Thesis cyber espionage within the Dutch industry and educational sector

Tim van de Ven

S3496023

21-04-2024

Version: 1.0 Final

First supervisor: Olga Gadyatskaya

Second supervisor: Kate Labunets

Leiden University

Content

Acknowledgement

I would greatly like to thank everyone for their help in the thesis process.

Executive summary

Purpose:

This thesis aims to find the way the Dutch government is currently monitoring (cyber) espionage within the Dutch industry and educational sector. This knowledge should shed new light upon a normally quite confidential subject. Without sharing any confidential information or case studies from within the interviews, challenges in combatting espionage in the ever-digitalising Dutch cyberspace have been shared and found successes have been subsequently highlighted in this thesis as well.

Research questions:

The following main research question, and research sub-questions have been formulated to match the intended research purpose of this thesis.

Main research question:
How does the Dutch government monitor (cyber) espionage within the Dutch industry and educational sector?

Research sub-questions:

1. Is the Dutch government aware of the espionage danger?
2. How big does the Dutch government perceive the danger of espionage to be in general, and what are the trends?
3. What are the main challenges for the Dutch government regarding managing national cyberspace against espionage?
4. What are the recommended practices and procedures for organizations to defend themselves against espionage?

Methods:

Through combining the knowledge obtained from twelve semi-structured interviews with experts, a document analysis, and a literature review, the research questions have been answered. The research approach was a qualitative analysis combined with semi-structured interviews. As this thesis' goal was not about creating a new security model, but rather to delve deeper into the state of espionage monitoring within the government, a thematic analysis of the interviews has been performed.

Findings:

To answer the predetermined research questions, seven inter-connected themes have been identified, based on the literature review, document analysis and interview data: 1. Difficulties to attribute an attack as cyber espionage, 2. Lack of awareness at organisations, businesses, and people, 3. Political importance, 4. Educational freedom allows for less control by the government, 5. Geopolitical changes cause a very dynamic environment, 6. New development of tools, policies and legislation and 7. Governance within the government; defined roles, and responsibilities. Out of these seven themes, the first five have been categorised as challenges for the government, while the last two are considered successes that the government has achieved. These themes have contributed to

the knowledge concerning the monitoring of espionage within the government. The challenges that the public officials have faced, have been categorised further on the amount of control the participants have over the challenges. This means challenges have been identified that the participants do not have much control over, but we also describe several challenges which the participants do have (some) direct control over.

The Dutch government has been making great strides in combatting espionage, and other threats that would harm Dutch interests. As knowledge- and economic security can be part of espionage it was quite difficult to fully separate these categories, but as the ministerial responsibilities for these topics have been separated across ministries, it was important to define the three topics: espionage, knowledge- and economic security beforehand. By interviewing participants within the public sector and slightly adjacent to it, several important themes have emerged which described certain challenges and successes the government has been facing.

In general, this thesis has shown that the general awareness of the government of the known threats has been rapidly increasing in the last few years. Due to the recent geopolitical changes, existing strategic dependencies have shown that the Netherlands is not always fully prepared, but also that the general need for good cyber resilience is as important as ever. Internally at the ministries, the last few years have proved quite successful in terms of improving the awareness of these threats, and actively creating tools/legislation to protect the knowledge- and economic security of the Netherlands.

Threat actors of all kinds attack the Dutch cyberspace, which causes a very dire need for an active cybersecurity approach. Countless number of cyber attacks take place that target various organisations within the Netherlands daily. State actors also attack Dutch organisations for various goals, which includes industrial and cyber espionage, as nation state threat actors, like Russia and China are still dependent on Western technology in certain domains. To combat this espionage threat within several industries, the government has released two different Desks. One of the Desks focuses on private organisations within the Netherlands, and the other Desk is focused on the educational sector and research institutions. Organisations can ask questions or lay-out case studies within these Desk’s to get integral security-advice from multiple ministerial organisations.

The Dutch public and private sector have also been intensifying their partnership. This allows public sector organisations to use the knowledge and expertise within the private sector. This means ministerial organisations, and municipalities do not have to take care of all cyber security related tasks alone, the public sector can choose to outsource certain services towards private companies more effectively than before.

As the NIS2 has recently been introduced and is currently being translated so it can be used in the Netherlands, governmental organisations themselves are preparing for the massive changes in existing responsibilities. The participants of the interviews have often described the introduction of the NIS2 as a very good

way of creating a more cyber resilient environment for the Netherlands, and the European Union.

There are however still challenges in getting the Dutch educational sector along with certain strict policy choices. Dutch research and educational organisations have certain academic freedom which allows them to operate independently. As the research and educational organisations are especially important within the knowledge security domain, more attention to the certain threats that lure here would be beneficial. State actors are actively targeting universities and research institutions to try and get as much information from them as they can. The government also must actively convince the organisations to use the advice they have given to the various organisations, otherwise these Desks might lose their value.

Implications:

The information that this thesis has uncovered can be used to further improve the awareness of certain threats and re-iterate the importance of using best practices within cyber security. As many different threats have been described, a specific focus should be placed on state actors as they are already one of the biggest threats to the Dutch National security and interests.

Keywords:

State actors, espionage, cyber espionage, industrial espionage, knowledge security, economic security, security monitoring, threat actors, governance, public sector, private sector, national security, policies, legislation, Dutch government, APT’s.

1 Introduction

This chapter is be dedicated to describing the goals and objectives of this thesis, and our main motivation. The chosen research methodology also has dedicated sections, which further develops the thesis approach.

1.1 Problem statement

Journalistic research shows that the Netherlands currently has a problem concerning the naivety around research collaborations between the Netherlands and foreign partners (Willemsen, 2023) (NOS, 2022). Dutch universities often collaborate on research projects with peers from countries all over the world, which includes China and Russia. Even though most universities are aware of the potential dangers these collaborations might bring, and the way China and Russia use the sought-after technology from the West, the choices made still often lead to intensive collaboration. Sometimes educational organisations state they were not aware of the potential dangers that could arise (NOS, 2022). These collaborations can still lead to unwanted situations and censorship of scientific work (AWTI, 2022). Hooghe & Dekker (2020), report that China often affects certain research projects in the Netherlands and try to directly steer research/educational organisations, which gives China access and room to indoctrinate China's ideals onto Dutch schools.

Another crucial factor of unwanted transportation of Dutch knowledge into China, is the Dutch technological chip sector. Not only is China gaining military technology and knowledge due to Dutch companies and research teams, but this knowledge transfer is also reducing Dutch companies' competitiveness in the global market (Clingendael, 2021). The book written by Hannas et al. (2013), also states that collaborating with a Chinese company can often be described as directly collaborating with the Chinese Communist Party/government (CCP). This is often because China is still dependent on Western technology, so business interests often overlap with those of the Chinese government (Button, 2019). The naivety described in these reputable sources together with the potential dangers of foreign interferences in technology and research, creates a need for better insight into the current level of monitoring of espionage activities, to see what the Dutch government is doing to prevent this phenomenon, and how it could potentially be prevented further.

1.2 Research objective

This thesis aims to shed light on the status of monitoring of cyber espionage activities from the outside by the Dutch government. As mentioned before Russia and China are big factors when mentioning espionage, but other countries may also spy on the Dutch technology sector to get an edge into the industries where Dutch companies excel. Understanding how the Dutch government monitors espionage and how they advise Dutch companies accordingly needs to be measured. Understanding the level of care the government shows for the Dutch industry and educational sector is important, as economic security is also often linked to the innovation and technology of a nation. To make sure the Netherlands remains economically safe, it is important to understand the current situation. This thesis also wants to show the potential dangers and benefits of research collaborations and business decisions that will include other nation states. By talking to important organisations within the Netherlands, our work has shed some light on the current situation regarding espionage, knowledge and economic security within the Dutch industry and educational sector. One of the goals of this thesis, is to find out what is being done now and what will be done in the future to combat this threat.

To achieve this objective, the following questions have been defined to give an insight into the stated goal:

Main research question:

How does the Dutch government monitor (cyber) espionage within the Dutch industry and educational sector?

Research sub-questions:

1. Is the Dutch government aware of the espionage danger?
2. How big does the Dutch government perceive the danger of espionage to be in general, and what are the trends?
3. What are the main challenges for the Dutch government regarding managing national cyberspace against espionage?
4. What are the recommended practices and procedures for organizations to defend themselves against espionage?

1.3 Research methodology

In this section the different methods that we have used in the thesis are discussed. From the research design choice to the sampling methodology, several important choices, and the way we try to reduce the initial researcher bias are discussed.

1.3.1 Research design

The master thesis has used a qualitative design with various methodologies adherent to this qualitative design choice. To get a better understanding of the crucial factors regarding the Dutch Government a few steps are taken. Firstly, a literature review has been executed to form a theoretical base which can be built on. Secondly, a document analysis has been executed on several documents that the Dutch government has shared with Dutch organisations/the public. This document analysis has given us an indication about the level of coordination and regulation from the Dutch government towards organisations in in the technology and education sectors. Then a more specific approach is followed to find specific measures/controls for specific sectors/organisations. For this analysis, complex reasoning has given us the option to further analyse important findings and combine it to current background knowledge.

To fully get an insight into the actual methodologies of the government, interviews have been held with several stakeholders at different governmental organisations. We have chosen to conduct the interviews through either Microsoft Teams or at an on-site location of the participants choosing, as this allowed us to speak the participants bilaterally. As different people from different ministerial organisations will be interviewed, customised questionnaires have been created for their different areas of expertise. These different questions are specified for the type of ministry and the function of the public official in question. A general question list has been created, and the custom question list has been derived from this general list. This way we could incorporate the general question list, without potentially losing valuable information derived from the personal experience of participants.

The conducted interviews are semi-structured by nature. This way not only can pre-structured questions be formulated beforehand to guide the interview, but semi-structured interviews also give some freedom for differing and longer answers by the respondent. It also allows for follow-up questions after the respondent has answered an initial (structured) question, as the complete interview structure is not set in stone. This has allowed the us to ask valuable follow-up questions, which provided important information. This method of interviewing might also increase the reciprocity between the interviewer and the participant (Kallio et al., 2016), which could prove to be beneficial in terms of usable information that can be collected. Some studies use set in stone interview guides, but for this thesis some lenience in the methodology was required. Which is why per interview a slightly different approach/structure was chosen. For every interview, the structure and question list have been reviewed, to make sure they were relevant for the participant. There were however some parts of the interview process that were part of the standardised approach, like informing participants about the data collection/processing process (Hove & Anda, 2005) and allowing the participants to ask questions about the thesis.

Several interview methods have been considered, yet we believed semi-structured interviews would fit the qualitative design and goal of this thesis the most. As we are asking professionals, questions about espionage, economic- and knowledge security, we wanted the professionals to have the opportunity to answer the questions with the amount of detail and depth that they would have liked to use. We also used certain reflexive practices as follow-up questions to make sure the participants had plenty of opportunity to express themselves in the way they wanted. As the study from Hove & Anda (2005), mentions, it could be beneficial to ask reflexive questions, which allows the participant to give corrective information. An example of such a reflexive question, is by asking a participant if a certain decision they made, lead to the desired effect they originally had in mind.

As most of the participants were experienced personnel, one could also argue that their real work experiences provide more worth to this thesis than quantitative data would. As this thesis tries to uncover the actual way the Dutch government monitors espionage and what this would look like on the operational side and is not necessarily about taking conclusions about a certain population.

One of the downsides, the semi-structured interviews with a focus on the experiences of certain individuals does create however, is that the research team could be more exposed and reliant on individual opinions and biases that have been built up by the participants and eventually also the researcher (Anderson, 2010). Another downside is the great amount of time and manual work this method causes for the research team.

The thesis uses thematic analysis to quantify results in the qualitative research design. Using thematic analysis allows us to identify themes within the interviews. Thematic analysis gives some flexibility for us to identify potential categories of information, but it is however reliant on a certain level of coding quality (Clarke & Braun, 2016). How we planned to keep the coding quality high, will be explained later. Thematic analysis can be used from small datasets to datasets with more participants, which allows us to find empirical saturation through inductive analysis. Thematic analysis also has the aim of analytically examining real-life experiences by breaking the text into small units of codes and transforming them into descriptive pieces. This method has allowed us to ask participants of interview for their specific view of certain events and their opinions on the current situation within a particular subject (Vaismoradi et al., 2013). This is information that this thesis needed to answer the main research question and research sub-questions.

As the name implies, thematic analysis tries to identify themes through analysis of qualitative data. As the interviews used a semi-structured design approach, the data is filled with opinions and real-life experiences of participants. This data is quite valuable when talking about the topics that this thesis is researching (Braun & Clarke, 2006). Even though there is no perfect methodology to use for qualitative research, as grounded theory is also a solid option, the flexibility together with the goal of this thesis, we argue that thematic analysis was the best fit. Figure 1 below, shows the main characteristics of thematic analysis in comparison to content analysis:

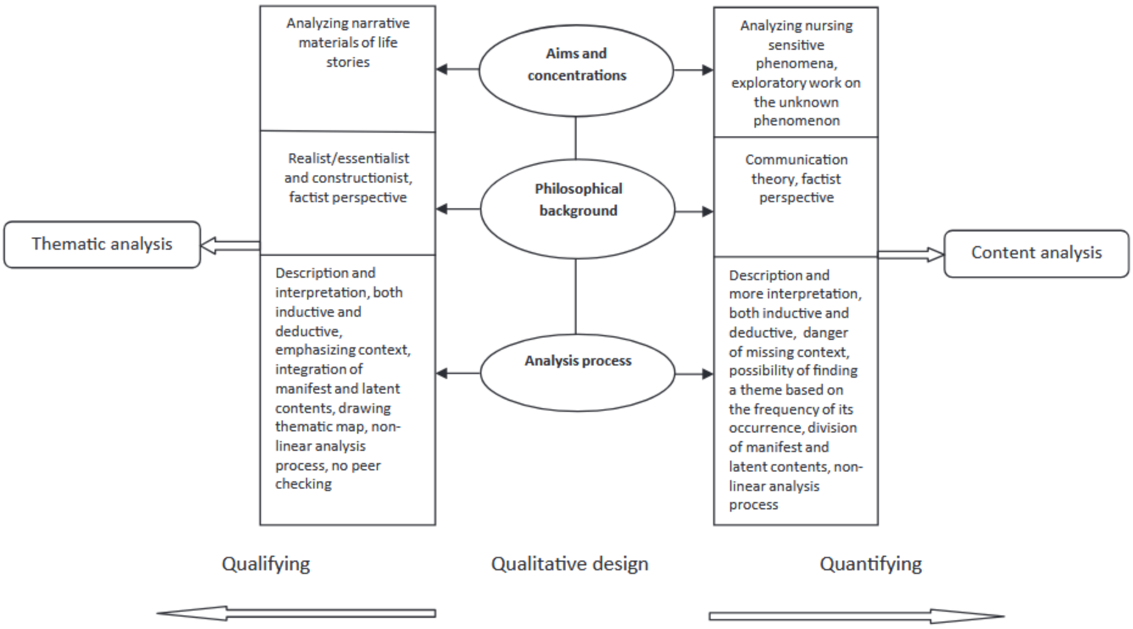

Analyzing narrative materials of life stories
Aims and concentrations
Analyzing nursing sensitive phenomena, exploratory work on the unknown phenomenon
Realist/essentialist and constructionist, factist perspective
Philosophical background
Communication theory, factist perspective
Thematic analysis
Content analysis
Description and interpretation, both inductive and deductive, emphasizing context, integration of manifest and latent contents, drawing thematic map, non-linear analysis process, no peer checking
Analysis process
Description and more interpretation, both inductive and deductive, danger of missing context, possibility of finding a theme based on the frequency of its occurrence, division of manifest and latent contents, non-linear analysis process
Qualifying
Qualitative design
Quantifying

Figure 1: Main characteristics of thematic analysis in comparison to content analysis by Vaismoradi et al. (2013).

As from the designing phases of this thesis it was clear the research method would be qualitative, this thesis would also use open-ended questions, thereby focusing on discovery and trying to find empirical evidence through conversations with professionals in the field. Often it can be difficult to know when you have enough data, but with twelve respondents, the research team has deemed that enough data has been garnered to reach what normally should be a satisfactory empirical saturation (Baker & Edwards, 2012). To create useable pieces of information from the interviews, the transcriptions will be labelled/coded with important categories. As the interviews are open and allow for a rich diversity of opinions and answers, it is important that these responses can also be coded accordingly. As we use thematic analysis, it is important to code parts of the transcription that describe certain themes. These themes can later be used to draw results from the various transcription sources.

