its policy announcement sums up advantages of public cloud services, such as low start-up costs and pay-what-you-use. Due to the large investments by cloud service providers in the security of their services, states the policy announcement, risks are more controllable than before. Moreover, it states that the government cannot and does not wish to make investments of such magnitude into information security.

Aside from these motivations, the Rathenau Institute (2020) points out that use of cloud services is not always the free choice of the end user. Suppliers are forcing users to opt for using cloud services, because they are no longer supporting products on local servers. Some examples of these from practice include Microsoft, which often requires an online account³ in order to install and activate Office versions 2013 or later, and even applications such as the customs declarations software of Beurtvaartadres, is renewed with the implementation of the new customs system (DMS) in 2023 and from that moment on, will only be available as a cloud solution. Customers of such suppliers must either accept using a public cloud, or pay the costs related to a change of supplier. Such change of supplier can be at the expense of cyber security, reports Rathenau Institute, because the offline products are not always the best secured products available.

³ <https://support.microsoft.com/nl-nl/office/waarom-u-een-microsoft-account-nodig-hebt-met-sommige-microsoft-365-of-office-producten-d1b81992-d824-4e3f-8351-e2c03172df62>, accessed 6 january 2023

Overlap in regimes

Finally, interviewees mention that multiple regimes being applicable to security compliance make the situation more difficult to manage. In some areas of compliance, there is for example an overlap with export controls such as the U.S. International Traffic in Arms Regulations (“ITAR”). Furthermore, there is protection of the intellectual property of the company. Finally, the marking of classified information is not only restricted to the classification level, but also includes “eyes-only” markings such as “NL-eyes-only”, “NL and German eyes only” or even “NATO-eyes-only”. All these regimes require different markings of the information, which leads to confusion for the users of the information within the company.

c. Capacity and agreements

On the topic of staffing, we have already seen that the difficulties can be summarized as a time constraint due to security screening, when hiring non-Dutch personnel. Causes that can be indicated with regard to staffing include a lack of skilled personnel, as well as a complicated organizational structure in terms of availability and content of the bilateral agreements which can facilitate the industry.

Lack of skilled personnel

Indeed, from the interviews as well as from the literature study it becomes clear that the amount of non-Dutch nationality personnel is on the rise. This is because there is a shortage of available skilled personnel in the Netherlands. This is the case both for the industry companies, as indicated by the interviewees, as well as for the government. Shortage of staff in the ministry of Defense also becomes apparent from various media outings, such as articles by the ministry itself (*“Groei personeelsbestand, maar innovatieve werving blijft nodig”, 18 may 2022*) and by BNR (*“Ondanks investeringen loopt personeelstekort bij Defensie verder op”, 16 September 2022*).

Another cause for the difficulties experienced by the industry when dealing with the data confidentiality rules, is foreign co-operation. Interviewees indicate that the challenges in designing the IT systems in a secure way are mostly coming from the cooperation with external parties, such as suppliers or partners. Access rights must be managed, and additional attention is required for non-Dutch persons.

Complicated organizational structure - agreements

As described in the literature study, general security agreements (GSA's) and memoranda of understanding (MOU's) are agreed upon bilaterally to achieve agreed ways of handling classified information, with the aim to reduce the differences and thus reduce the compliance burden. While MOU's are agreed upon between the ministries of defense of two countries and are not made public, GSA's are agreed upon between governments and are published online. These publications, however, are not easy to find for the average industry representative. There is, for example, no list or link on the website of the ministry of defense, nor a separate heading for such security agreements in the "treaty database" of the Netherlands.

The Netherlands only has a few general GSA's in place, as shown in the map of Annex IV. An analysis of these GSA's shows that they are for a large part similar, but differences can be found in some crucial points. For example, we can see that there are differences in the requirements to be fulfilled in order to have personnel from the other country to have access to classified information. All GSA's require that the person has a "need to know", but only in the GSA with Belgium is it required that a person who does not hold a Dutch or Belgium nationality, requires prior written authorization for access of the party from whom the classified information is originating. Such clauses in one GSA can add more time required for security screenings as opposed to other GSA's. It also becomes apparent that GSA's are not always updated. For example, the GSA's with France and Germany do not have provisions for transfer of classified data using encryption. Since there is no formal agreement reached on the subject, it could mean that classified data may only be hand-carried, and other types of transfer require prior agreement from the authorities or consultation with the authorities which would be, again, time consuming. The reason for this deficiency, as is that achieving an agreement on a GSA is a long process of negotiations between two countries, which requires many hours of effort from government staff. Therefore, and taking into account the availability of staff, the government generally chooses to prioritize negotiations for new GSA's over the revising of old GSA's.

TABLE 2
Comparison between GSA's of the Netherlands

		General Security Agreements between the Netherlands and...				
		France	Germany	Spain	Belgium	Finland
Conditions for person to have access to classified information:	Need to know	yes	yes	yes	yes	yes
	Hold personnel security clearance	yes	yes, exception lowest level (DV)	yes, exception lowest level (DV)	yes, exception lowest level (DV)	yes. Alternative: authorized to have access by virtue of function. Exception lowest level (DV)
	Is briefed on responsibilities	no	no	yes	yes	yes
	Has signed a statement of confidentiality in accordance with national law	no	no	yes	no	yes, alternative: legally bound to confidentiality
	If person does not hold single or dual nationality of either country, prior written authorization of originating party	no	no	no	yes	no
	Transfer of classified data can be done using encryption and subject to national law	no	no	yes	yes	yes
	Transfer of classified data to third parties (any organisation, state, entity, individual in other jurisdiction) require prior written consent of originating party	yes, "third countries" includes employees if higher than "confidential"	yes, "third countries"	yes	yes	yes