As participants were allowed to give open answers with their own preferred amount of detail, difficulties in the coding process occurred as answers could be long and drawn out while using multiple examples to describes certain themes. These themes could include the challenges they were facing, or the victories they achieved while working, and potential pitfalls of the industry in general. As these lengthy and complex responses can add to the difficulty of coding and potentially reduce interrater reliability (Campbell et al., 2013), we have chosen to categorise codes on the subject at hand, these categories could than later by redistributed within a broader semantic domain. By categorising the codes within semantic domains, certain themes still emerge overall, but do not lose the original intent, opinion, and knowledge of a participant.

Another coding approach that could have been chosen is part of the grounded theory (Weston et al., 2001). This theory uses several phases of coding to validate certain codes by categorising the codes further and further. Grounded theory can often be used to point to well-rooted and fruitful new links in certain variables. Grounded theory is an iterative process, which could have suited this thesis as well. But this thesis does not aim on creating a new theory or setting up a new methodology, which meant that grounded theory could not be fully utilized in the way it was meant (Wolfswinkel et al., 2013).

To make sure the coding process is validated, two external people outside the research team have been contacted to try and code two transcripts based on the existing codebase, while being allowed to change the codebase when needed. As confidentiality is particularly important in this thesis, measures have been taken to protect the integrity and confidentiality of the data. The external code reviewers have created a separate code list which is based on the original code base, which the research team has compared to their own. Any potential discrepancies that have been found, have also been discussed and either ended up in revision of the original code base, or after certain discussions, a middle ground compromise had been found.

By allowing external variables to validate the codebook an attempt has been made to prevent researcher bias in the coding process. As we are trying to implement a reflexive practice towards the research methodology and overall thesis approach. This reflexivity impacts both the mindset of the researcher about existing bias, but also the concrete actions they take to actively prevent bias in the research results (Mackieson et al., 2018). But reflexivity is broader than that. It is also about critically reflecting every part of the research, from who you choose to include, how you ask the questions, to how you perceive the results. We want to be aware of potential pitfalls in qualitative research and actively try to incorporate ethical research standards that might lead to more rigorous research results (Guillemin & Gillam, 2004). By validating the coding process with external forces, it is an initial attempt to combat the biases. Following this validation method two times, we have concluded that the codebase has been validated with a certain level of confidence.

1.3.2 Sampling

To set out a strategy of garnering enough information about the way the government monitors espionage within the Dutch industry and educational sector, it was important to speak to various people from different organisations. To create a concrete image about the espionage cyber chain, several interviews (n=12) have been conducted with people from within the public sector and slightly adjacent to it. This way not only the views of governmental officials could be considered, but this also includes the views of the people that might have to deal with the policy pieces the government officials create.

Even though we have not defined a very specific profile of interviewees, the participants were selected based on certain criteria. The criteria consisted of the expertise, role, and position of people within certain organisations. A variety of people have been interviewed with distinct roles and expertises. This led to the research data containing a wide variety of opinions, views, and experiences, which was planned for beforehand.

By using the snowball method, participants of the interviews have been asked to share the contact details of certain individuals within their network that could be potentially interesting to interview. By using this technique, a larger audience has been reached as the interpersonal connection of all the different participants has been used. This way far more participants have been reached that could be of interest (Handcock & Gile, 2011). In reality, snowball sampling has also been the method which allowed us to contact most of the participants for the interviews.

After the first interview had been successfully conducted, we had already started working on the transcriptions and coding in the background. This caused us to have insight into the current level of empirical saturation. After every interview this saturation was reviewed. This is a method of purposeful sampling (Cutcliffe, 2000). Problems regarding the collection of the right participants were experienced by the research team, as specific areas of expertise were identified early on. A lot of time was spent on searching for candidates, convincing them of the added benefit of this research and eventually planning interviews with the participants. After every planned interview, some background research went into the specific participant to make sure the questions aligned to their expertise.

1.3.3 Confidentiality

As this topic is often considered extremely sensitive within the government, educational organisations, and technological sector, it was important to set up some ground rules before starting with the thesis. The confidentiality and integrity of the research data was particularly important, as we wanted to make sure that participants of the interviews could speak openly about this topic and share their opinions/experiences. This did mean that several crucial choices were made, including the choice to not publish the interview transcripts together with the thesis itself. Just as only the principal researcher himself has access to the research data, transcriptions have been anonymised, which means all organisational names and personal names have also been replaced with identifiers. These identifiers can be used to connect the participant to the interview, but only the principal researcher has access to this list. These ground rules have been discussed with all participants, and a contract has been signed between both parties while giving the participants some opportunities to change certain rules for their specific interview. This could mean that the participants had the opportunity to include or exclude quotes from their interview into the research results and were actively involved in the way data was collected.

1.4 Academic contribution

To secure the competitiveness of the Netherlands within different industries of the future, it is important to hinder any espionage that aims to steal or copy valuable technology. Currently, to the best of our knowledge, there are no academic studies on how the Dutch government monitors espionage within the Dutch industry and educational sector. This thesis aims to shed light on the status of monitoring by the Dutch government of any espionage activities within the Dutch industry and educational sector.

The increase in knowledge regarding the monitoring of espionage within the Dutch industry and educational sector, will bring more awareness of the dangers that have been lurking in the Netherlands for a while. There is in general a lot of ground to cover in the way the government must deal with digital espionage in academic literature. When mentioning the role of the government, the amount of research papers regarding economic security and espionage becomes even smaller. While the government plays a critical role in maintaining economic and digital security of its citizens, businesses, and organisations.

1.5 Outline/Scope

In this thesis the focus has specifically been placed on espionage factors within the Dutch industry and educational sector. Especially on how the Dutch government tackles the problems within these domains. Examples of other EU countries will be examined to learn from already existing experiences within the secondary data. Interviews and secondary data have been used to research the Dutch government and its current trajectory with battling espionage within the Dutch industry and educational sector, the focus will be on the on Dutch national situation. The interviews will be held with public officials from different ministries of the Dutch Government. Individuals that work at important organisations that deal with espionage, but also knowledge-and economic security have been interviewed. This gave us a good image of the current way of working of the government.

As a lot of information within these subjects is confidential, the questions will be formulated broadly to make sure the public officials can give contextual answers without feeling the need to skip out on questions if they might invoke a specific confidentiality clause. There are also many forms of espionage, which is why this thesis will focus specifically on industrial espionage, economic espionage, and cyber threats/espionage and further include relevant topics like knowledge- and economic security. To make sure a clear outline is defined, the thesis will be mostly about how the government deals with espionage targeted at organisations within the Dutch industry and educational sector. It focuses more on the tools and communications that the ministries provide the technological companies and organisations.

2 Literature review

To get a better grasp of the potential dangers of cyber espionage within the Dutch industry and educational sector, certain definition and terminologies shall be explained. As several terminologies and espionage forms can overlap, this chapter explains the differences before the results are discussed. The characteristics that are described within this chapter will later be mentioned in other parts of the thesis. The literature review will be based on academic literature and grey literature, which includes media citations and governmental publications. We have chosen to include grey literature, through the Google search engine, Google Scholar and Dutch/English news articles, as many espionage cases and APT's are discussed in grey literature but are generally not represented as well in the academic literature. This means news articles in both Dutch and English are included, as well as documents and reports from either the Dutch government or other governments.

2.1 Cyber and industrial espionage

Cyber espionage is a new form of espionage that takes places in the cyber domain. Spying is said to be the world's second profession, as gaining an advantage ensures competitiveness and improves the likeliness of survival (Wangen, 2015). In general, *cyber espionage* can be defined as: "the activity of breaching computers and other endpoints to collect or damage information/systems through hacking or other techniques without the target knowing about the attack or consenting to it" (Dilek & Talih, 2022). The definition of regular espionage, which we will be following in the rest of the thesis, is as follows: "the access to sensitive information without obtaining approval by the holder of the information" (Thorleuchter & Van Den Poel, 2013). The definition of cyber espionage is somewhat similar to the definition of espionage which we are using. Cyber espionage specifically targets systems and/or networks of the victims, however. Cyber espionage can have various goals and targets: Libicki (2018), states that "Cyber espionage can create knowledge and help set up cyber attacks; yet, if discovered, it may alter the target's assessment of the intruder's capabilities and intentions". Cyber espionage can be used to determine the status, readiness, and intention of the other sides armed forces.

Van Os & Kole (2020) states that cyber espionage is used by certain countries like China and Russia to close the technological gap between themselves and the west and potentially even gain an advantage. To give an example of very current threats of espionage, Chinese IP (intellectual property) theft costs the United States between 225 and 600 billion dollars annually (Navarro, 2020). The European Commission has already issued a report in 2018 which concludes that the dangers of espionage are much larger than originally perceived and espionage poses a serious threat to trade secrets and can have a noticeably big economic impact (European Commission, 2019). Button (2019) states that the terms industrial espionage and economic espionage are often difficult to distinguish, as the interests of the state and companies often overlap, like in China. China currently has a massive reliance on cyber espionage and industrial espionage alike which Gilli & Gilli (2019) state. It is also no surprise that the high technology sector is especially vulnerable to espionage attacks (Sinha, 2012).

The Dutch universities and educational organisations are also involved in the process of collaboration of knowledge and technology. The aerospace engineering division of the TU Delft has already barred Chinese (PhD) students from entering certain fields of research (Teer, 2022). Other universities still allow Chinese students for computer science tracks. Sometimes, Dutch universities mention specifically about Chinese students that they are admitted due to two reasons: the first being that Chinese students look at problems differently and the second reason is to attract top talent from Chinese universities which only select the top students in the country per default (Ministerie van OCW, 2020). This is however an optimistic view on a difficult subject, as foreign students/scientists can be part of a strategy that countries with offensive cyber strategies have historically used to spy on Western academia/businesses (Borak et al., 2019) (Williams, 2022) (Ben Moshe, 2022). As mentioned before, in specific sectors, certain countries still need to gain more ground to be equal to Western countries.

These international students' networks allow foreign countries to gather information from foreign educational organisations and research institutions. And even if the original intent of students is not to spy for these state actors, the reach of these state actors into the lives of these students still allow them to use the students for information (Poreba, 2012). Dutch universities also claim that they do not work with universities in China which are part of the "China Defence Universities Tracker", but research by the Dutch government has also shown that this claim is false (Ministerie van OCW, 2020). The Dutch Intelligence agency (AIVD) has already warned the public of the higher chances of potential espionage and sabotage from certain state actors, because of a higher number of foreign-owned businesses (RTL Nieuws, 2022).

2.2 Cyber espionage laws and regulations

Dutch Regulation is lacking behind the trend of current cyber espionage activities (AIVD, 2022). With new regulations currently being proposed, more modern ways of espionage will be made illegal, these newer forms will also carry a larger punishment than before. Currently the laws against cybercrime are: The "Richtlijn voor strafvordering cybercrime" and Article 138a/b of the Dutch Criminal Law. The common law against breaches in personal computers in Dutch is called the "Wetsartikel computervredebreuk". This article is an addition onto the article of trespassing, so it is not necessarily part of a separate legislation. The "Wetsartikel computervredebreuk" is a generic legislation about the breaking and entering of a computer. This crime is either punishable by a prison sentence or a certain fee that must be paid. The legislation does have certain requirements and definitions from when someone would be in offence to this law. An example would be to digitally impersonate someone by forging certain keys (OM, 2019).

Another important piece of legislation is the Vifo (Wet veiligheidstoets op investeringen, fusies en overnames), this legislation has been in effect since the first of June 2023. This has allowed the Dutch government to intervene with certain takeovers that might happen within certain critical sectors. It has given the government several tools to deal with investments and fusions of certain companies.

The two core categories for which this legislation was made are companies within the vital sector, and companies that hold sensitive technology. With this legislation the Dutch government has more tools to prevent unwanted takeovers that might harm Dutch national security, which includes economic interests (EZK, 2024). Another important control will be the security check on foreign researchers, students, and teachers, this is called the 'Wet Screening Kennisveiligheid' which means law (for) screening knowledge security. This check along with a package of other controls is aimed at reducing the chance of knowledge exploitations by state actors. In the same letter that has been sent to the House of Representatives, the minister calls for improvements to the field of knowledge security policies within universities and specifically mentions the lack of overview about the current foreign partnerships and financing they receive (OCW, 2023b). This letter has not been received that well by the scientific community as there have been responses by for example the KNAW, which is the Royal Dutch Academy of Sciences. They are a general overseer of scientific principes in the Netherlands.

In the statement by KNAW they denote that the law is too complex to be executed by the universities, and states that blocking researchers that will be working in high-risk areas is damaging the scientific principles (KNAW, 2023). Other than that, the KNAW states: The ministry should use a custom approach for the different areas of expertise within science and that researchers themselves are the ones that should be spotting where the dangers and sensitivities in the research will be.

There are regulations and agreements fore different cybersecurity topics, such as breaking and entering of computers/networks. But generally, legislation for cyber espionage is lacking. China, for example, has promised to reverse its prominent policy position and has committed not to engage in commercially motivated cyber espionage (Banks, 2017). Like explained in section 2.1 before, this promise only seems to be done on paper, as Inkster (2015), shows that China has been linked to many cyber espionage cases over the years. Lindsay (2015), shows that several members allegedly linked to the Chinese People's Liberation Army have been indicted on several counts of industrial espionage. Another example is the APT group called APT 40 or otherwise known as "Leviathan", which is linked to the Chinese MSS Hainan State Security Department (APT40, CISA, 2021). This group has been involved in various cyber-attacks by using different methods and techniques and is generally considered a state sponsored attack group which focuses on espionage (Leviathan | MITRE ATT&CK®, n.d.). This group often targets military technology, but they have also been found targeting universities which research maritime technology (Mandiant et al., n.d.).

Even though the Sulmasy & Yoo (2007), state that international law does not allow for intelligence collection within foreign states, in peace or wartime, however regulation of intelligence gathering has historically always been left to domestic enforcement. This information collection can also be used to track down terrorists and the proliferation of mass-destruction weapons, which in turn causes the collected intelligence to protect nation states and promote peaceful solutions to violent conflicts.

2.3 Cyber Security

Cyber security is defined by the NIST as: "the ability to protect or defend the use of cyberspace from cyber attacks" (NIST, n.d.). Cyber security can also often used as an all-inclusive term. In this thesis 'cybersecurity' will be defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (Von Solms & Van Niekerk, 2013). (Thakur et al., 2015) defines cyber security as a measure to protect computer systems, networks and information from disruption or unauthorised access, use, disclosure, modification, or destruction. Cyber security is now something all organisations will have to deal with or have been dealing with for a longer time. At the time most of the economic, cultural, and societal challenges are also formed in the digital dimension, which makes the need for good cyber security even more important (Li & Liu, 2021).

Another frequent problem of cyber security is about the responsibility of the cyber security risks and regulations. Who is responsible for enforcing the cyber security regulations internationally, while national regulations often end at the border. Large infrastructure is usually privately owned, and this makes protecting national interests/security even more difficult (Hiller & Russell, 2013). The end-users are often regarded as the weakest link in the security chain, while the technology is sufficiently protected, the fault is often at the users (Yan et al., 2018). To deal with this phenomenon, a new way of looking at security has been created. The security culture, this culture is part of organizational culture and focuses on implementing a security awareness within the existing organisational culture (Ruighaver et al., 2007).

To deal with cyber security in a more organised fashion, certain information security standards have been constructed. Originating from the BS-7799, several other ISMS (Information Security Management System) standards have been created. The most popular one arguably is the ISO 27001 (Broderick, 2006) (Susanto et al., 2011). The ISO 27001 offers organisations a methodological way of creating a baseline of security by implementing an ISMS. The ISO 27001 ISMS is used to achieve that certain baseline. An organisation can obtain a certification if its infrastructure and operations match the requirements laid out by the auditing boards. The ISO 27001 certification does not have a significant impact on business performance, but it is seen more as a regulatory obligation (Hsu et al., 2016).