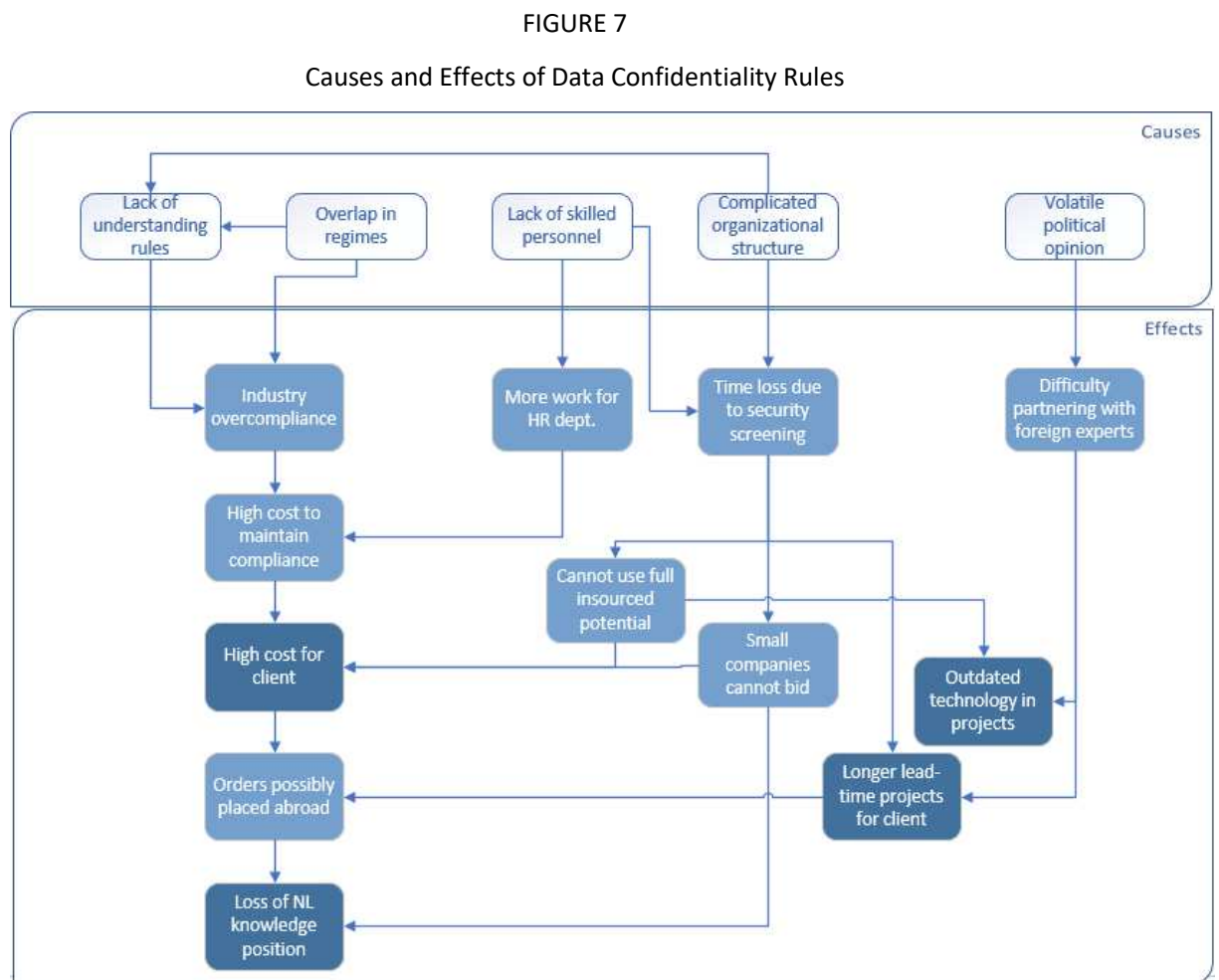
It is clear that these agreements can facilitate the industry, as it makes it less time-consuming to do business with those countries as opposed to countries with which the Dutch government has not negotiated a GSA or MOU. For example, personnel from these countries which have already been subject to a security screening in their home-country, would only require the Netherlands to check whether that screening was successful, but would eliminate the need for re-screening and thus save time.

In summary, more non-Dutch employees, and more international cooperations lead to more complexity when working to comply with the data confidentiality rules. Industry is facilitated by the government by way of GSA's (treaties) and MOU's, but the provisions of these treaties are not all the same and require in-depth analysis to determine what measures need to be taken to comply with the bilateral agreement in question.

6.3 Conclusion: causes and effects

The question to be answered in paragraph 6.2 was: what are the potential causes of the impact experienced by the defense industry?

This question can be answered by identifying which causes may have led to which effects, experienced by the industry. The effects, which have been discussed in paragraph 6.1, can be divided into experienced difficulties and the final expected effects of these difficulties. The outcome of the cause- and effect analysis are shown in the following figure:



As can be seen in the figure, five main causes can be identified. These cause a certain effect in defense companies, which we can call the “experienced difficulties”, and these are indicated in light blue. Some of these difficulties by themselves are causing other difficulties. In the end, four main effects can be identified which are external, and affect external parties other than the defense company itself.

The time needed for the industry to obtain government authorizations, seems to have its main cause in the complexity of the organizational structure on the side of the government, as well as on the side of the industry itself. When decisions are taken, various departments are involved, and all these departments have their own interests.

The complexity of the organizational structure also adds to the compliance burden that is experienced by the industry. Individuals, both on the government as well as on the industry side, are involved in taking certain decisions, however these individuals may not have had sufficient training, may not have sufficient knowledge, or may not have access to sufficient sources in order to oversee the compliance-related consequences of their decisions. These individuals furthermore have to deal with a multitude in compliance regimes, such as export control regimes from various countries. Such regimes have overlaps but also differences in applicable security rules.

The Dutch government does facilitate the industry, amongst others by making available bilateral agreements in sharing classified data. However, the extent of these agreements does not always reach the industry, and is not always used to its fullest potential by the industry. Thus, figure 4 holds true for all countries, including those which are “partner countries” through a bilateral agreement. However, referring back to the conceptual model: being a partner country can certainly be considered a moderator on the effect of the government data confidentiality rules on the possibilities for sourcing international knowledge and skill by the industry, because if these agreements are used to the fullest, then the experienced impact shall be expected to be less severe for these countries.

Complicated organizational structures, overlap in various applicable security regimes, and a lack of understanding of the rules are leading to an overcompliance in the defense industry, as following the government rules is their license to operate, thus causing a behavior of risk aversion.

7. Overcoming the difficulties

“Speed and predictability are very important in facilitating international trade. We are very much aware of the task we have as Dutch Customs in promoting the competitive position of the Netherlands and the EU.” *Dutch customs services about “how we work”, as published on the website of the Customs Administration of the Netherlands.*

The final sub question to be answered, shall be answered in this section namely: what are recommendations for overcoming the experienced difficulties regarding data confidentiality rules when sourcing of international knowledge?

Some actions have already been proposed by the interviewees. Other recommendations become apparent from the analysis in this chapter.

Actions suggested by the interviewees can be divided into three categories, as pictured by the thematic map in the Annex. These are: communication, compliance by design, and long-term vision.

For each of the identified causes, this chapter will summarize the related difficulties and eventual effects as shown in figure 4, and provide recommendations in one or more of the three categories proposed by the interviewees. These recommendations are aimed at overcoming the experienced difficulties, by mitigating their causes.

7.1 Overcompliance and risk aversion

The rules which are imposed by the government, may be misinterpreted in some ways by both the industry as well as by some departments within the government itself. In addition, the industry must also comply with other regimes, such as the Dutch and U.S. export control regime. Furthermore, the industry must protect its own intellectual property, which calls for other ways of security than security of classified or export controlled information. This leads to a great variation in protection measures implemented in firms, which also lead to confusion among the employees.

Thus, two causes are generally leading to a suspected overcompliance by the industry companies. First, compliance with government (classified) data confidentiality rules is a “license to operate” for the defense industry. Therefore, if there are misinterpretations with regard to the rules or the classification level, the industry likely tends to implement more security measures than necessary. Second, the variety in regimes and the rules of compliance for each of these regimes, drive industry companies to implement more overarching compliance measures to ensure that each of these rules is met. Although this makes the rules easier to understand for employees, the measures are more strict than they need to be in certain cases.

Although overcompliance is difficult to measure, it is often caused by risk aversion, which is a consequence of systematic risk (Zhang et al, 2014). On the other hand, risk aversion can also be a temporary effect after the occurrence of a catastrophe (Bordeau-Brien & Kryzanowski, 2020). Within the defense industry, it is more likely to be a consequence of systematic risk, since the data confidentiality rules are applicable to data transmissions which are happening on a daily basis. A similar case of overcompliance caused by risk aversion can be clearly identified in the financial industry. Financial institutions, in particular the banking industry, must apply counter-terrorism financing measures, which requires the bank to ensure proper risk management of each customer. However, this has led to a tendency by banks to reject high-risk customers (Goodway, 2014) which is an outing of overcompliance that seems to be due to the fear from being penalized (Malakoutikhah, 2020 and Basaran-Brooks, 2022).