In the newest version of the ISO 27001:2022, cloud security is also included. The research from (Malatji, 2023) shows that cloud computing has become more popular in several industries and carries a lot benefits, but also some security challenges with it. There are technical and organisational challenges when using cloud-based technology, as cloud computing still deals with the problems of the loss of rights, controlling of data, availability of data and regulations (Ali et al., 2020). Data stored on the cloud can also count on attacks from the outside, but also from insider threats. This is because cloud providers themselves are also untrusted (Shi, 2018). There are however also clear benefits to using cloud technologies, like high scalability, limited maintenance efforts, cost savings, and less energy usage (Anggraini et al., 2019) (A. Singh & Chatterjee, 2017).

2.4 Risk management

In the current world in which cyber-attacks are permanently ongoing, securing the operational processes of an organisation is an important challenge, organisations can combat with risk management. Risk management also gives organisations insight into their crown jewels, important operational processes and gives them a methodological way of securing these said crown jewels. (Bojanc & Jerman-Blaič, 2008). Standards like the ISO 27005 give organisations levers to implement risk management step by step. Putra & Mutijarsa (2021), state that the ISO 27005 can be difficult to understand for newer implementers because of its wide use of technical expressions, interpretations, and technical terminology. To fully make use of an integrated security approach, organisations are recommended to implement the ISO 27005 together with the ISO 27001 ISMS. After an ISMS is implemented, it is also often recommended to implement additional security standards, as an existing ISMS is easier to further build upon (S. J. Putra et al., 2020).

2.5 Espionage cases

Currently, espionage against corporations' innovations and technological advancements are prime targets for espionage (Thorleuchter & Van Den Poel, 2013). Specifically, China has a lot of ground to gain when it comes to technological innovation. After 1978 China had to do something as the country was in a desperate shape. China opened its border for Western investment, the main goal was to gain Western technology through licit but mostly illicit means (Lewis, 2013). Lewis (2013), also states that China has no tradition of protecting Intellectual Property (IP) and this trend does not seem to change over time. Even though China has been successfully stealing innovations through several methodologies of espionage, it will not instantly be available for China to use. There are more factors at play to understand and use innovations that were created in another language and by other cultures/people.

The damage a nation state might experience, is dependent on what kind of information has been stolen. Important intellectual property being stolen might not instantly translate into damage for a nation/company, as technology can be difficult to replicate instantly. But for confidential business information the monetary damage might be far greater, and will also be experienced faster. What kind of information is being stolen by nation states depends on the current trend of technology, like was seen with the high-speed trains in Germany and Japan and investing in green energy in the US (Lewis, 2013). The long-term effects are also dependent on certain variables, like whether important IP was stolen, or a lot of information has been lost, but industrial espionage can lead to loss of corporate and tax-revenues, which in turn leads to a lesser ability for a nation state to maintain its spending program for military capabilities, social benefit, or healthcare (Jones, 2008).

An important example of the potential negative geopolitical effects an espionage case can have, is the stealing of technology chip data by a Chinese employee of ASML. As (*Bloomberg*, 2023) describes, ASML accused a China-based employee of stealing important chip data from its manufacturing plant. This case also exacerbates the political tensions that already exist between countries like the USA, China, and the Netherlands.

2.6 Defending against espionage

Espionage has a physical component but in the current day and age a far bigger digital cyber component. Many different countries have invested into their cyber security strategies which includes the security services that operate digitally (Deibert et al., 2009). As espionage is now also very much a digital activity, fighting espionage also becomes a cyber security task. Physical attacks on nations can often be considered an act of war. Libicki (2017), describes that the United Nations Group of Governmental Experts have states that existing international law for conventional combat also applies in cyberspace. Which means that nation states may not carry out cyberattacks with the intent violating a systems integrity or availability, in other words, sabotage the system. The act of espionage by nation states has however been described as acceptable state behaviour, as this is also the case for espionage not within the cyber-domain.

These rules are often not concrete enough to fully capture the weight some of these cyber attacks can have. There have also been initiatives to create norms to try and create an even playing field, but this has also proven to be difficult to implement (Libicki, 2017).

2.7 Economic security/espionage

Within the Dutch government, the ministries usually divide economic and knowledge security as they have different meanings. These classifications are often categorised under the bigger definition of espionage. To be able to thoroughly research espionage within the Dutch Government it is critical to use the terms and definitions they themselves apply, otherwise comparing definitions and terminology will become increasingly difficult. Industrial espionage can be compared to economic security in the Netherlands, but sometimes the term “economic espionage” is also used within scientific articles to describe similar problems.

Bellaby (2023), describes that even though sometimes the impact of economic espionage might feel like it is lower than of its industrial/cyber counterparts, this is in fact not true. Economic espionage could even have a significant effect on the day-to-day lives of certain people. Individuals can experience direct hinder from economic espionage, as many people will be affected at once. The society of a country is often linked to its economy, which is why destabilizing the economy can hurt social cohesion, well-being, and stability. These can translate into economic compound harms, which could include an increase in crime, loss of education and progression opportunities.

These considerations become increasingly alarming when mentioning nation states committing economic espionage. China is a country that has historically been very dependent on Western literature and open-source scientific knowledge

(Lee, 1982). Even to this day, China is in some technological aspect's dependant on Western countries (Hannas et al., 2013).

A while ago, the Office of the National Counterintelligence Executive's 2011 report Foreign Spies Stealing US Economic Secrets in Cyberspace boldly asserts: "Chinese actors are world's most active and persistent perpetrators of economic espionage." (Hannas et al., 2013) Various nation states are active in stealing overseas knowledge and technology, which has an exceptionally significant impact on the nation states which the information is being stolen from. Nation state actors often use co-opted insider threats to gather information on national adversaries.

2.8 Methods of threat actors

In this section several methods for classic espionage, economic espionage and knowledge espionage are discussed. As espionage as a profession is quite old, methods have evolved over time. Firstly, we discuss older ways of espionage to give a background about older methods that might have inspired new ones. Afterwards, we cover more modern approaches. For example, how certain APT's function and perform their attacks.

Classic economic espionage

Espionage has a long history and there are several methods that have historically been used, also for economic espionage. Fraumann (1997), shows that there is also a physical side of espionage which can also be exploited for economic espionage; These often rely on surveillance, observation, and photography. But it can also involve illegal trespassing and stealing physical documents and other data-containers (e.g. USB-sticks). There are intrusive and non-intrusive methods that can be (mis)used. Some of the aspects of intrusive methodology focus on misusing the human psyche. This could eventually translate to blackmailing or extorting someone to get the sought-after information. These methods can involve the usage of a good-looking person, but also the use of prostitutes to create a situation in which extortion becomes feasible, these people try to create a relationship with another person to potentially siphon information. For organisations there are also notable risks that are created by direct competitors and malicious intent of their (own) employees. This can differ from planting a mole into a competitor's organisation but also by organising fake interviews with employees that might have trade secrets.

Advance Persistent Threats (APT's)

Singh et al. (2016), show that APT's and other criminal entities can use several different methods within their tactics, techniques, and procedures (TTP) to collect proprietary information involving certain trade secrets. There are the more classical ways of unauthorized access to protected environments, such as eavesdropping through wiretapping, bugging offices, or capturing cellular telephone conversations and of course brute forcing access into an electronic device through hacking.

APT's attacks often go through several phases, like described below:

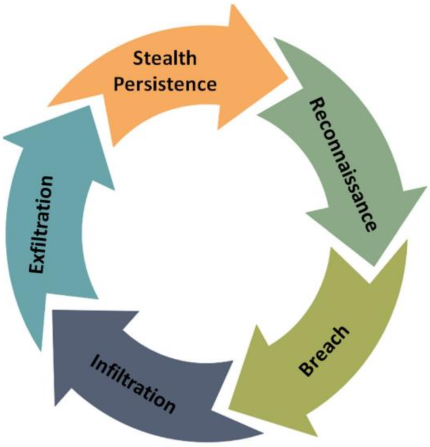
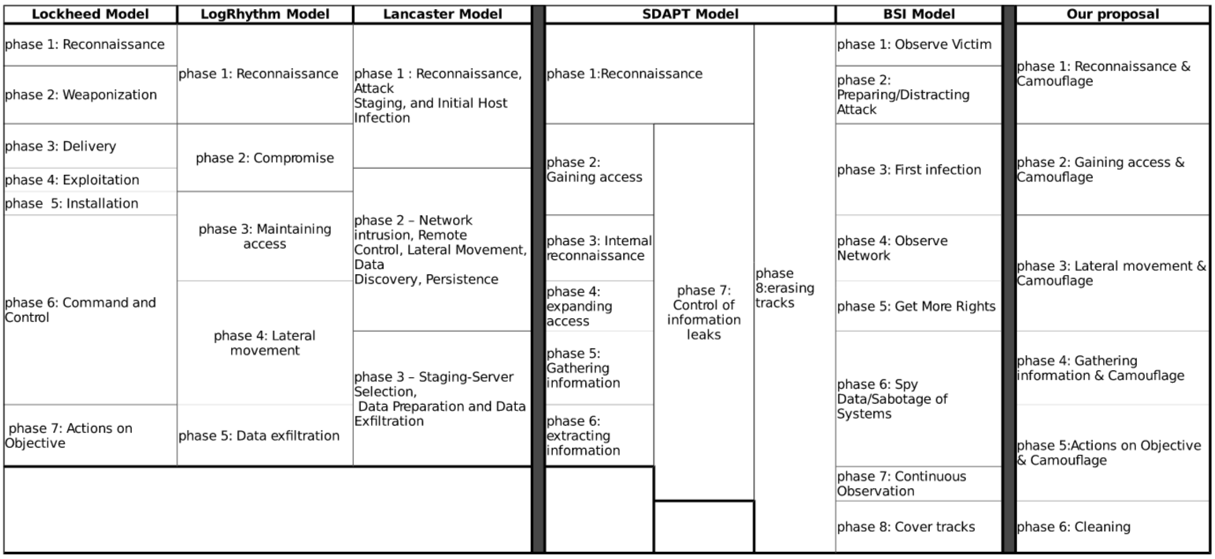


Figure 2: APT methodology phases (Singh et al., 2016)

The phases describe the different type of actions and behaviours that an APT attack goes through. Below we will shortly describe each phase and what it entails, we will also discuss any common methodologies. As not every cyber attack is the same and even within the security world, not all cyber kill chains look the same (Mazurczyk & Caviglione, 2021), we will denote a general concept of the phases.

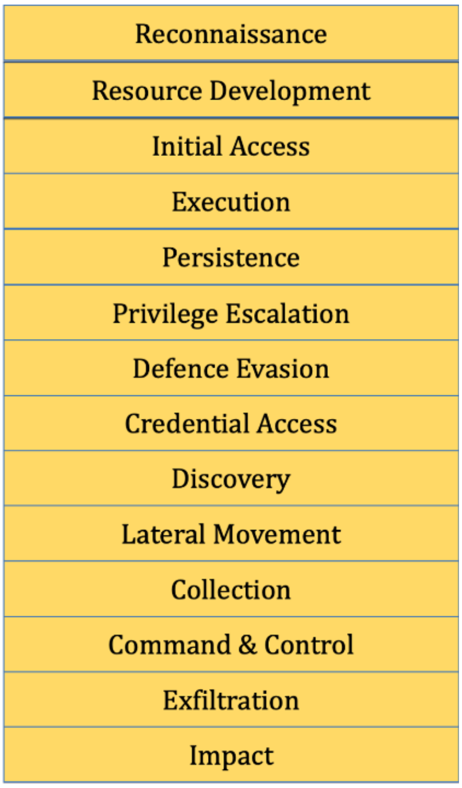
As there are different threat modelling models, comparing them to see any overlap is important. If any overlap is detected, each phase can be identified without the loss of information or context from the initial model. Below in figure 3, Messaoud et al. (2016), created a comparison between the different threat models, with a proposal for a common threat model with six separate phases, these phases are dynamic and not all attacks follow the same pattern.



Lockheed Model	LogRhythm Model	Lancaster Model	SDAPT Model			BSI Model	Our proposal
phase 1: Reconnaissance	phase 1: Reconnaissance	phase 1 : Reconnaissance, Attack Staging, and Initial Host Infection	phase 1:Reconnaissance		phase 8:erasing tracks	phase 1: Observe Victim	phase 1: Reconnaissance & Camouflage
phase 2: Weaponization						phase 2: Preparing/Distracting Attack	
phase 3: Delivery	phase 2: Compromise		phase 2: Gaining access	phase 7: Control of information leaks		phase 3: First infection	phase 2: Gaining access & Camouflage
phase 4: Exploitation		phase 2 – Network intrusion, Remote Control, Lateral Movement, Data Discovery, Persistence					
phase 5: Installation	phase 3: Maintaining access						
phase 6: Command and Control			phase 3: Internal reconnaissance			phase 4: Observe Network	phase 3: Lateral movement & Camouflage
	phase 4: Lateral movement		phase 4: expanding access			phase 5: Get More Rights	
		phase 3 – Staging-Server Selection, Data Preparation and Data Exfiltration	phase 5: Gathering information			phase 6: Spy Data/Sabotage of Systems	phase 4: Gathering information & Camouflage
phase 7: Actions on Objective	phase 5: Data exfiltration		phase 6: extracting information				phase 5:Actions on Objective & Camouflage
						phase 7: Continuous Observation	
						phase 8: Cover tracks	phase 6: Cleaning

Figure 3: Comparison between different threat models (Messaoud et al., 2016).

The MITRE attack framework has a lot of different threat models for different attack surfaces, the different tactics that the ATT&CK framework describes can be found in figure 4:



Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defence Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

Figure 4: The different Tactics of MITRE ATT&CK Framework of Intrusion Analysis (Naik et al., 2022).

In the comparison made between several threat models, Messaoud et al. (2016), shows that several models have their own distinct characteristics, advantages, and disadvantages, which makes the use of these models' dependant on the needs of its user. To give more information about the separate phases within each model that have been described in figure 3, some of the phases will be expanded further upon to give a global image about the attack methodologies. The attack phases below can be used by any threat actor.

Reconnaissance / observe victim(s)

Reconnaissance activities are of the key stages when discussing successful attacks. Reconnaissance or recon in short in cybersecurity refers to the process of obtaining as much information about a target system or network as possible that might be needed to successfully infiltrate said system (Roy et al., 2022). Even though it is difficult to fully grasp every method used by threat actors, Mazurczyk et al. has tried to categorise the evolution of cyber reconnaissance techniques into four classes: internet intelligence, network information gathering, side-channel attacks, and social engineering (Mazurczyk & Caviglione, 2021). These techniques might give an attacker information about the network structure and other key factors (Ahmad et al., 2019).

Breach / Weaponization / Gaining access

Any information that has been found which can be used to breach or infiltrate a specific network or endpoint will now be used. Ahmad et al. (2019), show that the following information that was collected in the recognisance stage can be used for an attack: "open ports, access points, addresses, firewall or intrusion detection or prevention system characteristics, the currency of active systems, running software applications or services, virtual hosts or platforms, or storage infrastructure". It could also be that access is earned through malware sent through e-mail, in this method not much is known about the structure of the network beforehand (Ahmad et al., 2019). Attackers often take measures to try and hide their breach from victims, by using several techniques, for example by stealing valid credentials (Brewer, 2014).

Infiltration / lateral movement / expanding access

In this phase the threat actor already has access to the system of the victim. Once this access is achieved, they will attempt move throughout the system, but will use several techniques to prevent their presence, like using a valid user account as to not raise any suspicion (Brewer, 2014). In the research done by (Tian et al., 2019) they show the capability of monitoring this lateral movement across a cloud network environment, but being able to effectively monitor is also dependent on the way the attacker has achieved access and has the way they decide to move across the network. The lateral movement within a network allows attackers to continually siphon information from multiple places in the network. But this lateral movement also allows attackers to try and gain higher privileges in other systems they might have detected, or even wait for new targets to appear (Chen et al., 2018).

Exfiltration / spy data / data exfiltration

Data exfiltration is for many threat actors the main reason for executing an attack (Ullah et al., 2018). By exfiltrating data, attackers will leak sensitive or confidential information/data to an unauthorised organisation. This phase can both be executed by external threat actors, but also by internal threats (Ullah et al., 2018). A current great threat to networked systems are malware attacks and botnets that are operating worldwide (Al-Bataineh & White, 2012). Attackers also use sophisticated techniques to hide their data exfiltration such as: the use of encrypted traffic and thwarting of the IDS (intrusion detection system) by not using any perceivable anomalies in their HTTP(S) requests (Al-Bataineh & White, 2012).