Overcompliance caused by risk aversion can lead to “Red Tape Barriers” (hereafter: RTB’s), as described by De Sordi et al (2021). These RTB’s cause various obstacles in the decision-making process. “Red tape usually implies excessive or meaningless paperwork (Bennett & Johnson, 1979); a high degree of formalization and constraint (Hall, 1968); unnecessary rules, procedures and regulations; inefficiency; unjustifiable delays; and as a result from all this, frustration and vexation” (Bozeman, 1993). RTB’s can be defined as “policy-induced trade barriers that do not generate revenue or rents” (Mrázová et al, 2018). Such procedural obstacles have indeed been identified in this research, namely the time constraints for government screening of new personnel and foreign business partners, the administrative efforts for maintaining compliance with the regulations, and insufficient transparency with regard to the communication of bilateral agreements.

Industry overcompliance by itself means that more costs are required for design, implementation and maintenance of the compliance framework within the company. Higher costs are also caused directly by a misunderstanding of the rules, when more time and effort must be spent to design, implement and maintain such a framework. Costs made by the company will eventually always have to be covered by sales, thus it is the client who eventually pays for these costs. In the case of the defense industry, the situation is unique in the sense that the client itself imposes the rules which lead to such costs. However, the fact that the rule-imposing and purchasing departments or ministries are different, means that there may not be sufficient realization amongst the purchasers that higher prices are caused by these rules.

It may be decided by a government, although this is not necessarily the case, to place orders abroad, where the prices are lower. If this happens, the interviewees indicate that this may eventually result in a loss by the Netherlands in general of its knowledge position in the defense technologies.

Recommendations

In order to overcome misinterpretations of the rules, interviewees foremost indicate that it is important for the industry to maintain the dialogue with the government. Nevertheless, research also suggests that “the increased contact with regulators and the use of consultants correspond(ed) with higher “...” costs and, by extension, the probability of overcompliance” (DeHart-Davis & Bozeman, 2001). Thus, DeHart-Davis and Bozeman suggest that overcompliance could be a reaction to extensive communication with the regulator, particularly if there are high volumes of information if the information is contradictory or ambiguous. For example in the context of compliance with data confidentiality rules, if the purchaser from the government side provides unclear indications about the level of classification or the specific information which is to be considered classified, the contracting defense company currently often does not, but according to some of the interviewees, should open up a discussion with the purchaser. One interviewee mentioned: “You have to indicate: up to here we can do NL-eyes-only, but we cannot do more. It stimulates, not everything is classified.”⁴

However, it should be acknowledged that this could lead to more ambiguous information. Therefore if the company is of the opinion that the provided classification level is too strict, or too extended, the consequences of this should be explained to the purchaser during the negotiation phase of the contract. For example, such a consequence could be an increase in cost, or the possibility that outdated technology will be delivered at the end of the contract term. Suggestions for classification level should be made, in order to prevent misunderstandings or ambiguity. The company could also elaborate toward the purchaser on the security measures taken by the company in order to comply with the data confidentiality rules, as it was indicated by one interviewee that some purchasers may not be aware of all the compliance measures taken by industry and would then tend to “check the security box” in the most reserved way.

This implies an extended role is required for the security departments, or security experts within the defense firm. Such experts should be included in the contract negotiations, and even though it may seem that this only increases bureaucracy and therefore time needed to finalize a contract, this time will be saved later on in the execution of the contract when less restrictions are applicable.

⁴ Translated from Dutch: “je moet ook zelf aangeven: tot hier kan NL-eyes-only maar vanaf hier gaat het gewoon niet meer. Dat stimuleert ook – lang niet alles is geheim.”

With regard to the overcompliance due to overlap in regimes, it is recommended for companies to bring together experts on each regime and discuss the overlap. Single security measures could be put in place which arrange compliance with aspects of various regimes, rather than each expert/department putting in place their own compliance measures. For example, a focus-group could be created consisting of the security department for classified data confidentiality; the trade compliance department for export controls; the finance department for customs; and the legal department for intellectual property protection. Such methods are also recommended in the AEO Guidelines, where it is suggested to team up with the security department, as they often already have procedures in place which cover compliance with most, if not all of the AEO-security rules.

The government could also play a role in preventing the unwanted effect of placing orders abroad. For purchase of innovative products, which are sensitive and needed for the international safety, government procedures are in place which allow the government to purchase directly from companies without having the requirement to write a tender. This is also laid down in article 346 of the Treaty on the Functioning of the European Union. The ministry of Defense could, when considering such purchases, also consider to make use of this exception on the requirement to tender when the exception is applicable to the situation.

7.2 Skilled Dutch nationals

There is a lack of skilled personnel available in the Dutch market, this problem is experienced both by the industry as well as by the government. This requires an increased capacity in the human resources- and recruitment departments, leading to higher costs which are eventually charged to clients of the firm. Furthermore, it drives the industry to look across borders for skilled personnel, thus increasing the time needed for (repeated) security screening of non-Dutch nationals. Additionally, each time such individuals are assigned to new projects which involve information that is marked “NL eyes only”, their access to such data must be authorized by the government. This in itself will eventually often result in a longer lead-time in projects for clients.

Recommendations

The lack of skilled personnel in the Dutch market cannot be easily solved by either government nor industry. Thus, increasing the work-force on site needs to be done by recruitment from abroad, by insourcing (from abroad). The problem with these solutions is that making use of non-Dutch work forces takes more time, because it requires security screening.

First of all, we can recommend a useful action to prevent the need for security screening through compliance by design. Interviewees suggest that production lines could be designed in such a way, that semi-finished products which are not subject to the restrictions are manufactured by non-Dutch personnel. Only the finished product, or specific parts of the finished product would then require Dutch nationals, for whom security screening is more easily achieved.

Another recommendation is for companies to make more efficient use of the GSA's, in order to determine which countries should have the focus of recruitment efforts. Individuals with a nationality of a GSA partner are more easily screened than non-GSA partner countries. Individuals from GSA partner countries who have already received a security clearance from their government do not have to go through the Dutch security screening at all, saving a significant amount of time.

Finally, interviewees indicate that non-Dutch individuals, even after having received their Dutch security clearance, need to receive a new government authorization through the Project Security Instruction for each new defense project they work on. The government could consider providing a larger "blanket" authorization for certain non-Dutch individuals, accepting only a report of the projects they work on rather than having to authorize their participation every time again.

7.3 Complicated organizational structure

Similar to other causes, the complicated organizational structure is also a cause which occurs both at the industry as well as at the government side.

At the industry side, we can see that often experts are working in different departments. These departments must all communicate together efficiently in order to take effective decisions, and in order to be able to communicate toward the government with the required knowledge so that results with regard to security screenings of personnel, security clearances of foreign partners, and the proper classification level of received and produced information can be achieved. However, there is often an proliferation of all kinds of procedures, making the process bureaucratic, confusing and lengthy.

At the government side, it is not clear from the outside which department is responsible for what. Crucial players are not indicated in organization charts published on the website, and the explanations regarding industry security are limited to those provided in the ABDO. GSA's are published in a treaty database but not elaborated upon elsewhere; the government does not actively draw the industry's attention to these GSA's unless the industry indicates first that it wishes to do business with either of these countries. Furthermore, one interviewee indicated that the security screenings are all done by the intelligence agencies, but sources must be found elsewhere in the government organizations. This puts a strain on the capacity of the intelligence agencies, and it is likely one of the causes why the industry must in some cases wait for such long times to receive results of security screenings.