With the GDPR being active in the EU, this has renewed the pressure on organisations to safeguard their data. It has also shown the importance of being capable of responding quickly to weird traffic on an organisations network (Steadman & Scott-Hayward, 2018). There are ways for organisations to detect this rogue traffic and data exfiltration attempts. One of the ways involves actively looking at DNS traffic more thoroughly. DNS traffic is usually allowed to move throughout the firewall without deep inspection or state maintenance, thereby providing a great opportunity for attackers to encode low volumes of data without fear of detection (Ahmed et al., 2020). Suresh et al. (2012), also plead for the development of a data exfiltration monitoring tool that is specifically targeted at highly confidential data.

Stealth persistence / erasing tracks / cleaning

As mentioned before, attackers can use several techniques to mask their identity while already having access to a network. Threat actors can also use many other methods to erase any potential tracks they might have left of their presence. (Messaoud et al., 2016). A potential method for attackers is to use the many anti-forensics tools which they have at their disposal. It is often the case that cyberattacks are dynamic and the separate phases are not followed in a chronological order. One potential method of threat actors is using the so called 'inertia state', in this state they will remain in the network for weeks to several months without emitting a single signal of its presence, during this period they can evaluate their attack. Attackers would also like to delete any potential evidence of their presence on a certain system.

Majed et al. (2020), define four categories which aim to hinder the forensic process: artifact wiping, data hiding, trail obfuscation and attacks against forensics tools & processes. Normally when deleting a file or folder, this data will remain on the disk, and will only be deleted if it is overwritten by other data. Artifact wiping focuses on erasing and destroying data. With data hiding, attackers will make it impossible to find certain digital trails on a device, making forensics research nearly impossible. With trail obfuscation, attackers purposefully plant false information and counterfeit evidence, this can be done by altering information in certain logs for example. Attackers can use program packers and anti forensics tooling that minimize the digital footprint to disrupt the forensics tooling of researchers. Other methods can include but are not bound to: memory injection, syscall proxying and using local bootable media (Majed et al., 2020).

All the phases above are not set in stone, and do not necessarily follow a chronological order. With stealth persistence for example, several tools and methods are also used during other phases.

3 Related work

To understand the state-of-the-art literature related to the thesis topic and to demonstrate the research gap that the thesis addresses, this chapter discusses academic pieces around espionage, knowledge- and economic security. These pieces have been searched for online with the help of Google Scholar and the search function within individual scientific journals. Articles published by: IEEE, Springer, Elsevier, Sagepub and Wiley, Taylor & Francis have been referenced, as these journals have many pieces available on information security, espionage, and public sector governance, which have been essential for this thesis.

Cyber espionage within legislation

Buchan (2021) describes how the Netherlands currently handles cyber espionage within the boundaries of the Dutch law. This article also investigates the question whether remote access of a system breaches the territorial sovereignty of a state, which remains unclear as of now. The article also researched whether in general terms of international law, political and economic cyber espionage breach the principle of territorial sovereignty. According to the paper, there is little doubt that cyber espionage operations breach the principle of territorial sovereignty. But whether remote access cyber espionage operations breach the same territorial sovereignty remains uncertain. The paper names certain organisations such as the World Trade Organisation, which could play a role in the persecution of countries that breach this territorial sovereignty, but whether this happens, is still unclear. The paper specifically talks about the caveats that exist within the cyber espionage domain, especially when comparing it to international law. However, there is no link to how the governments within the different countries monitor this specific espionage.

The paper rather focuses on proving whether cyber espionage breaches the territorial sovereignty of nation states. The article references certain G20 documents which state that they will not partake in ICT-enabled theft of IP, but this seems a rather optimistic take, as we argue in this thesis that China is still actively involved with industrial espionage.

Based on multiple academic, and OSINT (Open-source intelligence) sources, we conclude that China does not hold up their end of this promise. Whether they are state sponsored hacking groups or criminal organisations operating from within China, industrial espionage is still being performed by China.

Yoo (2015), describes that there are disturbing impressions that the capacity of technology has far exceeded policy thinking in the domain of cyberwar. The paper gives some recommendations on how international policies should clarify, whether cyber actions fit into the current existing law and legislation. The paper gives more details about how cyber operations currently do not fit in a classis case of warfare legislation, as there are no clear casus belli when dealing with cyber attacks that focus on espionage and economic damage. In general, the law and legislation need to catch up to the current development of technological capabilities within cyber warfare. There does not seem to be a pan-national answer to the dangers of espionage within the cyber domain.

Industrial and cyber espionage threat actors

Hannas et al. (2013), discusses the historic reliance of China on Technology from the West and how current espionage practices play a role for China in obtaining their needed relevant technology. Combined with the fact that China is actively trying to steal information to use in their military, this is a dangerous combination. The book also talks about dealing with non-reciprocators to make sure international scientific projects can exist, while not losing the existing competitive edge certain countries might have. The book not only discusses the industrial espionage, but also has a dedicated section for the Chinese cyber threats, which are also amply described in this thesis. The name of the book is: Chinese Industrial Espionage, as the name implies, this book focuses its scope on the dependency of China on Western technology. In this thesis, we discuss China as one the many nation state threat actors that might harm Dutch interests.

Jonsson (2023), discusses the war in Ukraine and how this has allowed European intelligence agencies to take centre stage. The article mentions multiple espionage convictions within Europe in the 2010-2021 timeframe. This article has tried to differentiate from earlier research in this field, by not using singles-case studies which are mainly of Anglo-Saxon origin. The researcher also denotes that they were not able to compare the dataset of espionage within Europe to a dataset of espionage within the USA, which means they cannot take certain conclusions about the similarities of contemporary espionage cases in Europe and the USA.

Liebetrau (2022) talks about three different NATO members, namely: the Netherlands, France, and Norway. The article talks about a vacuum that has been created by differing strategic environments characterised by increasing cyber conflict which is short of war. It challenges the idea of offensive cyber capabilities purely as a warfare matter. The article asserts that the current lack of strategic guidance is a fundamental challenge, that puts European societies at risk and undermines democratic governance, as navigating the new space of strategic cyber competition is a significant challenge to contemporary European statecraft.

As this thesis also tries to include several cyber espionage policies and international legislation to see whether these are effective, cyber conflicts are often included in these pieces. To fully understand the problems that arise within the digital domain, this article defines the challenges that currently exist, and how three countries, namely: France, Norway and the Netherlands have developed offensive cyber capabilities over the last fifteen years. This article does not answer the question what kind of and how frequently cyber countermeasures are launched as these are often ambiguous and secretive. This article does include the political problems that have occurred and the importance of legislation for certain challenges.

Thonnard et al. (2012), describes how malware can be used for several dangerous goals, like real-world destruction, cyber-terrorism, and industrial espionage. The article researches several ways attackers use malware, how these threat attackers get access to certain systems and the eventual goals these criminals might have. This article is very much focused on the functionality of malware and the associated malware deconstruction. Even though (nation state) threat actors use malware for various use-cases, the article describes how several malware attacks used zero-day vulnerabilities to deploy their malware at their targets. Most of the research data is provided by the "Symantec.cloud" during the year of 2011, which means that the research data is somewhat dependent on the detection rules of said "Symantec.cloud". In this thesis we describe that nation state actors use several methods of entering systems and potentially sabotaging them, but in general keeps it broader than only malware. The article does provide valuable insight into the deployment and danger of several malware types for specific organisational types like governmental agencies and specific business units.

Jung & Jung (2020), talk about the classification of espionage cases and seeks countermeasures by analysing the trend of industrial espionage activities. The paper argues that the importance of corporate intellectual property and technology is increasing because of the development in the modernisation of current-age societies. Just like in this thesis, they mention that the current cyber legislation cannot keep up with the growing amount of IP that private companies hold. The paper relies, however, on "public" information that is searchable on an online portal site. The portal delivers an overview of the incident, but does not provide in-depth information needed for analysis. The paper does describe certain characteristics of industrial espionage and included threats to SMEs.

Research collaborations in the context of cyber espionage

Snetselaar (2022), describes knowledge security problems that can arise when working together with China in research collaborations. The article offers crucial insights into how the great power rivalry is shaping scientific research and the international exchange of knowledge and technology. The authors describe that in future iterations of this specific research topics, corporations like Huawei should be included to take a more symmetric approach towards the research design. They would also like to explain terms like knowledge security and technological sovereignty. In this thesis, the topics: knowledge security-and economic security are very important to the core research questions. Just like in the article by Snetselaar (2022), we also argue that research collaborations with China can be of added value. We, however, argue that certain security criteria must be met before these collaborations are started and that high-risk technology should generally be avoided in these collaborations.

Adams et al. (2021), talks about the fact that collaborating with China in research collaborations often provides China with disproportionate benefits that some national research policies have not yet accounted for. In the UK, there have been an increased number of papers released in collaboration with Chinese-based researchers, and research between the UK and China is often concentrated in technology-based fields. The article also discusses various policy consequences which exist because of the risks these collaborations could entail. The article does argue that Chinese researchers are getting full insight into the research methodology used by the British, while the question remains if the British are getting an equally candid view of their Chinese counterparts. While the article does talk about potential pitfalls of collaborating with the Chinese, there is no mention of knowledge security. The article describes some form of contract as a mediation for potential problems that can arise when collaborating with the Chinese, even when researching high-risk technology. In this thesis, we also discuss the topics of high-tech research collaborations with China and various associated threats.

J. J. Lee & Haupt (2020), describes the winners and losers within US-China research collaborations. This article describes that in the past few years, China has been funding and publicizing way more research collaborations than before and will catch up to the US in released publications in time. The article talks about the benefits of China-US research collaborations, but also discusses some of the security concerns that exist within these collaborations. The security concerns quickly disregarded however, as the authors see China as an industry leader in these research domains and not as a net-benefiter of these collaborations. The article also describes these collaborations from a positive-sum point of view, which observes scientific advancement as a global good.

One chapter of the book written by Johnson (2019) talks about the role of national security intelligence agencies within American universities. The chapter discusses the difficulties in attributing certain individuals as spies while they move overseas to study in a foreign university. The book does mention that these espionage activities are happening, but that branding every foreign student as a potential spy, is equally dangerous. The book also discusses cases in which certain American professors have been linked to the CIA, and if this is a positive or negative development. In general, the notion of freedom for academia and academics, seems to be particularly important to the author.

We see that most of the existing academic literature in this field focuses on one of the following topics: industrial espionage, (broader) espionage, knowledge security, cyber warfare, legislation within the cyber domain or other cybersecurity related topics, and not necessarily a combination of these topics. To the best of our knowledge, nobody has yet researched how national governments aim to monitor cyber espionage activities in a qualitative study. The context of the Dutch government has also not been addressed in the literature. However, there is a rich literature covering studies with humans in the role of experts in their professional field: like the following paper by Haqaf & Koyuncu (2018), which is about the key skills required for information security managers, the paper by Boroš et al. (2019), which is about the required competencies of security managers, and the paper by Caruson et al. (2012), which is about cybersecurity policy making at a local government level. These papers describe key functions and the skills required for correct governance and policy creation within the cyber security field. As the Dutch government also creates policy for espionage and relates subjects, identifying crucial variables is important for our own research. Our study thus follows a rich tradition of human studies but addresses a new and timely research topic.

4 Document analysis

To give an indication of some of the work the Dutch government is already doing regarding the topics; espionage, economic- and knowledge security, the document analysis in this chapter serves as a different type of literature review. Instead of focusing on academic articles, this document analysis focuses on the documents and articles that the government, news stations or educational organisations have released. These documents have been analysed before the interviews were conducted, and some of the documents have been analysed after multiple participants mentioned these documents in the interviews (or changes thereof). The documents have been selected based on their correspondence with the thesis subjects. So, documents or policies mentioning knowledge- and economic security or espionage have been taken into consideration. Documents or policies mentioning national security have also been considered. This effectively means that the following documents have been selected: "Risicoanalyse nationale veiligheid bij inkoop en aanbestedingen (National security risk analysis in purchasing and tenders)", "Dreigingsbeeld Statelijke Actoren 2 (Threat assessment of State Actors 2)", "AIVD Annual Report 2022", "Cybersecuritybeeld Nederland 2023 (Cyber Security Assessment Netherlands 2023)", "Jaarplan 2024 (NCSC) (Year plan 2024 NCSC)" and the "MIVD Annual report 2023". There have also been various policies which have been researched but did not necessarily make it into the document analysis, as they gave us good background information, but were not relevant enough to directly mention here.

By reading the various documents and denoting the most important parts we could summarize the documents in a way they were relevant to this thesis. This document analysis should also give a brief introduction to the current level of awareness of the government and potential improvements they are looking to implement in the future. The document analysis focuses mostly on identifying the different documents defined by the government and some academic literature to further expand on the information given by the governmental topics. We have specifically sought out documents online through the Google search engine, Google Scholar and the governmental document portal to find documents that are publicly available. There are also some instances of using Google Scholar to find academic pieces which were created in Dutch in collaboration with the Dutch government. This means both English and Dutch search terms were used in finding the sought-after documents. Since we either knew about the documents beforehand or was directly informed about the existence of these documents by participants in the interviews, these items were easier to find. Laws like the "Wet uitbreiding strafbaarheid spionageactiviteiten (Act on expanding punishability of espionage activities)" and the "Wet screening kennisveiligheid (Knowledge security screening act)" have been discussed during the interviews to ask questions about creation and intent the public officials have with these policies or laws. This way we could also directly ask if these policies had the actual impact that was calculated beforehand.

The difference with the earlier literature review, however, is the focus on the governmental documents and not necessarily academic literature. Within this document analysis, we have expanded on laws and regulations that have been either discussed during the interviews or have been researched before the interview phase had initiated. This is also the case for policy pieces or tools released by the government. The document analysis eventually serves the purpose of combining both the knowledge of academic articles together with the real-world experiences of the government and their public officials.

These documents have been used during the creation of the interview questions to make sure that policies that are either new or important for the thesis topics could be discussed. To properly adhere to the reflexive practice that had been described in a prior chapter, it was important to know about the different policies that the different ministries have been working on. This way actual questions could be asked that fit the roles of the participants.

The document analysis starts with a general overview of the ministries that are creating the relevant documents for this thesis and a few examples that mention espionage. Afterwards, the document analysis focuses on the following topics: espionage, economic security- and knowledge security with some examples of choices that have already been made. At the end, a small section is dedicated to state actors as the importance and danger of the different state actors have been re-iterated many times during the interviews.

Document creating organisations

There are several important organisations which release documents that are relevant for this thesis. The AIVD (General Intelligence and Security Service), MIVD (Military Intelligence and Security Service), NCTV (National Coordinator for Security and Counterterrorism) and the Dutch NCSC (National Cyber Security Centre) are organisations which publish information that is relevant for the Dutch public. All these aforementioned organisations have their focus points, which allows the documents to handle different topics as well. Some of the documents that have been created, have been in collaboration with multiple organisations. An example of one of these collaborations is the "Dreigingsbeeld Statelijke Actoren 2 (Threat assessment of State Actors 2)" created by the MIVD, AIVD and NCTV (AIVD, 2022). Figure 5 visualises the different documents and who has either co-authored a document or provided valuable input.