These long lead times have, as gained from the interviews, the effect that companies cannot make use of insourced experts from sister-companies in other countries. This ultimately leads to higher costs for clients because the industry could not make use of its full potential, but it could also lead to outdated technology in projects for clients because the industry cannot apply expert knowledge from other countries which may be more advanced in certain technologies. Furthermore, small companies cannot afford the wait, and may not be able to bid on requests for proposal from the government. While this could lead to higher costs for the client because there are less alternatives available, interviewees also point out that this in itself leads to a loss of the Netherlands' knowledge position of defense technologies, because innovative small companies cannot develop themselves easily in this area.

Recommendations

In order to solve the complicated organizational structures, both companies and government could contribute.

For industry companies, it is first and foremost recommended to review their procedures, and reduce to the essence wherever possible. Here, the focus groups recommended under paragraph 7.1 could also contribute to simplifying the compliance framework without losing the essential procedures contained therein. Interviewees from industry and government agree that if the security measures are implemented well within the compliance framework, as a solid basis, that the company is then ready to grow without having the future need of changing policies and procedures around. This also counts for IT systems. When implementing "compliance by design", and taking into account the ABDO and other rules from the start, there will be more clarity for the business. Furthermore, government and industry agree that well-designed training plans are essential in order to distribute and maintain the knowledge levels required.

For the government side, it is the opinion of the researcher that the responsibilities and structure of classified information rules are difficult to find in online sources, especially compared to the documentation and guidance published in the area of export control. This is evidenced by some interviewees from the companies who were unaware that the GSA's were available online, as well as confusion amongst the interviewees as to who in the government is responsible for the policy-making. Thus, the government could publish more clearly for the outside world who is responsible for what, and provide more guidelines or best practices on how and when to implement the ABDO rules. Furthermore, important documentation such as the ratified GSA's should be more easily accessible.

Additionally, the government could consider to provide additional assistance to small companies, in order to prevent that they consider the ABDO rules too late in the process because they do not have in-house subject matter expertise and consequently decide not to bid on government tenders. Such assistance could be directed proactively at small companies or startups which are considered potentially interesting by the ministry of defense in terms of innovation, and could consist of (online) trainings, personal approach or availability of a general helpdesk. Finally on the topic of industry support, the government could actively stimulate and support companies to motivate their own interpretation of what should be classified information, if it is not communicated in such detail by the purchaser from the client side.

In order to minimize the time spent on security screening, government could consider moving the screening operations away from the intelligence services, where resources are much needed for intelligence gathering, and move them to a department or ministry where there is more capacity and similar access to sources. Furthermore, certain screenings could be prioritized, for example screenings of individuals who have already received a security clearance in their home country, or individuals who are nationals of countries with which the Netherlands has ratified a GSA.

7.4 Politics

In the Netherlands, the ministers and state secretaries (cabinet) govern the country and implement policy. They must be supported by the House of Representatives, which is elected by the public, and thus subject to change, every four years. From the composition of the House of Representatives, it is decided which political parties will deliver which ministers.

Decisions on whether a company is allowed to share a certain level of classified information must be made by the ministers. Due to the political system in the Netherlands, such opinion could be different depending on the political opinion on certain countries, but also depending on the political composition of the House of Representatives and cabinet. Here, the emotions of the general public also play a role, because it is the general public which elects the House of Representatives, which in its turn must have confidence in the cabinet.

This uncertainty for the industry has the effect that partnering with foreign companies, especially those established in countries with which there is no GSA in place, becomes more difficult. This difficulty can be mitigated in various ways: some companies do not take the effort of trying to get an approval, other companies make use of (external) advisors to get a feeling of the political opinions, and it is even thinkable that other companies may simply wait for a new cabinet before applying for an approval. Such cross-border partnerships can however bring more expertise, work force, and a cost reduction, as evidenced by the literature review. Therefore, the effects of this political system are mainly the risk of providing outdated technologies to the client, as well as a longer lead-time because work cannot be outsourced to countries where there is no shortage of staff.

Recommendations

Useful actions to overcome difficulties related to politics and the opinion of the general public, should be sought in mitigating the effect of the political opinions, as already suggested above.

First of all, companies should consider in some cases to make use of an (external) strategic advisor, who has a good knowledge of the Dutch government. This could help companies to understand the possibilities and limitations before applying for approval.

Furthermore, interviewees here also suggest to implement compliance by design, in order to prevent restrictions in an early stage. Here, it is suggested to create products which are not in the basis subject to restrictive regulation. In principle, interviewees suggest, the confidential information is found in the parameters of products. Therefore the product could be designed in such a way that these parameters are contained within modules that could be added to the product in a final stage.

In communication with the government, the industry should consider to adopt declassification clauses in contracts. This is primarily interesting for original equipment manufacturers (OEM's) rather than for system integrators, because OEM's design products which may be sold to other clients again at a later stage. In fact, one interviewee mentioned, some classification levels may "vaporize" after the product has been sold a few times, because by then the classified information is already internationally known. Industry could in such cases also discuss the possibility of declassification later, even years after the original contract has been closed.

Finally, government could consider revising its classification levels. As a long-term vision, interviewees mentioned that if you make everything classified, you also devalue the concept. Instead of: "as secret as possible, as open as necessary", the motto should be "as open as possible, as secret as necessary". As found by the researcher, some countries such as France have reduced the number of classification levels, by eliminating the "confidential" level. When only the levels "top secret" and "secret" remain, there is more clarity for the industry, and for government purchasers the assessment of whether information should be classified could become more simple – it is either secret, or it is not.

8. Conclusion and recommendations

“If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place. “...” the reality is that search engines, including Google, do retain this information for some time. And “...” we are all subject in the U.S. to the Patriot Act, it is possible that that information could be made available to the authorities.” *Eric Schmidt, CEO of Google, during a CNBC interview in 2009.*

In this research, the main question was:

“How can the impact of the restrictive nature of government-imposed data confidentiality rules, on a defense firm’s sourcing of international knowledge and skill, be minimized?”

In order to answer this question, the following sub-questions were posed:

- *What are the (government) data confidentiality rules?*
- *How do companies source international knowledge and skill?*
- *What impact of the data confidentiality rules is experienced by the defense industry?*
- *What are potential causes of this impact?*
- *What are potential recommendations for overcoming these difficulties?*

8.1 Conclusion

First and foremost, it must be stressed that this research did not intend to pass judgement on the content of the government-imposed data confidentiality rules. Such rules are indispensable for the security of the Dutch citizens and government, as well as for the protection of defense companies. However, this research has also shown that it cannot be denied these rules have an impact on the international business conduct of defense companies established in the Netherlands, and ultimately on the clients of these companies, which is often a government. Therefore, the analysis done in this research gives rise to recommend actions for minimizing the experienced impact.

From this research, it has become clear that government data confidentiality rules are national rules which secure against the unauthorized access to sensitive government data, also referred to as “classified” data. In the Netherlands, these rules are contained within the ABDO framework. These rules govern several areas of security concern, amongst which the international sharing of data.

Companies source international knowledge and skill in three general ways. First, by attracting employees from foreign countries, in order to solve a shortage of skilled staff in their own country. Second, by insourcing staff from sister companies in foreign countries. This is done by multinationals, and could be for the length of a specific program, or for a longer period of time. Third, by partnering or outsourcing certain work packages, such as production or engineering of semi-finished products or of the final product, to foreign entities. These entities may be owned by the defense

company, or they may be third parties to the company. The ability to source such knowledge and skill is influenced by the government restrictions on confidentiality of classified information sharing.

The impact of these restrictions is ultimately felt by the customer, in the form of higher costs, longer lead times, delivery of technology which is outdated by the time the contract comes to a close, a decline of companies who are willing and able to enter in on a bid, and a potential reduction of the knowledge position of the Netherlands with regard to defense technologies. This impact is, in the opinion of the interviewees, leading to the potential effect that Dutch defense companies to lose their market position in the Netherlands, and consequently a certain loss of the current knowledge position of the Netherlands with regard to defense technologies.