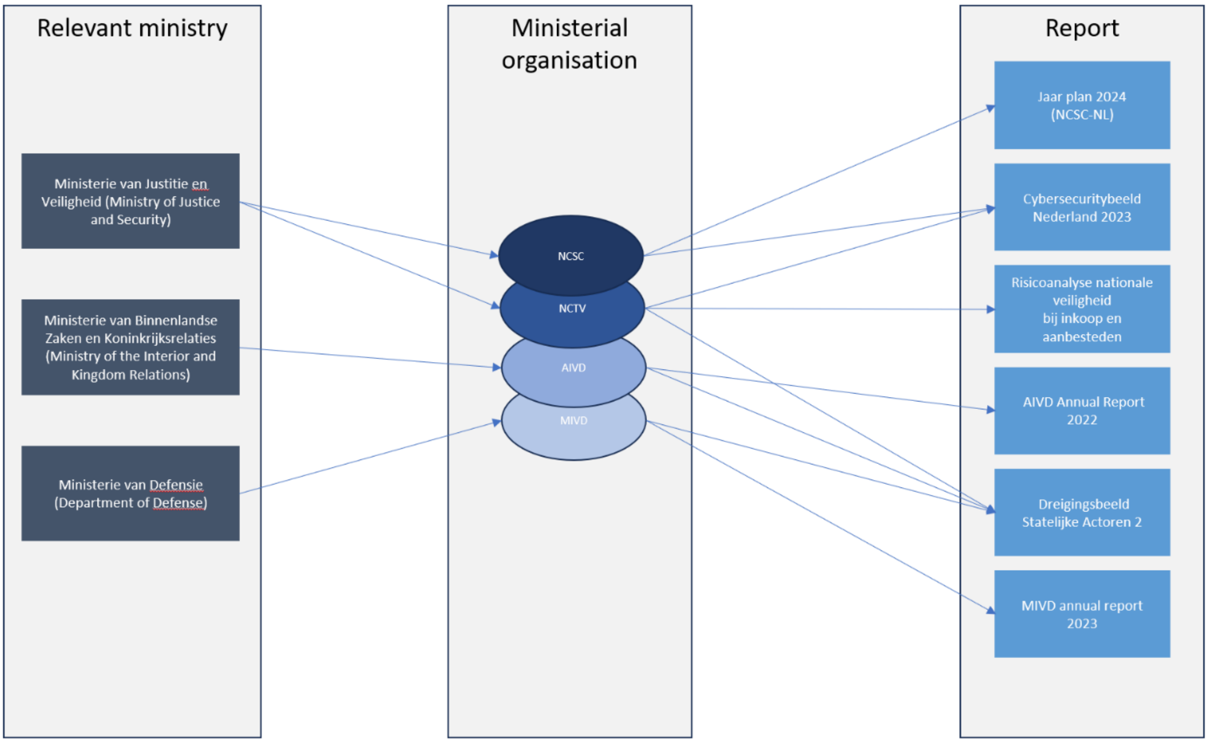

Relevant ministry
Ministerial organisation
Report
Ministerie van Justitie en Veiligheid (Ministry of Justice and Security)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministry of the Interior and Kingdom Relations)
Ministerie van Defensie (Department of Defense)
NCSC
NCTV
AIVD
MIVD
Jaar plan 2024 (NCSC-NL)
Cybersecuritybeeld Nederland 2023
Risicoanalyse nationale veiligheid bij inkoop en aanbesteden
AIVD Annual Report 2022
Dreigingsbeeld Statelijke Actoren 2
MIVD annual report 2023

Figure 5: Visualisation of important documents and (co-)authors.

As can be seen in Figure 5, several ministries and ministerial organisations are involved in writing the reports that concern the following topics: espionage, knowledge-and economic security and cyber security. Several documents, like the "Dreigingsbeeld Statelijke Actoren 2" have been referenced in this thesis to describe certain threats that the Netherlands currently faces and, in the future, will face. Some documents that have been referenced in this thesis will be from other ministries, but they have been referenced accordingly. With these documents, the government tries to be transparent towards the Dutch public, which is also mandated by a law called "Wet open overheid (Woo)" (Min-AZ, 2024).

4.1 Political and governmental espionage

The Dutch General Intelligence and Security service (AIVD) produces yearly reports on the status and dangers of certain foreign state actors. This report called "Dreigingsbeeld Statelijke Actoren 2", is made together with the NCTV (National Coordinator for Security and Counterterrorism) and MIVD (Military Intelligence and Security Service). These government agencies track and document several different threats that certain state actors pose for the Netherlands and its citizens. One of the focus points within this report is the danger of cyber espionage and economic security. They describe that certain state actors pose threats and have offensive cyber strategies against the Netherlands.

The Dutch government has already taken some steps to improve the rigidity of its own national government and therefore reformed some parts of its internal rules and procedures. A recent action within this plan, is the ban on certain apps from the work devices of public officials (Ministerie BZK, 2023). Included in the list of banned apps, is the Chinese app "TikTok". Even though TikTok claims that they are a private company, people still fear the Chinese government has a hand in the organisation (Wang, 2023). A mechanism China uses to create influence is a term named "corporatism". In a corporatist arrangement, a government only recognizes one national organisation as the sole representative of the sectors interest (Unger, 1996). The Chinese government however has a history of political involvement into private sector organisations (Livingston, 2022). China's obvious intervention into its "private sector", has many international trading partners questioning how much they want to accommodate these partners. For TikTok and other Chinese-owned apps, the Dutch government has decided to ban the use of the apps on public officials' work devices out of fear of potential espionage by the Chinese state. These apps were not relevant for productivity anyway but could still be downloaded if the public official chooses to do so.

Even though various nation state actors might have different goals when aligning cyberattacks, some countries will actively try to inflict damage on Dutch companies and/or harm Dutch national interests. For example, the AIVD (2022), mentions that Russia is actively trying to disrupt Dutch political and economic discourse. Russia will encourage and exacerbate certain differences in the Dutch public discourse, hereby trying to sow doubt and even hatred. Polarising certain decisions that affect Russia negatively, is a useful tool for Russia to try and stop the Netherlands and other EU countries from applying further political and economic pressure on Russia. One of the biggest targets for Russia, is trying to undermine the research towards the MH-17 plane. The Dutch Ministry of Justice has concluded that the MH17 plane was shot down by a Russian BUK-rocket (MinJenV 2022). RTL (2018), has received indications that both Russia and Ukraine have been caught spying on several public officials carrying out the investigation towards MH17. As the intended goal is not clear when these espionage acts are being carried out, the nature of this attack points towards a political motivation.

Another phenomenon that is active within Europe is the influence of diaspora communities on a political level. The Netherlands contains several groups with large communities from other countries. These different countries can choose to influence their diaspora for various end-goals. One of them could be to improve relations with their former country, or to influence their diaspora to represent certain interests within other countries like the Netherlands (Gooijer & Veiligheid, 2019). Or even to vote for certain leaders while not living in said country, a more known example here, is Turkey. In the 2023 elections it has been shown that 66% of the people that have voted in the RAI office location voted for Erdogan while living in the Netherlands (*DPG Media*, n.d.). Even though (Yavuz, 2021) states that Erdogan shows a lot of signs of an autocrat, he remains popular with Turkish nationals in European countries. In Dutch, this phenomenon is often referred to as "de lange arm van Turkije" (The long arm of Turkey).

This phenomenon references the fact that Turkey influences their diaspora communities in various EU countries as the AIVD mentions. The NCTV has concluded that unwanted foreign influence was one of the nine biggest threats to the Netherlands (Gooijer & Veiligheid, 2019). Turkey is not the only country however that are actively following and influencing their diaspora, but China and Iran are also notorious offenders. These countries use various techniques to get support from certain groups within the Netherlands, these can include positive actions, like inviting them over at the embassy or with practical help with an administrative action. Often however these countries try to influence these people in a negative and dangerous way, which could include trying to pry information from these diaspora groups.

Another famous example which lead to serious geopolitical consequences is the theft of nuclear secrets by Abdul Qadeer Khan, who stole these secrets from the UNC (UNESCO Centrum Nederland) and brought them to Pakistan. Some argue that this theft of nuclear secrets has led to Pakistan and other nations being able to develop nuclear weapons (N. Singh, 2009).

Authoritarian countries often trace individuals with double passports that might have negative perceptions of the authoritarian country. Iran has often lured people to travel to certain regions close to Iran to capture them and prosecute them further in Iran itself (AIVD, 2023). The AIVD report mentions various threat actors with offensive cyber programs against the Netherlands. There, once again Russia, China and Iran are mentioned. However, when it comes to offensive cyber programs, North Korea also targets the Netherlands. Even though North Korea is a poor country and technologically wise it can be seen as a "Hermit" country (Boo, 2017), this does not prevent them from being an APT against certain countries, like the Netherlands, other European countries, and South Korea.

Dann & Haddow (2007), show that not only do certain state actors steal information from others to use in their own countries, but it can also happen that companies that operate within certain nation states also provide information to these countries. These corporations could be stationed in nation states which some would define as authoritarian regimes which supress human rights. Organisations providing certain information could also eventually lead to the arrest of certain dissidents or political opponents within these authoritarian regimes. This has happened before, when Yahoo! provided information to the CCP which led to the arrest of Li Zhi for posting comments that criticized government officials of corruption. Yahoo's operation in China causes discussion about ethical dilemmas as they must adhere to local CCP legislation, but this does actively lead to supporting an authoritarian regime which seeks to silence its opposition.

4.2 Economical espionage

In the current day and age, economic security is becoming more important. Due to economies becoming increasingly dependent on international trade, international factors of economic interests could be exploited by state actors as a geo-political pressure tool. Organisations are already increasingly focusing on data technology and intellectual property (Grabiszewski & Minor, 2018). Actively protecting these aspects is crucial for organizations. Hannas et al. (2013) show that China is actively looking for Western technology to steal, which they will use for their own economic and military goals without informing the owner of said information/technology. As Western countries still have an edge over Russia and

China technology-wise, Western countries form a prime target for China and Russia to spy on. The Netherlands especially is a leader in forms of technology in which China is extremely interested (AIVD, 2022). In the latest 2022 annual report the AIVD mentions that espionage does not only do damage in the Netherlands, but also to the greater partnership within the EU and NATO. Once again, the AIVD mentions that China and Russia are the biggest threats when it comes to the Dutch national security interests. The Netherlands is not only the target for the knowledge held nationally, but also for the information that might be received in an international partnership/coalition. These countries have a vast interest in secrets regarding the EU and NATO. This could be information regarding technology used in military appliances, but also for economic advantages.

In general, the Dutch government has a clear set of rules and procedures when it comes to IT acquisitions. The Dutch government also releases several reports regarding the current IT trend and cybersecurity risks that are currently relevant. These also include the dangers of state actors and hacktivists (*Tweede Kamer*, 2022). In the questions asked by the members of the House of Representatives they specifically mentioned if the government gave any baseline tools for organisations to use regarding products/partners from countries that practice an offensive cybersecurity strategy against the Netherlands. The government responded with several methodologies and checklists that can be used to determine the threat of certain suppliers. But these checklists and other controls are recommended and not required (*PIANO*, 2019). The government also references the ICO tool they have offered on one of its websites (*BIO-overheid*, n.d.). This tool can help public officials and suppliers get an insight into what type of requirements they must meet and what documents they can use to do so. But these are often standards and baseline requirements of the government themselves or direct suppliers.

4.3 Knowledge security

As the educational/research sector is particularly important for protecting the knowledge and technology within the Netherlands, we have investigated what this sector has done themselves to protect the knowledge security. Knowledge security has garnered more attention over the last few years. Even the Dutch NWO (Nederlandse Organisatie voor Wetenschappelijk Onderzoek) which is an organisation that funds research within the Netherlands has published information about knowledge security and what this means for the Dutch scientific research. They state that "knowledge security focuses on the covert influence of state actors on education and research" (*Knowledge Security | NWO*, 2024). In general, in the Netherlands, working with Chinese universities on advanced technology is considered unethical. Especially considering China's advances of becoming a world leader in the field of Artificial Intelligence. There are also many different perceived threats when working together with China, which can include: Undesired knowledge transfers, intellectual property theft, the covert influencing of individuals, compromising ethical standards or principles of scientific integrity, and the misuse of dual-use technology (Snetselaar, 2022).

In the "Nationale leidraad kennisveiligheid - Veilig internationaal samenwerken", the Dutch science sector has worked together with the Dutch government to create a piece which should help researchers with the knowledge security topic. They also mention that for knowledge security it is crucial to prevent unwanted transfers of sensitive knowledge and technology. They qualify this transfer as unwanted when it concerns the national security of the Netherlands (NWO et al., 2022). Even though this "leidraad" gives the knowledge institutions and universities another tool that they can use to perform a risk assessment about potential research collaborations, the tool does not actually have any mandate whatsoever. Knowledge institutions and universities can still decide to accept research collaborations even though every risk assessment might advise them not to, as there is academic freedom in the Netherlands which gives the knowledge institutions a lot of freedom when it comes to research projects. The same is true for the knowledge security Desk the government has recently introduced for businesses and knowledge institutions (OCW, 2023).

The KNAW has published a piece about the academic freedom in the Netherlands. In this piece they describe the terms and conditions of the academic freedom; they also describe which law and regulation protects it and the actual responsibilities of the researchers. The principles that the KNAW describes are honesty, carefulness, transparency, independence, and responsibility. In the code of conduct these principles have been translated into sixty-one controls for the different research phases (KNAW, 2021). In the code of conduct for researchers the KNAW denotes that the fact of plagiarism with research results will result in sanctions, which can include reprimanding, transfer, degradation, or dismissal of the research project. As (Snetselaar, 2022) describes, working with China can have potential negative consequences, one of which is the compromise of scientific integrity.

Follow the money, which is a platform for investigative journalism, authored an article about different Dutch universities that have worked together with Chinese universities (De Bruijn et al., 2023). Not only do they describe that that there are many Dutch universities that have research topics that are interesting for the Chinese military, but also that often Dutch institutions are providing the funding or even NATO (5.56) ammunition for testing. According to the Australian tracker called Unitracker, many of these universities can be considered "high risk" universities (Australian Strategic Policy Institute, 2024). So not only is there the risk of working with counterfeit research data provided by Chinese universities, but the research is also funded for by Dutch institutions and might later potentially serve Chinese military goals. The Dutch HCSS (The Hague Centre for Strategic Studies) describes that working with Chinese universities is possible when it concerns economic, political, and sociological goals, but high-end technology is a different environment altogether (Willemsen, 2023). So, working together with universities in China is still a possibility, but there must be some form of risk analysis done before these collaborations are started.

It is equally crucial to give organisations within important sectors that carry significant Intellectual Property, the right tools to protect their technology from espionage/cyber threats. In the yearly report of the MIVD (2023), the MIVD recognizes the dangers of (attempted) Chinese industrial and military espionage within several different Dutch sectors. Namely the Chinese are trying to pry information from different Dutch sectors, such as: the semiconductor, quantum technology, aerospace technology and maritime industry sectors. The MIVD has claimed to have intercepted and prevented several Chinese espionages attempts within these industries. But it is not only China that has an offensive (cyber) espionage strategy towards the Netherlands. The MIVD mentions that countries like Russia and Iran have also shown to have an interest in the Dutch technological sector or in the military technology the Netherlands possesses (MIVD, 2023).

4.4 State actors according to the government

To give insight into the way other nation states are attacking the Netherlands, the NCTV together with the Dutch intelligence agencies release a report every year. This report in 2022 (AIVD, 2022) focuses on the national security interest that could be damaged by state actors and in which ways this is already happening. The report covers four pillars which they deem to be the biggest threats to the Dutch national security:

1. Geopolitical changes like the war in Ukraine also translate into a bigger threat for the Netherlands and its partners.
2. The Netherlands and it European partners remain a target for state actors to try and influence individuals within European borders. This puts pressure on the society of the Netherlands, and state actors also influence diaspora communities within the Netherlands and others that might be opposed to the authoritarian regimes in their home countries.
3. Economic threats are becoming increasingly apparent in the Netherlands. Vital processes are still in danger because of takeovers and sabotage from the outside. There has also been an increase in the number of strategic dependencies within the Netherlands, for example Russian gas for Dutch power needs. Businesses and knowledge institutions are also being targeted for their research or possession of advanced technology. Currently China is being marked as the biggest threat to the Dutch knowledge security.
4. The last threat has to do with the international legal order that currently exists, this is described by some state actors as a “Western construct”. But they are also undermining international norms such as non-intervention, non-proliferation and peaceful dispute settlements are being violated.

All four of the pillars above could be simultaneously attacked by state actors even though they might have different goals in mind (AIVD, 2022).

5 Interview process and data analysis

In this chapter, the conducted interviews, and data analysis process. In this study, twelve interviews have been conducted, which capture the subjective views of participants and any real-life experiences they might have. Different opinions and focuses were easily discussed within the interviews and the participants had the freedom to tell their story the way they wanted to. The interviews have taken place over the span of several months. Below you will be able to find a table with all the corresponding dates of the conducted interviews:

Interview	Interview date	Interview duration (H/M/S)
1	04/10/2023	00:32:07
2	13/10/2023	00:46:31
3	21/10/2023	00:27:21
4	12/12/2023	00:31:41
5	20/12/2023	00:34:23
6	21/12/2023	00:31:50
7	22/12/2023	00:34:46
8	17/01/2024	00:33:00
9	18/01/2024	00:44:50
10	24/01/2024	00:46:58
11	07/02/2024	00:24:30
12	08/03/2024	00:25:57
Average interview duration		
00:34:30		

Table 1: Dates and duration of all interviews.

The interviews followed a semi-structured approach, which means we originally used a standardised question list, which had been customised for the participant beforehand. We started off by talking about the informed consent document and whether the participant understood their rights in regard to the interview and the collected results. Afterwards, we would inform the participant the recording was going to start. From this point the interview could officially start, while going through the structured questions, we asked follow-up questions when we felt it would deliver important information for the thesis topics. Again, this was part of the reflexive approach we wanted to implement in this interview process. At the end of the interview, we discussed and summarized the interview, afterwards the participants were free to ask questions. In the end we asked the participants whether they would like to be informed when the thesis would be publicly available.

In these interviews, we have interviewed people from different organisations and within the public sector, but also slightly adjacent to it. This means many different people were interviewed with different opinions, views on difficult topics and various expertises. Between the interviews, there was plenty of time for evaluation before the next interview would take place. This also allowed us to search for participants that held information which might not have been collected yet. As one of the main difficulties of this thesis was collecting the right participants for the interviews, a lot of time has been spent on searching for and contacting potential participants. This also means that after an interview had been conducted, proper evaluation was done to see whether the right results had been collected. This evaluation also led to slight changes in the structure of the interview and even the removal/adjustments of certain questions.

A general question list has been developed to answer the research questions. As we have interviewed many professionals within the field who might have slightly different roles and responsibilities it was important to slightly adjust the general question list, so it matched the expertise of the participant. This did increase the time it took to prepare the questions and properly research the relevant policies beforehand, but as the interviews have been quite spread out, this was deemed possible.

Demographics

Most of the interview participants have followed a higher education, two people have a PhD, six people hold a master's degree and two people hold a bachelor's degree, for 2 candidates it is unknown as it was not disclosed. They collectively share at least 188 years of working experience among them. Out of the 12 participants, eleven are male and one is female. Many of the participants of the interviewers were people that have hands on experience with the policy pieces that have been created in the last few years. Several participants were active in the operational departments of the organisations they were working for. This meant several policy officers, but also experts within the fields of cyber threat intelligence (CTI), SOC (security operations centre) operations, security governance and security advisories have been interviewed. As participants have asked for their organisation names to remain private, we only disclose that we have interviewed specific individuals from hand-picked ministries that were deemed important for this thesis.

Coding process

As an initial part of the process, the interviews have been transcribed. As the interviews have been performed in Dutch, we had to make sure the translation into English matched the same intention and tone the participants had left in Dutch. This already posed several challenges as the Dutch language has several particularities when describing certain phenomena. The tone also had to match the way the participants originally intended when answering all the questions in Dutch, especially when certain politically sensitive subjects were discussed. Only by retaining the original intent and answers, could the codes be applied in the right way. As the codes had been applied globally and were applied with the goal of finding commonalities and themes among the transcripts, it was important the codes were applied for short sentences and not whole paragraphs. As answers were sometimes long and drawn out, this became even more important. During the multiple coding iterations, more themes emerged which have been used for the research results.

An open coding method is used to apply codes to the transcriptions. We used open coding to check if the initial codes found in the first round of coding matched the themes that emerged out of the literature review and document analysis. Cascio et al. (2019), describe an iterative-inductive way of open coding which has been beneficial for this thesis. By starting with open coding, and allowing for external coders to check the intercoder agreement, axial coding could also be used later on to identify axial themes. As several themes had been identified early on, the coding process followed several iterations to achieve a certain coding quality. Hruschka et al. (2004), describe that intercoder reliability improves substantially when you follow a systematic process to revise and test the codebook, which we have done by allowing two external controllers to test the codebook. More about the intercoder agreement can be found in the coding reliability sub header. After the first controller had tested the codebook and the codebook had been slightly revised afterwards, we started by axially coding the existing codes by adding semantic domains to them. These semantic domains gave the already existing codes broader categories, which made identifying the axial themes slightly easier. These semantic domains have also been important in calculating the intercoder agreement level.

To control the codebase, two separate coders, outside the research group, were introduced to control the codebase to check for interrater reliability. The two coders first familiarized themselves the codebook. The codes and codebase were explained to them by us before they started with their coding session, and this helped them understand not only the concepts but also when and when not to apply certain codes. The coders then each coded a different transcription, to see whether the original codes would be applied or if they would create many new codes. If the current codebase could not be used or the coders felt like a lot of codes were missing, this would have given the researcher the input that was needed to improve the codebase. In our case, the coders could comfortably code the transcription after an initial introduction was given. Even though the first controller had a slightly harder time applying the codes than the second, in general, the codes applied by the controllers were relatively consistent with the codebase of the original researcher. After the first controller finished coding a transcription, some slight revisions had been made to make it easier for future controllers. Because of the use of two controllers and the use of the intercoder agreement tool, which supplied a good score, the researcher has good confidence in the strength of the codebase. As we finished several iterations of the coding process, clear commonalities and themes had emerged. These themes have been described in the results chapter.

Coding reliability

To make sure the coding is of sufficient quality, we used the Inter Coder Agreement (ICA) tool, this tool allows the use of the Krippendorf's alpha formula built into the ICA tool of AtlasTI. As the controllers were external coders, which were allowed to place their own quotations and tried to use the existing code base, we have chosen to use the Krippendorff's c-Alpha-binary instead of the Krippendorff's Cu-Alpha/cu-Alpha formula.

For the user "coder 2", the Krippendorff's c-Alpha-binary is the following: 0.631.

For the user "coder 3", the Krippendorff's c-Alpha-binary is the following: 0.722.

The average c-Alpha-binary = 0.677.

After the initial control of coder 2, some slight revisions have been made to the code base, which better encapsulated the categories, and made the coding process easier for the second controller. The second controller, named "coder 3", also scored a higher Krippendorff's c-Alpha-binary and mentioned the categories were easily applicable to the transcription. As the c-Alpha-binary also used the length of the quotations to calculate the score, it is important to denote that on a subjective level, coders will interpret the length of a quotation differently, so this will impact the score drastically if the difference in equation length is substantial. All assessments which only had one rater have been removed as Zapf et al. (2016), mention they must be removed from the Krippendorff's c-Alpha-binary calculation.

5.1 Results

In this section, all the themes that have been discovered will be discussed. These themes have been explained, where possible and allowed by the participants, by linking several random quotes from certain interview transcripts with the codes that have been identified during the coding process. Note that we only specify the anonymised code of the transcription (from which specific interview they have emerged) to preserve the anonymity of the interviewees. Some information in this results section is collected from other section of the thesis, namely the document analysis and literature review.

5.1.1 Codebook

In Annex D, you can find the different codes which have been applied to the transcripts. The initial open coding rounds were developed into the first themes, then the codes were categorised by semantic domains that have re-occurred in all the interviews. Even though some participants might have approached a certain theme slightly differently, they still described similarities.

5.1.2 Emerged themes

As we are using thematic analysis to analyse the data which has been collected, creating themes based on the codes, literature review and document analysis provides us with information about the current status of espionage monitoring. These themes also allow us to quantify the research results. Out of the initial round of open coding, some themes already emerged as several codes have been used together often. semantic domains have been added to the codes after the initial rounds of open coding, the semantic domains give the codes categories which further describe certain themes. As an example, participants mentioned several times that there has been a lack of awareness, but some participants also mentioned that the awareness has been improving the last few years. By adding a behaviour tag, we further categorise a trend that impact the human factor of security by talking about the government officials/politicians. The themes shall be separately described below with mentions towards the codes/quotes of several transcriptions. These themes have also allowed us to answer the research questions as the themes that have been identified match the information that was needed for answering these questions. Even though a lot of topics have been discussed in the interviews, some participants have chosen not to include their quotations in this thesis, which means they will not be found here, but rather processed in an indirect way.

5.2.1 Challenges

A common emerging theme that has emerged during every interview are challenges that are experienced by participants when mentioning certain topics. Whether discussing espionage, knowledge or economic security, the challenges the participants were facing when dealing with these topics were quite clear. As every interview could have different viewpoint and topics that have been specifically discussed, we have linked every potential challenge they were facing with generic codes that could describe a potential challenge. We have divided the challenges in two categories:

- **Challenges that have often been described that are within the participants influence are:**
    - Difficulties to attribute an attack as cyber espionage.
    - Lack of awareness at organisations, businesses, and people.

- **Challenges that have often been described that include external forces are:**
    - Political importance
    - Educational freedom allows for less control by the government.
    - Geopolitical changes cause a very dynamic environment.

To further expand on these themes, they are discussed below.

5.2.1.1 Difficulties to attribute an attack as cyber espionage

One of the most mentioned themes, is the difficulty of measuring an intent when monitoring certain cyber attacks. As a lot of attacks are performed digitally these days, making sure these attacks do not do any damage is a core focus. But you do not know beforehand what the original intent between an attack was, this way you do keep the network safe, but you do not know what they were trying to achieve. So, when asking how the government monitors espionage, knowledge- and economic security, many participants mentioned it is difficult to fully get a grasp of the quantity of attacks with these different topics in mind. For all you know they could all be script kiddies performing cybersecurity attacks. This is one example of a participant mentioning this phenomenon:

> "When someone is trying to port scan your organisation, you will only be able to tell what their intent is once they are inside the network. We could not speculate about the intention beforehand. People from the outside often think that this is something that we can actively tell".
>
> (ID3)

As this thesis is focused on researching the way the government monitors espionage, economic and knowledge security, it is important to consider the fact that, many of the attacks that will be experienced by organisations will (hopefully) be blocked by proper detection rules. For any blocked attacks, it will be exceedingly difficult to know the original intention behind it. Several codes have been created which describe a certain situation in which new cyberattack will be judged based on its characteristics, this means they might have been blocked by detection rules, or initial threat intel.

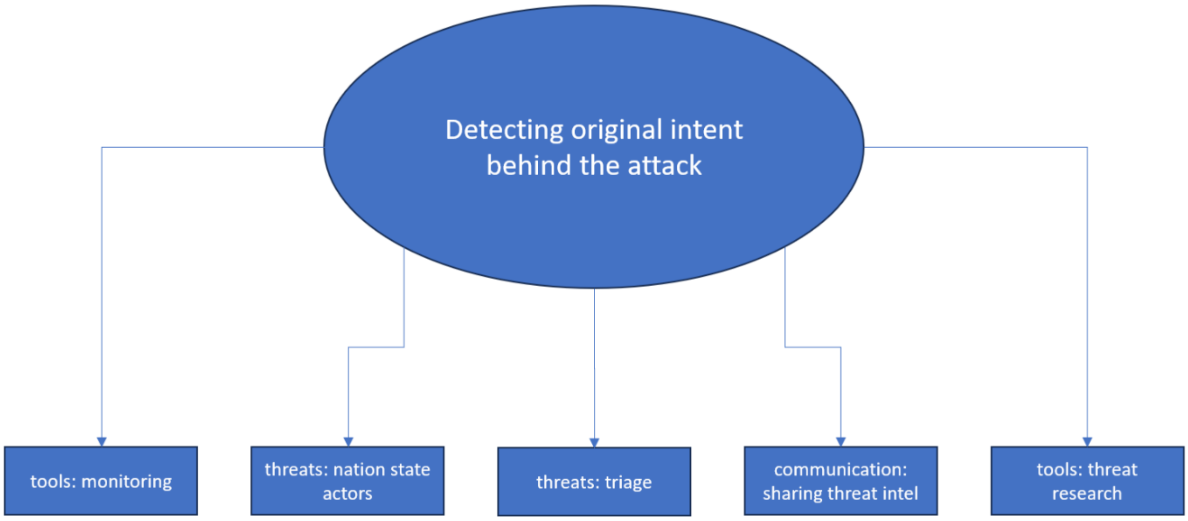

Detecting original intent behind the attack
tools: monitoring
threats: nation state actors
threats: triage
communication: sharing threat intel
tools: threat research

Figure 6:Codes linked to detecting the original attack intent.

The codes mentioned in figure 6 have been used several times to describe the challenge of finding the initial attacker and their intent. It is extremely difficult to get a full grasp of all espionage attempts that might be thrown towards certain organisations, as they do not make their intention clear from the start, which makes monitoring in pure numbers exceedingly difficult.

What does not help this already existing scenario, is that governmental environments are digitalising at a rapid pace. This means the attack surface for different environments has grown significantly. As mentioned before, a lot of attacks are performed online, which makes creating cyber resilience environments especially important. As this topic came up in different interviews, the code "digitalisation" also has been applied. As digitalisation could be brought up as a reason to explain a bigger attack surface, but also political objective, it has not been categorised further. A participant mentioned the following about the digitalisation at the government:

> *There is a society which is digitalising rapidly which will increase the attack surface significantly. The digitalisation increase the attack surface but also the dependency on digital processes, which both have to do with digital safety and therefore cyber security. If you look at all the ministries, you can see that digitalisation is within the strategic ambition noted as a precondition.*
>
> *(ID2)*

5.2.1.2 Lack of awareness at organisations, businesses, and people

Another widespread problem was the lack of awareness for the several different topics discussed in this thesis. Historically, the Netherlands has had the tendency to focus on monetary gains, which put doing business at the forefront. This could also mean that potential partnerships and collaborations were started while these might have also induced dangers of which the public was not yet aware of. There might also be a conflict of interest when comparing the job of the Dutch government against the commercial interests of Dutch businesses. The Dutch government does value these organisations highly as they are important for the Dutch economy and economical security, but the balance in the scales might have been missing in the prior years. By increasing the awareness in commercial businesses, they might learn more about the potential dangers of doing business with certain state actors, instead of only focusing on the potential monetary gains. A participant said the following about the importance of awareness:

> *That is something awareness suffers from, nobody has time and everyone finds it annoying. But it is a important factor, and what I often hear from institutes is that they should they should do more about awareness, but in the meantime it kind of stays behind.*
>
> *(ID5)*

Another participant mentioned the following about certain awareness challenges:

> *What we often hear is ownership. That has to do with awareness as well. There is often the thought that the CISO is for security and the FG is responsible for privacy. But if you look at Business Continuity plans, it is very important for a department director to be aware of the various processes that need to be up and running.*
>
> *(ID4)*

When discussing these topics, the participants often discussed patterns which were connected to the following codes: “behaviour: lack of awareness”, “threats: economic security”, “threats: espionage” and “threats: knowledge security”. When these topics were being discussed, several participants did mention that in the last few years there has been a great uplift of attention and awareness for these topics. Often the geopolitical changes like the war in Ukraine caused more people to see the dangers of untrustworthy suppliers and business partners. For this phenomenon, the code “threats: nation state actor” together with “threats: espionage”, “threats: knowledge security” or ”threats: economic security” were often applied. These consequences could be the realisation about certain political decisions, but it could also be used when geopolitical changes lead to different behaviour by state actors. These geopolitical changes will be further discussed in 5.2.1.5.

From the interviews that were dedicated to the educational sector, this lack of awareness was also often discussed. The educational sector is a little bit different though, as participants often mentioned that internationalisation is part of the modern-day science, and that the Netherlands is also often dependent on other countries to be able to research certain subjects. But in the interviews, it was often mentioned that the awareness for knowledge security was increasing, this also included the research institutes. Knowledge security has become a far more important topic that is actively on the radar of many organisations. A participant mentioned the following about the state of security within universities:

> *If we look back, we have done quite a lot in the last couple of years. If I look forward, I think we are almost standing still. If I look sidewards towards other EU countries, we are generally going quite fast. It depends at who you are looking, but in my opinion, we should be moving way faster.*
>
> *(ID9)*

In general, most of the participants thought that the Netherlands has a lot of success with securing their knowledge security, at least in the way it is properly secured in theory, which is the legislation/policy part. But in practice, not all the tools and information that the research institutions are receiving, are also being used. Even when an educational organisation uses the knowledge security Desk for information on a certain topic, they are not actually required to follow the advice that they might receive. Only when the government detects threats at a university that might actively harm the Dutch national security, is when they have the mandate to act.