Several potential causes were revealed in this research, amongst which a complex organizational structure in both the industry participants as well as the government itself, overlap in various applicable security regimes, and a lack of understanding of the rules. There are indications that these causes are leading to an overcompliance in the defense industry, which is appertaining to a behavior of risk aversion. So-called Red Tape Barriers can be identified which are a result of this overcompliance, these are procedural obstacles which are not strictly necessary for compliance with the rules.

With these answers to the sub questions, we can finally turn to the research question and provide suggestions for minimizing the impact of the government-imposed data confidentiality rules. Such recommendations can be done within the sphere of influence of the government, as well as within the sphere of influence of defense companies themselves.

8.2 Recommendations for minimizing the impact of data confidentiality rules

The impact of the government-imposed data confidentiality rules on the defense manufacturers can be minimized by either countering the causes of the impact, or by countering the effects these causes bring about in the defense companies. The proposed actions which serve to reduce the impact experienced by the defense industry can be divided into actions which are, in the opinion of the researcher, most feasible, and actions which may only be feasible in the long run.

Most feasible recommendations

In general, it is recommended to maintain a dialogue between government and industry. This dialogue is necessary to ensure an increased understanding on both sides: regarding the level of classification of information, the extent of the classification, the extent of security measures taken by the industry to protect this classified information, and the impact a certain classification level may have on the contract. Adopting de-classification clauses in contracts could, for OEM's, reduce the compliance burden for future sales. Dialogue could be supported by an improved communication between government and industry. Here, it is suggested that the

government proactively provides additional guidance and best practices to the industry, for example regarding the possibilities of general security agreements and memoranda of understanding ratified by the government. Defense companies could make smart use of such available agreements when sourcing international knowledge or skill, to minimize the time delays required for security screening.

In order to motivate companies to do so, government could choose to publish MOU's, which is not currently the case, and publish both MOU's and GSA's in a more accessible manner. Defense companies could also make use of an external advisor prior to bidding, to explore and understand the possibilities and limitations before entering a bid, or applying for approval to share classified data with certain countries or country nationals.

At defense companies, a certain level of overcompliance with the rules regarding classified information protection is noticeable. This overcompliance leads to so-called "Red Tape", and is leading to an increased impact on the firm's own international sourcing of knowledge and skill. It is therefore recommended for the industry to bring together the internal experts from different angles, such as security, customs, export controls and protection of intellectual property for the purpose of reducing the Red Tape Barriers. Such a focus group could work together in making common procedures on the security of information, which could reduce the compliance burden. With regard to overcompliance, it must also be recognized that the rules, in practice, are not always exactly as stated in the ABDO. There may be additional rules, which flow from the culture of a country or a company, from other regulations or interpretations of such regulations, or from certain opinions of involved decision-makers. Such rules cannot be easily set aside, but it is nevertheless recommended to take a critical look at the necessity of the procedures in place and, to the extent possible, reduce these to what is necessary for regulatory compliance. It is advised to keep in mind that it is best to keep accessibility as open as possible, and only protect what is necessary.

Small- and medium sized companies, as well as companies which are mainly operating in the civil domain, may not be willing or able to provide the investment needed to provide products for the defense domain. In this case, recommendations are made to reduce the time needed for both the decision-making process as well as the security screening process. First of all, with regard to the decision-making process, the government could consider to make more use of article 346 of the TFEU, when tendering for purchase of innovative products. Doing so would stimulate the defense industry of its own country. Second, with regard to the screening operations, it could be considered to move away the more simple security screening operations from the intelligence agency, so as to reduce the workload and save capacity. More simple security screenings could for example be screenings of Dutch nationals, and screenings of nationals from countries with which the Dutch government has ratified a GSA or has an MOU, and which nationals already have received a security clearance in that country. Such screenings could be moved to other government departments which have more capacity, or potentially be outsourced to an independent third party.

Less feasible recommendations

This research also provides certain recommendations which are less feasible, at least on the short term. They either require a serious change of operations, or a significant increase in capacity. Nevertheless, they can be considered by industry, as well as by government in long-term strategies, since these actions seem more likely to have a more permanent positive effect on reducing the impact for the industry.

First, defense companies are suggested to consider *compliance by design*, which could be achieved both in an organizational means as well as in product design. A company which takes into account the current rules on data protection when selecting and designing their IT environment, for example, will not have the necessity to spend time and money at a later stage when engaging in defense contracts. On the other hand, products could be designed in such a way, that semi-finished products do not include classified information, so that international sourcing of those products is not hampered. Another suggestion is to design products in such a way, that the main product does not include classified information, but that certain modules could be added to it in order to make it specific for the use by one government through the inclusion of classified information.

These recommendations are valid for the defense industry, but they are generic, and could also be applied to other types of industry where there is a question of national rules restricting the internationalization of the company.

Second, the government is suggested to reduce capacity requirements in security screening by considering blanket authorizations for certain individuals, eliminating the need to re-authorize the same individual for participation in new projects. Moving simple screening operations away from the intelligence agency was mentioned under the heading of more feasible recommendations, but moving away the screening operations entirely could be a subsequent step. Here, it would be needed to have more expertise in the government department where the security screenings would then take place, but it could free the hands of the intelligence agency to perform more intelligence tasks which require their specific expertise. Security screenings might also be reduced, if assistance is proactively offered to small companies or startups which are considered to be potentially interesting in terms of defense innovation. If these companies receive more upfront guidance from the government, this may also benefit the knowledge position of the Netherlands' defense industry as a whole. However, such guidance would again require capacity from the government side.

Finally, it is suggested to follow the example of certain other EU member states and revise the existing classification levels. The possibility to eliminate a level could be explored, in order to achieve more equality with the classification methods of certain other EU member states. This may also achieve more clarity for the government purchasers in their choice of classification, as there will be less levels to choose from, and thus, could also reduce Red Tape Barriers induced by "checking the box" of data classifications to remain on the safe side.

8.3 Limitations of the research

This research has its limitations. First of all, there is some difficulty in interviewing government representatives, and subsequently using their answers for the research. As mentioned before, there is good reason for certain aspects of the classified data confidentiality rules to remain somewhat obscure for the general public. Therefore, the outcome of this research may be different if executed by a government institution which has better access to such sources.

Furthermore, contractors executing government assignments involving classified information (regardless of the origin of such classified information) are not allowed to make this assignment publicly known unless specifically authorized⁵. Due to this, the possibility to identify and interview small companies working on classified assignments has not presented itself. This convenience bias means that small companies are not represented in the data, and conclusions related to small companies are solely based on the opinion of interviewees from government and from the large companies in researcher's network. Conclusions involving small companies may be different if the opinion of such companies would be included in the dataset.

Finally, due to lack of time, this research has retrieved information from only six interviewees. Although these interviewees do represent multiple defense companies as well as multiple government departments, the validity of their answers could not be cross-checked with their direct peers. A cross-check by way of more interviews, or by way of a survey, could have given a deeper understanding of the causes and effects, and may have provided insights into alternative recommendations.

This research can therefore suggest, but not prove a causal relationship between the causes and the effects experienced by the industry, as described in chapter 6. In order to prove such relationships, more data would be needed. Instead, the research provides a descriptive insight into the difficulties experienced by the industry and the events or actions that may contribute to the existence or level of these difficulties. The same holds true for the validity of the recommendations. These are derived from the interviews and analysis performed by the researcher. However, in order to verify whether these recommendations are indeed valid and effective solutions for the research question, it is needed to test the validity. This test could for example be performed by additional interviews, or by a survey of the Dutch defense industry to discover whether other companies could gain advantage from such recommendations.