5.2.1.3 Political importance

As the Netherlands is a parliamentary democracy, the House of Representatives decides what the ministries will be doing over the course of a certain parliament. This also means that financial decision and focus points are often not decided by the ministries themselves, but rather the parliaments that have been formed. This causes a certain dependency for the ministries on the current political wind that exists within the Netherlands. It will impact the amount of funding they will receive for certain projects, but also if they can keep working on already existing legislation/policies. This can create difficulties as they sometimes need to go back to the political side of things to ask for more funds or cut their own budget somewhere else. But a participant also mentioned that there has been a growing awareness at the political level of ministries as well when asked about the awareness of espionage, knowledge- and economic security trends and needed actions:

> *There is also a ongoing culture change at the c-level* of the organisation. At a ministerial level there is more attention and also at the SG/DG* level of the organisation. You don't have to explain why you would undertake certain actions in this field. So*

you can see there have been definite improvements in this area.
**c-level = "chief" executives*
SG/DG = secretary-general/director-general
(ID2)

Convincing the political side of the Netherlands of the importance of integral security remains a critical task within the Dutch government. This theme is often combined with other themes and can be a catalyst for more challenges that the government experiences. As the educational freedom exists as this is decided by legislation, which in turn comes from the House of Representatives. Even though Dutch institutions value this academic freedom very highly, the question remains whether the research institutes should have this level of autonomy.

The political aspects also impact the economic side of the legislation that businesses may experience, as there is also a Desk for middle to small businesses (SMEs) and larger corporations. Businesses also can ask questions to the Desk, but businesses also have a lot of freedom when deciding who they do business with. The House of Representatives must lay out clear legislation that also reflects their current stance in the geopolitical conflicts. Businesses are often forbidden to do business with Russia, but this is not the case for all state actors. You could also argue if this is something the Dutch government should do, this can be done by creating a distinction between normal products and elevated risk (technology) for all nation states.

5.2.1.4 Educational freedom allows for less control by the government

As mentioned, in the Netherlands, universities, research institutions and applied science universities have a certain level of educational/scientific freedom which allows them to operate with a certain level of independence. This independence does make it more difficult for ministries to steer and control policies within the institutions themselves. This academic independence is valued by the ministries themselves as it is an important reason for the scientific advancement in the Netherlands in general. A participant mentioned the following:

> *It is a difficult point as we say multiple things, because academic freedom is very important to us, so as the government we have a job to protect this as well. So this is one side. On the other side, academic freedom is not infinite, just like all freedoms have their limits.*
> *(ID12)*

In general, the academic freedom allows the institutions to operate independently and without too much intervention from the government. This might create difficulties in governance cases as universities might have other (business-related) incentives than the government might have. Another interesting quote from a participant is about comparing the way educational freedom functions in the Netherlands and Denmark:

> *In Denmark every day, an inspector from the university can walk in to see if the cybersecurity is up to speed, this is mandatory by law. Over there the universities can not say we have academic independence and freedom to try and block the inspector. In the Netherlands you have the law Higher education and science that gives universities a form of immunity and they can self regulate a lot. So the government has to do a lot to try and get the universities to keep going in the right direction.*
>
> *(ID9)*

This comparison is quite an interesting way to describe the way the Dutch educational/academic freedom works in comparison to another country like Denmark which is also in the European Union; their educational ministry has far more options to directly control the way these educational institutions operate. Whether this is something that the Dutch government would also like to implement, would be again up to the political side of the government and the greater electorate.

When mentioning academic freedom and the difficulties this creates, the following participant mentioned the political importance of this freedom:

> *Yes and this is again a sensitive point, good that you bring this up. Well I expect there to be more discussion about this politically. But we are having conversations with universities and also with researchers within universities, but also with the board of universities.*
>
> *ID(12)*

5.2.1.5 Geopolitical changes cause a very dynamic environment

While creating the codes, it already became clear that state actors impacting the geopolitical situation of the world often directly translated to a change in behaviour towards the Netherlands and other countries. The following participant mentioned the war in Ukraine and the effect it had on the Netherlands:

> *An example is the crisis happening in Ukraine and now in Israel, these geopolitical activities can change the economic and knowledge security environments in the Netherlands.*
>
> *(ID11)*

Another interesting quote in the same area was the following one:

> *Of course geopolitical changes also have an affect on state actors, they will behave differently, I am telling you nothing new*

when I mention that the attack on Ukraine caused a shift in the cyber tactic of the Russians.

(ID11)

Threat actors can be various in nature and can have different goals. As was mentioned before this chapter, it is difficult to fully grasp a threat actors' intention when they initially launch an attack. You can mostly only do so when they are already inside the systems you are trying to protect. The same can be said about the attacks that state actors set out, you first must find out that these threat actors are after, and you also must discover which state actor is targeting you. Annually, the AIVD and MIVD release reports in which they describe the current state actors that form the biggest threats to the Dutch national security. A participant stated the following when describing state actors:

Well, the biggest cyberthreat is most certainly the threat generated by state actors, let there be no doubt about that. This is also described in the national cyber security report.

(ID11)

There is a clear threat that the state actors pose for the national security of the Netherlands. This threat could then be further divided into threats for the economy, knowledge position or potential espionage related dangers. Different APT's might also target the Netherlands for several reasons. These APT's could be state actors but also other hacking groups, like a participant mentioned:

Criminals can be just as much an APT as state actors. The only difference is the scale at which they operate. You have some smaller criminals which perform WhatsApp fraud. But you also have large criminal organisations that can cripple hospitals and municipalities.

(ID11)

So, the different threat actors that exist can all form threats to Dutch security interests. This is important to know when measuring the number of attacks that might overlap with espionage or economic- and knowledge security related topics.

5.2.2 Successes

Just like there have been challenges regarding espionage, knowledge-and economic security, there have also been notable successes which should be mentioned. The mentioned successes have been formed based on information gained from the literature review, document analysis, but mostly by the interviews. These successes are often linked to each other, which is why the two following themes have reoccurred several times:

- New development of tools, policies, and legislation
- Governance within the government; defined roles, and responsibilities

5.2.2.1 New development of tools, policies, and legislation

The Desks

In the last couple of years, the government has been rapidly expanding their arsenal to combat potential threats that would damage Dutch interests. For the three topics: espionage, knowledge- and economic security, the government has been creating policies that focuses on at least one of the three topics. These topics often intertwine in the way they work however, which means an integral approach is often desired. An example of the way the government is currently trying to improve the knowledge security in the education sector is by providing them a knowledge security 'Desk', this Desk is quite unique in the way it functions, one of the participants even mentioned the following:

> *One of the concrete examples is the national Desk knowledge security. This is a Desk that has been designed by the government. And there will be a interdisciplinary view on your advice request and if you have no knowledge in your institute and you are not sure if what you are doing is a risk you can visit the Desk.*
>
> *(ID9)*

The same participant also mentioned that the Netherlands is quite unique in the way it has this Desk enabled for their educational sector:

> *No other country has something similar. I have mediated and given presentations for a group of 25 Western-European universities, and also for some Canadian universities. There is no other country which has such a multidisciplinary advice offering from the government.*
>
> *(ID9)*

This is also partially because of the educational freedom that the Netherlands has. The government cannot apply direct control towards the educational and research institutions which requires them to implement other ways of helping institutions with difficult topics. Like described in the literature review, research institutions have codes of conduct and ethical rules which they require for research, but they still decide themselves what the research topic will be and if they will cancel the research after a risk assessment. You could wonder if this is something that the institution should do themselves or if this is a task for the government, a participant mentioned the following:

> *What the government would like to see is that universities themselves, and not even the government, make the consideration to see what is and what is not responsible. For research you also have ethics and integrity rules, so there is a behavioural code, so researchers have a lot of freedom to perform research whatever they want and I don't think the government would like to police this very much.*
>
> *(ID12)*

The Dutch government also has the economic Desk made specifically for SMEs (Small and medium-sized enterprises) and of course larger corporations as well. This Desk will offer information on economic risks when partnering with foreign investors/state owned businesses. Some of the organisations that are also involved with the knowledge security Desk are also involved with the economic security one. In general, the responsibility for these Desks is given to the corresponding ministry. This would be the Ministry of Economic Affairs and Climate for the economic security Desk and the Ministry of Education, Culture and Science for the knowledge security Desk.

Legislation

Legislation is another powerful tool for the government to protect national interest. A new legislation that has been quite prevalent in a few interviews is called the law Vifo (Wet veiligheidstoets investeringen, fusies en overnames), this legislation came into effect on the 1st of June 2023. This legislation allows for a security check on investments, fusions, and takeovers, and it will be applicable for two types of companies in the Netherlands: vital (critical) providers and companies that possess sensitive technology. When asked how the government plans to secure important technology, a participant mentioned the following:

> *For that we have created some legislation which is the law Vifo (Wet veiligheidstoets investeringen, fusies en overnames). When certain acquisitions happen within important sector or technological companies or even the vital sector. But also with any harbours etc. If we see that a certain state is trying to acquire these companies, companies which would not be smart for the Netherlands to lose, than the government can step in and buy the shares themselves.*
>
> *ID(8)*

For this legislation, a new group has been established called the: "Bureau Toetsing Investeringen (BTI)". This bureau will perform the assessment for potential take-overs, fusions, and investments that the state deems a potential risk to the economy or national security. Investors in vital sectors and businesses that hold sensitive technology will have to report any changes in the ownership structure to the BTI. Then the BTI will decide whether there are risks to this change and might add additional conditions or block the change altogether.

The newest addition to the instrumentation for economic security is the Beschermingsvoorziening Economische Veiligheid. This legislation allows the government to create a fund that will allow them to buy (temporary) stakes of a certain company that might be beneficial for Dutch interest, whether they focus on national security or economic security. Most of these legislations are quite new and recently implemented, with the goal of improving the economic resilience of the Netherlands. Whether they will have the impact the government wants them to have, will have to be evaluated later.

For espionage, there has also been a new legislation which allows the government to prosecute potential criminals faster. This new legislation will criminalize more forms of espionage, which could be new or more modernised versions of classical espionage forms. The government specifically mentions things like foreign governments and diaspora espionage. This addition to the existing legislation is called "Uitbreiding strafbaarheid spionageactiviteiten (Expansion of criminal liability for espionage activities)", which will add to the existing "Wetboek van Strafrecht en het Wetboek van Strafvordering (Criminal Code and the Code of Criminal Procedure)". A participant specifically mentioned the expansion of criminal liability for espionage activities when asked about important upcoming legislation:

> *Yes I think there is. It is called the modernising of the criminalization of espionage. This has been introduced last year. There has been a proposal to expand the criminalization. This is now online.*
>
> *(ID8)*

These legislations along with some of the other economic security/knowledge security solutions often received codes such as "tools: economic security", knowledge security increase", "tools: knowledge security", "behaviour: increasing awareness", "tools: monitoring", "tools: law and legislation" and of course "tools: policy creation".

Another tool for the government is the new legislation called "Wet Screening Kennisveiligheid (Knowledge Safety Screening Act)", which allows for the screening of foreign researchers and students, a participant mentioned the following about this legislation:

> *There will also be a screening for foreign students and researchers. Which is also part of espionage, as this has to do with potentially unwanted foreign interference.*
>
> *(ID8)*

Another participant mentioned the following about the importance of this screening:

> *Finally, I have been saying we need this for years. Espionage is of all days and age, even if it is about a research result of whatever.* *(ID10)*

Figure 7 below shows a visualisation of how the codes have been categorised for the different topics that the participants have discussed. As the participants mentioned, both the new tools and the (updated) legislation should have a positive effect on espionage, knowledge- and economic safety. As the legislation and tools are two separate entities however, they are categorised slightly different.

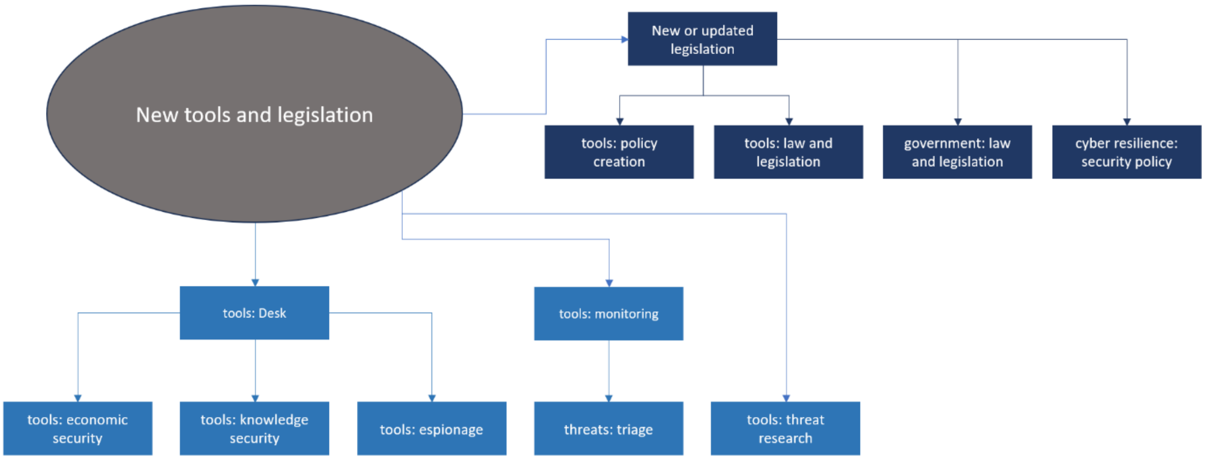

New tools and legislation
New or updated legislation
tools: policy creation
tools: law and legislation
government: law and legislation
cyber resilience: security policy
tools: Desk
tools: monitoring
tools: economic security
tools: knowledge security
tools: espionage
threats: triage
tools: threat research

Figure 7:Tools and legislation released by the government.

5.2.2.2 Governmental governance, defined roles, and responsibilities

One thing that came up often is the way the government is currently structured and how responsibilities are quite clear for many organisations within the government. Many of the participants quickly corrected us when a responsibility was connected to the wrong ministry. But not only the responsibilities are ordered within the ministries, the whole governance structure facilitates an easier way of working as it is clear who is doing what, and why. The ministries themselves will carry the responsibility of getting their cyber security in order, but they can ask for help at the NCSC and the AIVD in case of a severe threat. For espionage-related activities, separate ministries can contact the NCTV for advice and the AIVD for assistance. The NCTV will be the one that will be taking the lead for policy pieces concerning espionage, while the AIVD is very operationally focused on the threats that could damage the Netherlands, which will also include espionage. A participant mentioned the following about the roles and responsibilities especially in regards to researching nation state actors:

Within the national government roles are clearly defined, so you have security agencies which will investigate bigger and more dangerous actors.
(ID2)

The Ministry of Economic affairs and Climate is responsible for the policies created that concern economic security and this responsibility has been developing over the last few years. As economic security can also impact the national security, the NCTV and AIVD can be involved when necessary. Knowledge security-related policies will be developed by the ministry of Education, Culture and Science as this is the ministry that is responsible for the educational sector, which includes the scientific research institutions. As stated earlier, this ministry has more difficulties in getting the institutions in line with the policy because of the academic freedom.

Within certain interviews, various participants could quickly identify the most important organisations for cyber, espionage, economic security, and knowledge security.

To visualise these responsibilities, relevant organisations are plotted in a Venn diagram below. This plot is based on information gathered in the interviews, document analysis and literature review. Only the NCSC is missing as they are mostly responsible for the (cyber) operational monitoring, technical solutions, and expertise.

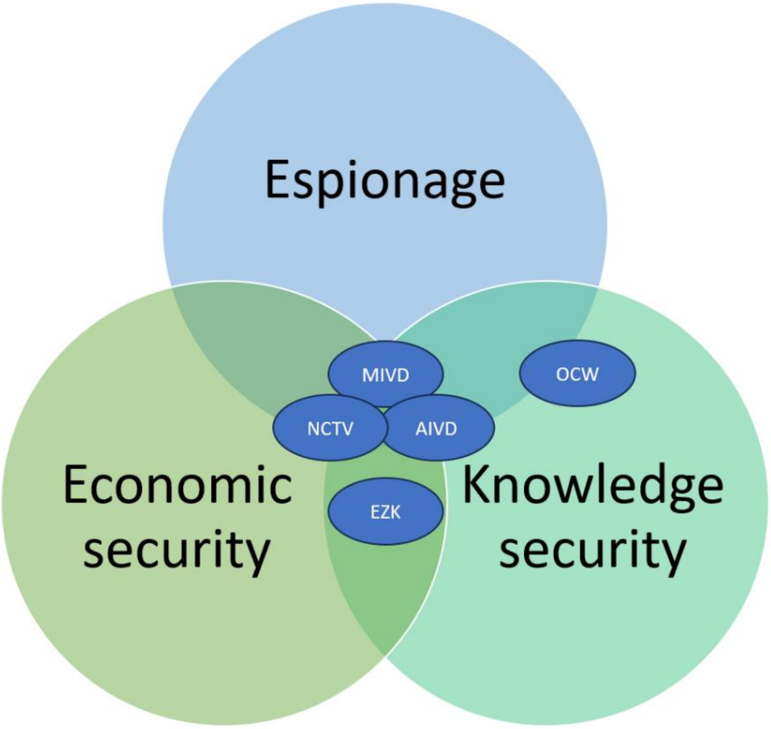


Figure 8: Governmental responsibility.