Nevertheless, as a consequence of having drawn upon the experiences and opinions of both the industry and the government, this research can be used for input to other research which seeks a more confident assessment of external validity (Leviton, 2001) in the area of industry compliance with government-imposed data confidentiality rules.

⁵ As per government security restriction (ABDO 2019) number 1.8.1 on dealing with classified information

8.4 Contributions for research and practice

We have seen that four effects of the imposed government rules can be identified, namely:

- Higher cost for client
- Longer lead-time in projects for client
- Outdated technology in projects for client
- Loss of Netherlands' knowledge position

Even though this is a practice-oriented research, this research contributes both to the literature, as well as to practice.

With regard to the literature, we have seen that there is a gap in research of the impact which is felt by the industry and its clients, as a result of the Dutch government-imposed data confidentiality rules. This does not mean that the rules are too strict – on the contrary. These rules should absolutely be considered a necessity in the protection of state secrets. Drawing a comparison with the customs domain, we see that the Dutch Customs authority acknowledges the necessity of balancing between supervision and trade facilitation. For the intelligence services however, the focus is on supervision and not on trade facilitation. This research contributes in providing suggestions for the government to facilitate international trade, without compromising the policy and values of the protection of information.

In the practical sense, in the case of the defense industry, we can see that the government is making the rules and another part of the same government is the client, and therefore has to deal with the ultimate effects. The defense company therefore has the ability to go back to the rule-maker to explain the consequences they themselves will have, due to their choices. However, in other industries, the clients are not the same party as the rule-makers. Rule-makers of such other government divisions could therefore take into account the effect rules will have on the business on which the rules are imposed. One interesting example which comes to mind is the anti-money laundering legislation, which is becoming more strict for the financial industry. As a result, the financial industry is imposing more compliance requirements on their clients, who in some cases lose their ability to make use of banking services or are even unable to open a bank account. This increased compliance burden is likely to be a result of the increased rule-making, and it remains to be assessed whether such increased rules are proportional to the problems they are meant to prevent.

8.5 Recommendations for future research

From this research, various recommendations can be given for future research, mainly because there is no research literature available about the impact of the Dutch ABDO rules on internationalization of the industry.

First of all, it has become clear from the interviews that there is a certain interconnectedness between classified data security and export controls. In fact, the data security policy is at the foundation of export controls. With regard to agreements on the EU level, this research has shown that for data confidentiality in some cases there are already standardization projects on EU level, such as standardization of project security instruction templates related to the European Defense Fund. Other than this, there are very little agreements on the EU level, because defense is a national competence. For export controls however, there are multiple agreements on the EU level, even though the level and means of implementation of these by member states are varied. It would be interesting to investigate the EU level playing field on export controls, as this could provide insights on the level of success when increasing standardization of classified data security across the EU.

Another interesting recommendation for future research involves smaller companies in the defense industry. From the interviews, there are various opinions on how such smaller companies deal with the data security rules. Some interviewees are of the opinion that small companies have little knowledge on the topic and deal with the rules in a pragmatic manner. Other interviewees are of the opinion that they may be non-compliant, or that they cannot comply and therefore cannot bid. Researching the impact of the rules on smaller companies would, in addition to this research, give a more broad insight in the needs of the Dutch defense industry.

Finally, it was indicated during the interviews that new rules are being designed for classified data confidentiality, which will then be applicable to all government contracts. Instead of ABDO, these will be called ABRO. These will be based on the NATO- and defense rules, and therefore the rules for civil government contracts are likely to become more strict than they are now. It would be interesting to research what comprises the gap between the current civil government contract security requirements and the new ones, since this would also give insight into the additional burden that defense companies have had in comparison to civil companies which are also essential for the Netherlands, such as telephone, public transport, IT, and energy companies.

9. References

- Basaran-Brooks, B. 2022. *Money laundering and financial stability: does adverse publicity matter?* Journal of Financial Regulation and Compliance v30 n2, p. 196-214.
- Bennett, J.R. & Johnson, M.H. 1979. *Paperwork and Bureaucracy*. Economic Inquiry, 17, p. 435-451.
- Bozeman, B. 1993. *A theory of government "red tape"*. Journal of Public Administration Research and Theory, 3(3), p. 273-304.
- Braun, V. and Clarke, V., 2006. *Using thematic analysis in psychology*. Qualitative research in psychology 3(2): 77-101, January.
- Britz, M. 2010. *The role of marketization in the Europeanization of defense industry policy*. Bulletin of Science Technology & Society, v30 n3, p. 176-184
- Butler C., Kenny B., Anchor J.R., 2000. *Strategic alliances in the European defence industry*. European Business Review v12 n6, p. 308-322
- Calcara, A., 2017. *State-defence industry relations in the European context: French and UK interactions with the European Defence Agency*. European Security v26 n4, p. 527-551
- Carrnicazeaux, C. and Frigant, V. 2007. *The internationalisation of the French aerospace industry: to what extent were the 1990s a break with the past?* Competition & change, 11 (3) p. 260-284
- Central Bureau of Statistics, 2022. *"Ondernemers zien werkdruk toenemen als gevolg personeelstekort"* <https://www.cbs.nl/nl-nl/nieuws/2022/33/ondernemers-zien-werkdruk-toenemen-als-gevolg-personeelstekort> August 17.
- Chase, R.B.; Jacobs, F.R.; and Aquilano, N.J., 2004. *Operations Management for Competitive Advantage*. 10th ed. Boston: Irwin/McGraw-Hill
- Cobelens, P., 2021. *"Het is koude oorlog op cybergebied"* <https://www.securitymanagement.nl/het-is-koude-oorlog-op-cybergebied/> December 7.
- Conijn, F. & de Lange, R., 2023 *"De wapenindustrie moet opschalen, maar kampt met onzekerheid en trage procedures"*. <https://fd.nl/bedrijfsleven/1465886/de-wapenindustrie-moet-opschalen-maar-kampt-met-onzekerheid-en-trage-procedures> Financieel Dagblad, 27 January
- Daams, J., 2022. *Ondanks investeringen loopt personeelstekort bij Defensie verder op*. <https://www.bnr.nl/nieuws/binnenland/10488387/ondanks-investeringen-loopt-personeelstekort-bij-defensie-verder-op> . BNR News, September 16
- Dehart-Davis, L. & Bozeman, B. 2001. *Regulatory compliance and air quality permitting: why do firms overcomply?* Journal of Public Administration Research and Theory: J-PART v11 n4, p. 471-508
- DNB, 2015. *Integrity risk analysis – more where necessary, less where possible*. Guidance document.
- Draghia R., 2018. *Data matters: ethics, data, and international research collaboration in a changing world: proceedings of a workshop*. National Academies of Sciences, Engineering, and Medicine, Policy and Global Affairs .
- Dul, J. & Hak, T., 2008. *Case study methodology in business research*. Elsevier
- Dutch Government, yearly report and defense material budget 2021: *"Jaarverslag en Slotwet Defensiematerieelbegrotingsfonds 2021"*

Dutch Government, yearly report state-owned businesses 2021: "**Jaarverslag beheer staatsdeelnemingen 2021**"

Dutch Government, 2022. "**Groei personeelsbestand, maar innovatieve werving blijft nodig**". <https://www.defensie.nl/actueel/nieuws/2022/05/18/groei-personeelsbestand-maar-innovatieve-werving-blijft-nodig> Published 18 may.

Eurofound, 2019. **The Future of Manufacturing in Europe**, Publications Office of the European Union, Luxembourg.

European Commission, directorate-general taxation and customs union, 2016. **Authorized Economic Operator Guidelines**. Published 11 March, reference TAXUD/B2/047/2011 – Rev. 6

Feddersen, H. 1995. **The european defence firm, national procurement policies and the internationalisation of arms production**. Nato ASI Series D, Behavioural and Social Sciences 79, p. 37

Goodway, N. 2014. **Paying the price for sanctions**. <https://www.independent.co.uk/news/business/analysis-and-features/paying-the-price-for-sanctions-the-customers-with-iranian-links-being-ditched-by-british-banks-9679692.html> Independent, August 19.

Gulf Business, 2021. "**Global chip shortage**." SyndiGate Media Inc. October 31.

Hall, R.H. 1968. **Professionalism and Bureaucratization**. American Sociological Review, 33 p. 92-104

House of Representatives document, 2022. **Kamerbrief Rijksbreed cloudbeleid**. Ref: 2022-0000478290, published August 29.

House of Representatives document: Kamerstuk, 2011. **Brief van de minister van binnenlandse zaken en koninkrijksrelaties**, Informatie- en communicatietechnologie, dossier- en ondernummer 26643 nr. 179, published April 24.

ISO/IEC 17788:2014 **Information technology – Cloud computing**

Jadayil, W.A., Khraisat, W., Shakoor, M., 2017. **Different strategies to improve the production to reach the optimum capacity in plastic company**. Cogent Engineering v4 n1

Jain, N., 2021. **Survey versus interviews: comparing data collection tools for exploratory research**. The qualitative report 2021, v26, n2, 541-554.

Klomp, J. and Beeres, R., 2021. **Does legal origin matter for arms control treaty ratification?** NL ARMS Netherlands Annual Review of Military Studies 2021.

Latham, A. and Hooper, N (Eds), 1995. **The future of the defence firm: new challenges, new directions**. Kluwer academic publishers, Dordrecht.

Leviton, L.C., 2001, **External validity**. International Encyclopedia of the Social and Behavioral Sciences, Twenty Five Volume Set, Elsevier 2015, p. 617-622

Louwers, T.J., Vandenburg, W.M., 2003. **Data confidentiality in an electronic environment**. The CPA Journal v73 n3, p. 24-27

Malakoutikhah, Z. 2020. **Financial exclusion as a consequence of counter-terrorism financing**. Journal of Financial Crime v27 n2: p. 663-682

Malterud K., Horton R., Sassower R., Grodin M., Stein H., Wulff H., Sackett D., Richardson W., Rosenberg W., Haynes R., Schön D., Skelton A., Murphy E., Murphy R., O'Dowd T., Miller W., Stensland P., Malterud K., Malterud K., Barbour R. (2001). **The art and science of clinical knowledge: Evidence beyond measures and numbers**. Lancet, 358(9279), 397–400.

Ministry of Defence (Netherlands), 2019. **ABDO – General Security Requirements for Defence Contracts**

- Nikulina, A., 2022. **Case study research**. Presentation and study material, Erasmus Universiteit Rotterdam.
- Rathenau Instituut, 2020. Report: **Cyberweerbaar met nieuwe technologie**.
<https://www.rathenau.nl/nl/digitalisering/cyberweerbaar-met-nieuwe-technologie>
- Rathenau Instituut, 2022. **Overwegingen bij het Rijksbreed cloudbeleid**.
<https://www.rathenau.nl/nl/berichten-aan-het-parlement/overwegingen-bij-het-rijksbreed-cloudbeleid>
- Reiter, B. 2017. **Theory and Methodology of Exploratory Social Science Research**. Government and International Affairs Faculty Publications, 132.
- Romney M.B., Steinbart, P.J., 2019. **Accounting information systems**. Figure: relationships among the five trust services principles for systems reliability.
- Rosenkranz, A. **A.Q Khan**. Stanford University, 2017.
<http://large.stanford.edu/courses/2017/ph241/rosenkranz2/>
- Saunders M., Lewis P., Thornhill A., 2009. **Research methods for business students** (5th ed.). Pearson Education.
- Schniederjans, M.J.; Schniederjans, A.M.; Schniederjans, D.G., 2005. **Outsourcing and insourcing in an international context**. Taylor & Francis Group
- Villena, V.H., 2018. **The missing link? The strategic role of procurement in building sustainable supply networks**. Production and Operations Management v28 n5, p. 1149-1172
- World Customs Organization, 2018. **Customs Guidelines on Integrated Supply Chain Management ("ICSM Guidelines")**.

Annex I: Interview protocols

The interviews were semi-structured. Interviews were held in the native language of the interviewee in order to minimize risk of misunderstandings. For each interview, a set of questions was prepared beforehand. This included some generic questions, and in addition some questions specifically geared toward the subject matter expertise of the person being interviewed. Follow-up questions were in all cases asked during the interview itself.

Each interview was preceded by an introduction; in some cases these were full unstructured interviews which were not recorded, in some cases these were merely five to fifteen minute introductions describing the general aim of the interview. These introductions are not included in below interview protocol, as they were different depending on the relation of the interviewee to the researcher. Two of the interviewees were known to the researcher prior to the research, but work in different departments. Four of the interviewees were hardly or not at all related to the researcher prior to the research.

The generic questions which were posed during the interviews, are listed below. The last question of each interview (not listed below) was “Is there anything that you feel I should have asked, or that you would want to add?”. In every case, the interviewee either provided some additional interesting insights, or used the opportunity to enforce an opinion expressed earlier in the interview.

Manufacturers:

Can you elaborate on your role?

Can you elaborate on the extent to which government data confidentiality rules apply to your business?

In which ways have you implemented these government rules?

How do you deal with the NL-eyes-only concept?

How do you know or determine if, and which data within a project is classified?

Do you (sometimes) put the classification level of data up for discussion with the purchaser from the ministry of Defense?

What is your opinion on declassification of data?

To what extent do politics influence your business opportunities?

To what extent do you experience difficulties related to data confidentiality:

- when outsourcing?
- when insourcing (using skill from other, foreign entities within the same company)?
- when hiring/ increasing capacity?
- for any other activities your company wants to undertake, such as cooperations, sales, etc?

What can government do to make it easier for industry to comply?

Government:

Can you elaborate on the tasks of your department?

Can you elaborate on your role?

What are the responsibilities of your department in relation to ABDO?

Who is responsible for determining the correct classification toward the industry?

What is your opinion on declassification (after some time)?

Can you elaborate on the way the ministry of Defense applies the NL-eyes-only concept?

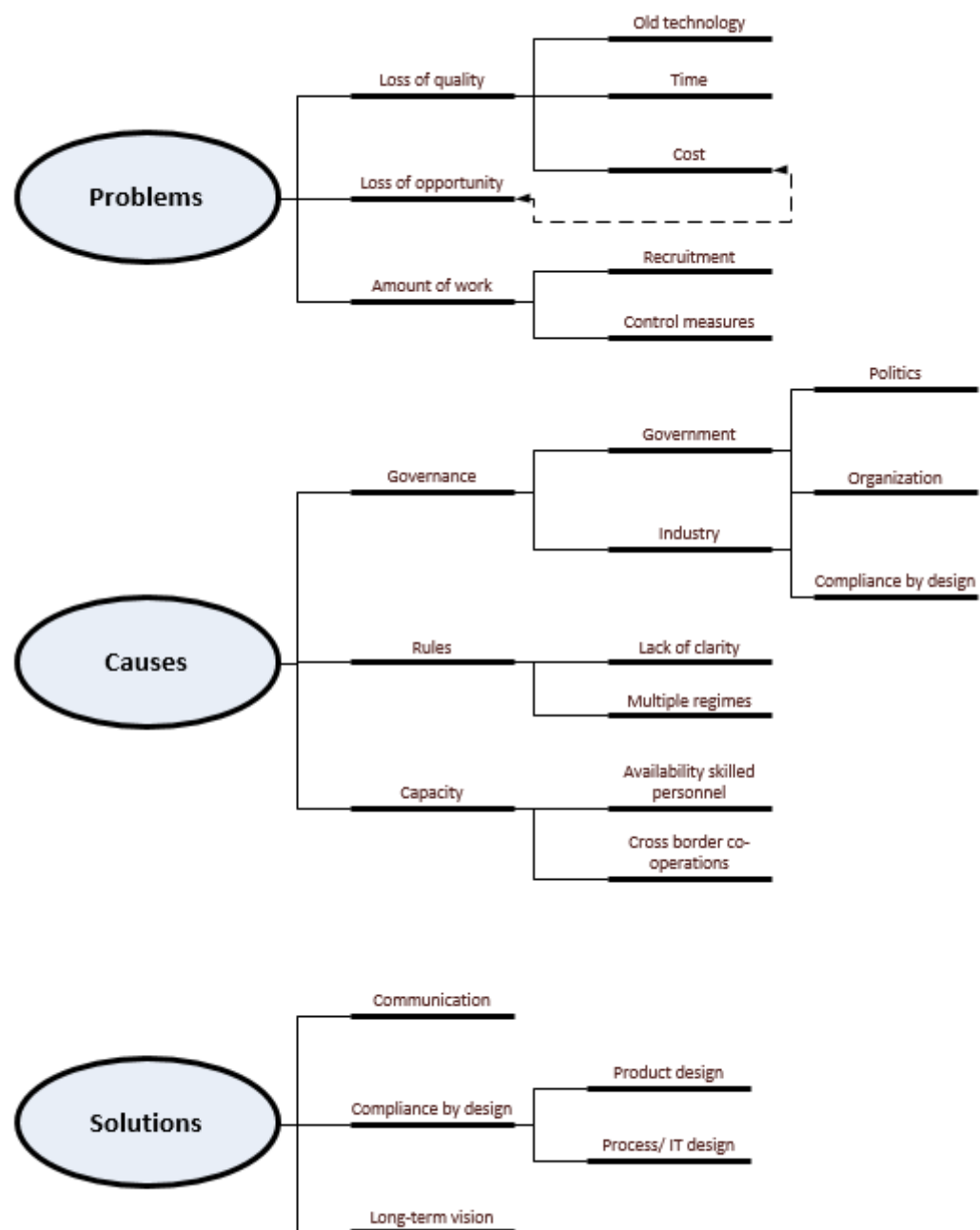
When are general security agreements applicable?

To what extent do politics influence:

- ABDO and/or security rules imposed on the industry?
- classification?
- general security agreements?
- any other aspect of your tasks related to data confidentiality rules?

What can industry do to make it easier for themselves?

Annex II: Thematic map



Annex III: ABDO rules related to foreign resources

<i>Risk area</i>	<i>Theme</i>	<i>Nr.</i>	<i>Rule</i>
<i>Organi- zation</i>	Staff	1.4.1	The contractor reports to BIV/MIVD ⁶ in writing and without delay any proposed appointments to the executive board of persons who do not hold Dutch nationality.
	Governance	1.4.9	In the case of a Special Contract ⁷ where large amounts of Special Information ⁸ are transferred, the Contractor is a Dutch legal entity.
	Governance	1.4.11	The Contractor only appoints employees with Dutch nationality to Confidential Positions which require access to a large amount of Special Information.
	Outsourcing	1.7.1	The Contractor reports to BIV/MIVD in advance any proposed outsourcing of work pertaining to a Special Contract to domestic or foreign Subcontractors. This is at the discretion of BIV/MIVD, which grants permission where possible.
	Outsourcing	1.7.3	Once permission for outsourcing has been granted by BIV/MIVD (on the basis of a Facility Security Clearance submitted by the foreign Partner), the Contractor incorporates the security requirements applicable in the country in question in its contract with foreign Subcontractors coming into contact with classified information. A completed RAL ⁹ is submitted to BIV/MIVD in this regard.
	Staff	1.7.6	The Contractor requests permission from BIV/MIVD in advance for any plans to outsource work for a Special Contract to a foreign Subcontractor. Outsourcing to a foreign company requires the permission of the Commissioning Party and authorization from BIV/MIVD.
<i>Personnel</i>	Staff	2.1.10	In the event of interim necessity, for example in case of a change of personal circumstances, the security officer requests a new Security Screening.
	Staff	2.1.11	The appointment of a member of staff without Dutch nationality to a Confidential Position must be approved by BIV/MIVD prior to the application for a Security Screening.

⁶ The Dutch abbreviation is used here in order to achieve consistent use of abbreviations throughout the thesis, namely: *Bureau Industrie Veiligheid* as a part of the *Militaire Inlichtingen en VeiligheidsDienst*. However, in the English version of the ABDO, the names of the intelligence services have been translated to English.

⁷ **Special Contract:** a contract that involves an interest to be protected (classified information) with the government as the Commissioning Party and a civilian party as the Contractor.

⁸ **Special Information:** classified information

⁹ **RAL:** Rubriceringsaanduidingslijst. A list which indicates per subject the level of classification of the information provided. The English translation of the ABDO abbreviates this as “SCC” but does not provide a definition for the abbreviation.

Physical	Staff	2.1.12	The Contractor only appoints employees with Dutch nationality to Confidential Positions which require access to a large amount of Special Information.
	Staff	2.4.2	Employees holding a Confidential Position will report any proposed trip abroad for the purpose of the Special Contract to the Security Officer without delay.
	Visitors	3.1.14	Access to a compartment containing classified information by visitors without Authorization (such as visitors) who do not have Dutch nationality will be reported to BIV/MIVD via the security officer at least five working days in advance. Without the permission of BIV/MIVD, this visit will not take place.
	Transport	3.7.1	Transport (abroad) of classified information only occurs through the agency of BIV/MIVD.
	Transport	3.7.2	Without the permission of BIV/MIVD, classified information will not be taken abroad.
	Transport	3.7.3	International transport of classified information takes place following the approval of the transport plan by BIV/MIVD.
Cyber	Working	4.2.21	Teleworking is not permitted (for levels confidential and up. For the lowest level, restricted, there are five additional rules under which circumstances teleworking can be allowed).
	Working	4.5.6	Remote administration (access to networks and network services) is not permitted (for levels confidential and up. For the lowest level, restricted, there are three additional rules under which circumstances teleworking can be allowed).
	Working	4.9.29	The use of a public Cloud service is not permitted.
	Working	4.9.30	The use of a Private Cloud Service is permitted (only for the lowest level, restricted, and only if specifically approved by BIV/MIVD, if carried out on Dutch territory, at a Dutch legal entity and by personnel with the Dutch nationality).
	Outsourcing	4.11.1	If an external party is involved in the management of a classified information environment, an ABDO authorization has been issued for this party by BIV/MIVD.
	Outsourcing	4.11.2	If data storage of classified information is facilitated by an external party, an ABDO authorization has been issued for this party by BIV/MIVD.

Annex IV: World map of GSA's of the Netherlands