Even though there are many different ministries with various portfolio’s, they are primarily always responsible for the compliance within their own ministry. They can ask for assistance with security-related activities from the NCSC, but in the end they themselves make the decision if they will implement said advice. Within the government, there are also specific roles that are filled for compliance/legislation purposes. One example of these governmentally wide programs that focusses on the resilience of the whole organisations is the BVA-system (Security authority system). This legislation focusses on implementing a system of integral security, where clear roles and functions must be filed within key departments of ministries.

This legislation also lays out certain responsibilities for the ministers, as they must adhere to the tasks that have been defined in this BVA-system. One of the examples that ministries and other governmental agencies are now required to implement are: a policy for integral security; roles like the CISO and CIO having a certain level of mandate; having regular audits that control the integral security; and organising the physical security of ministers within policy pieces. About the BVA, a participant mentioned the following:

> *In the BVA (Beveiligingsautoriteit) stelsel which is publicised in the staatcourant, four domains are mentioned: Physical security, personal security, security of people and information security. If you look at those four domains of threat, on which you apply risk management.*
> *(ID2)*

As the distinct roles and responsibilities between the governmental organisations were an often-discussed topic within the interviews, several codes have been created to group these distinctions. Codes like “organisation: role”, organisation: department” and “government: defined responsibility” have often been used to describe the different governance structures within the government. As the responsibilities for these assorted topics is often concentrated within specific ministries, that does also often mean that the expertise for these topics is also concentrated there. This does however cause ministries to be dependent on expertise outside their own ministry for policy creation or incident management.

For (political) responsibility regarding knowledge security, participant ID12 mentioned the following about the Ministry of Education, Culture and Science:

> *So there is a minister that also creates plans for knowledge security and they will also have to inform the House of Representatives about it and they will receive questions about these plans, so in the end, the minister will still have to claim responsibility.*
> *(ID12)*

There are also differences in the organisation-types within the government: you have operationally focused organisations and organisations that focus on the creation of policies. One example of this construction is the NCTV as policy creating organisation and the NCSC as an operational organisation. In this case the NCTV is also the contractor of the NCSC. So, in some case they also decide what type of actions the NCSC will perform and what type of budget they will receive for it. Another example would be the ministry of Infrastructure and its operationally related organisation RWS (Rijkswaterstaat). For these organisations, the overall policy and rules get created at the policy generating ministry, which means the operational departments are also dependant on the rules and policies of these organisations. If these policy organisations choose not to implement certain security standards, this will often mean that the operational organisations will also not implement them, unless specifically required. This is also important when mentioning the budgeting of these organisations. The overall ministries get a budget from the political side, this budget will then have to be redistributed between all the different tasks of the ministry, but this will also include the budget for operationally focused organisations like RWS or the NCSC. We have also noticed a lot of participants describe the NCSC to be an important partner for cyber security related ventures. The participants had to say the following about the NCSC:

> *You have a NCSC that gives a image at a holistic level for any digital related cases. The NCSC also has a cooperation team in which they work together with the security agencies and the national police, in which they share information.*
> *(ID2)*

When asking a participant about their communication channels they said the following:

> *Yes definitely, we have a direct line with NCSC and that is our central line which most of our communication goes to.*
> *(ID3)*

The same participant mentioned this is because of the following reason:

> *Yes but this is because the NCSC functions as a spider in the web for certain threats. They also have the coordinator for terrorism which gives a lot of input for relevant organisations, so we also actively listen to the information.*
> *(ID3)*

However because of the new NIS2, the NCSC has been given a lot more responsibilities in general and their list of focus organisations has grown, a participant mentioned the following about this development:

> *With the NIS2, Europe has appointed a lot of different organisations as critical. The NCSC used to have 300-400 organisations that they had close ties to before the NIS2, but it will now grow to 10.000 organisations. So as an organisation they will also have to grow to make sure they can actually scale. (ID11)*

An often-discussed topic is also the involvement of the minister of the ministries that were discussed during the interviews. It was often made clear that the responsibility for several topics was spread over several ministries and therefore delegated to several minsters. Certain portfolios and responsibilities were "owned" by specific ministries, this is however also a recent development, at least for the topic's knowledge- and economic security. The participants mentioned that certain ministries have been taking far more ownership over these topics. This once again confirms the importance of proper political will and support for these organisations.

The better relationship between the Dutch government and the Dutch business community has also been improving as Dutch governmental agencies are free to seek advice outside the government and are also able to hire private companies for contractual work. As the Dutch government does not have the capacity to help all organisations at the same time, the Dutch private sector can play an important part in making sure the Netherlands will become safer. During the interviews, participants mentioned that the private sector has become more actively involved in certain areas of cyber security, like for example threat intelligence that focuses on nation state actors. A participant mentioned the following about the government's relationship with the private sector regarding digitalisation:

> *The government works together with private IT partners for the digitalisation. It is also difficult to secure everything yourself. (ID2)*

6 Discussion

In this chapter, we discuss the answers to the research questions using the knowledge of the document analysis, literature review and the results of the interviews. All these different information points will be used to answer the different research questions. The documents that have been referenced in the document analysis have also been mentioned by the participants within the interviews. In the interviews, we have been able to ask questions about these documents and corresponding policies. This caused us to have plenty of information about the why the policy has been created in the first place and has been able to ask if any preliminary results have already surfaced. Any unreleased policy pieces could not fully take part in the results section as they were still confidential in nature. Some participants of the interviews have also chosen to not include their quotes in the thesis, which means their answers will be processed in an indirect way.

6.1 How does the Dutch government monitor (cyber) espionage within the Dutch industry and educational sector?

To fully answer this question, it should be clear what is meant with monitoring. Many of the participants of the interviews answered the questions by not only talking about technical measures in which attack metrics get measured and researched, but also often included policy pieces and audits that are required to fully grasp the current level of monitoring. The government will never be able to fully monitor all espionage attempts and all other potential dangers to the economic- and knowledge security. This is because they will often rely on the information that is being shared with them by businesses or knowledge institutions and the fact that it is not clear from the start if a cyber attack actually concerns an espionage attempt. If the organisations do not share information with the government, the government will not be able to act on these specific cases or create policies to potentially negate these dangers. Specific organisations, like the businesses and organisations in the vital sector, are often required to report certain information to the government by legislation.

But there are a lot of companies and knowledge institutions that are not within the vital sector and are under no obligation to share such information. The follow-up question would be: is it the government's job to control all these organisations? In the Netherlands there is an academic freedom and freedom to trade, if it does not damage the Dutch national security. But this rule often finds itself in a grey area in which it is not yet clear beforehand if a certain research collaboration or business deal will damage the national security. The Dutch government has been making a lot of strides in tackling the espionage problems, especially with the globalisation and internationalisation of universities creating prime opportunities for different espionage forms. For both the educational sector and private sector, the government has created Desks that organisations within these domains can use to get advice on dealing with certain case studies. There is still a lot of ground to cover, especially with the monitoring (auditing) of the educational and research organisations, which often hide under the shadow of academic freedom.

6.2 Is the Dutch government aware of the espionage danger?

The Dutch government is aware of the potential dangers of espionage, but also has the topics of knowledge- and economic security clearly within scope. Even though the participants of the interview mentioned that the last few years have been very productive when it comes to these topics, this does mean that the last few years have been a race to catch-up. Previously, there has not been that much attention towards these topics. Mostly the AIVD and MIVD have been tasked with combatting espionage and protecting economic security, but now many more organisations are actively busy with implementing integral security practices. The Netherlands is often considered a knowledge-economy, so protecting this knowledge has become more of a focus for businesses and the government alike. Whether it has been the geopolitical conflicts that ignited the need for more attention to these topics or the fact that globally there has been a stride in favour of digitalisation of services is not entirely clear, so more investigation into this phenomenon would be required.

The same could be said for research institutes that have to deal far more with knowledge security, the past few years have ignited the need for awareness far more than the years before. This means some universities and research institutes must still take a lot of steps to get to a level that they themselves would find acceptable. The Dutch government has released several tools that can be used by a variety of organisations. These tools also allow research institutions to ask certain questions within the safety of a governmental Desk, to which most important governmental organisations are connected. There is also a Desk that is specifically tailored to businesses. One caveat of awareness is the fact that the government can only be aware of the threats they know. And in some cases, they are dependent on information from these research institutions or businesses to report certain cases to them.

Another crucial factor is the awareness at the political level of the Netherlands. As the Dutch politicians decide what kind of legislation will be implemented across the Netherlands. But seeing many different of forms of legislation that are already accepted by the House of Representatives that focus on the economic- and knowledge security terrains, it for now at least looks like it is going in a direction where espionage, knowledge- and economic security are considered more important. As new elections have been held, it also remains unclear if these topics will receive the same amount of attention as they have been given by the previous parliament, and whether this change will impact the budgets of the ministries trying to combat these threats.

6.3 How big does the Dutch government perceive the danger of espionage to be in general, and what are the trends?

The government classifies espionage as a big threat and one of the findings states that it is quite difficult to tell the intent behind a cyber attack. It is unclear what various threat actors are planning when they are launching their cyber attacks. As both state actors and criminals can be APT's, it is important to make sure an organisations cyber resilience is up to the task, this is the case for both public organisations as well as private companies. So, the dangers are bigger than just espionage, and the topics of espionage, economic- and knowledge security are often intertwined. For example, China might want to start a research collaboration with the Netherlands to gain modern technology/knowledge. This will then both be part of the espionage branch just as it will touch the knowledge security approach.

Regarding the trends, this has proved to be a tricky question to answer. Like mentioned before, the initial attribution of a cyber attack is quite difficult. It could be that a threat actor is trying to enter an organisations network with the intention of spying on them, but it could also be a ransomware attack with monetary goals. As there are clear trends for cyber attacks, these could also be applied for the potential espionage attacks, but these are not necessarily espionage methods as much as they follow regular cyber attack methods.

There are however different forms of (classical) espionage that have existed for a long time which are still relevant. For example, the use of spying student networks and the use of diaspora communities that enable countries to boost their own interests overseas. As these espionage methodologies often evolve over a longer period and are not necessarily reliant on cyber attacks, it becomes difficult to tell if there are short term trends like with cyber attacks. It was quite clear however that geopolitical shifts caused a change in the behaviour of state actors. This change could mean, an additional focus on specific countries or specific sectors. The Participants of the interviews often named the increased number of cyber attacks on Ukraine, launched from Russian territory as an example of changing nation state behaviour.

6.4 What are the main challenges for the Dutch government regarding managing national cyberspace against espionage?

There are multiple challenges for the government when managing the national cyberspace against espionage. Firstly, the ever-growing attack surface due to the rapid digitalisation of the Dutch National government is creating more potentially unsafe digital environments. The services that the Dutch government is providing are becoming more readily available online or will be solely accessible on the internet. This causes the need for a better nation-wide cyber resilience even more important. Especially when considering that many more European countries are digitalising their government services, this trend is bound to continue.

Another important challenge is the difficulty when initially triaging attacks. As we mentioned, when initially triaging a cyber attack, you do not know the intent behind it. So, you might suspect that a certain attack is an attempt to enter the system and seek for information, but it could also be a ransomware attack for monetary gain. As both attacks are unwanted in an organisations network, these attacks can be blocked by detection rules in a SOC (security operations centre) environment. This does however mean that you cannot actively measure the amount of attacks the are happening solely with the goal of spying. Just like the intent behind the attack, the person/group/state behind the attack is also hard to guess beforehand. You might have indicators that can show it could be a larger APT, but this still does not tell you whether it is a state actor trying to spy on their target.

Another problem is the actively growing threat of script kiddies and criminals APT's. Not only state actors perform cyber attacks, and while cyber attacks can have various goals, criminals could also be looking for information that they could sell. So, all the different threat actors form a danger for the Dutch national cyberspace and its information. Especially when you factor in that topic like economic- and knowledge security could also potentially be exploited within these cyber attacks. As the Dutch national government is quite big, there are different targets within the various ministries. The responsibility for knowledge security is mostly located at the Ministry of Education, and the responsibility for economic security will mostly be located at the NCTV, AIVD and the Ministry of Economic Affairs.

6.5 What are the recommended practices and procedures for organizations to defend themselves against espionage?

After completing the interviews with twelve professionals in the field, the literature review and document analysis, it was clear that cyber security is something that you have to keep investing in, whether it is time or money. With the many different TTP's being used by threat actors that are currently present in the threat landscape, the need for a pan-national standardised level of cybersecurity becomes increasingly important. This is where the NIS2 will play a big part. Currently the Dutch government is still translating the legislation from the European Union into a Dutch variant which will become required for all vital Dutch organisations. During many of the interviews, a lot of the participants mentioned that the new NIS2 being introduced had a positive connotation. They were also optimistic that it will make the EU more cyber resilient.

Furthermore, as the need for good cyber security keeps increasing, organisations themselves are responsible for getting their cyber security in order. The Dutch Government can help organisations with certain parts of this cyber security chain. And are also sometimes legally obliged to do so if they are within certain vital sectors. The organisations and businesses can ask help from the Dutch government when it comes to espionage, knowledge- and economic security risks as well as some cyber security related risks. There are tools available that the government provides, but the companies and knowledge institutes themselves, are responsible for using these tools well.

There are multiple ways an organisation can weapon themselves against cyber threats. A common baseline that governmental organisations use is the BIO (Baseline Informatiebeveiliging Overheid), this baseline is based on the ISO 27001/2/5. The BIO is relevant for all governmental organisations, so that also includes the municipalities and water works. Business and organisations slightly adjacent to the government can use the original ISO 27001/5, as the BIO is based on these standards, to create more digitally resilient organisations.

6.6 Implications

These results can be used to inspire further research towards monitoring espionage within a governmental domain. This thesis is specifically tailored to the way the Dutch government is monitoring espionage, but as the NIS2 will (theoretically) provide the whole EU with the same amount of cyber resilience, certain monitoring methods which have been described within this thesis might be relevant for other countries as well.

Other studies mentioned in this thesis often describe the dangers of different forms of espionage and the potential loss of data/technology. By combining the knowledge within this thesis together with the already pre-existing academic literature, an interesting perspective on espionage emerges. This thesis tries to describe the difficulties in protecting the national cyberspace against the aforementioned espionage dangers, while offering a light at the end of the tunnel, in the form of potential improvement points. This could also prove beneficial for other researchers to compare these results against the method of monitoring done by other countries.

In the end, the goal of this thesis is to give insight into the level of monitoring, differentiate between challenges and successes experienced by the government, and eventually providing some insight on how to improve the cyber resilience in the future.

7 Limitations

We now discuss the main limitations of this research.

The digital domain is ever evolving, which means new legislation and documents will arrive at certain intervals. This does mean, however, that certain documentation that will be published after April 2024, will not be taken into consideration for this thesis.

Another caveat is the fact that the scope of this thesis would be too large if we were to include all the Dutch research institutions and knowledge institutions. Researching all the different knowledge institutes and organisations would take time out of the already busy schedule, which was required to answer the main research questions. For a Master thesis, including all the different research organisations would make the scope too grand.

Currently, the sample size is still too small to take conclusions about all knowledge institutions, but the interviews that have been conducted did paint a clear picture of the current status of knowledge security within certain educational organisations.

Even though we do deem the studied sample to be sufficient, we initially would have liked to include more participants from other organisations as well. This is something that we recommend for future research on this topic. In future research, it would also be interesting to create groups for different participants and categorize them based on their affiliation with the public or private sector.

The participants have been selected due to their knowledge and expertise within various fields, some forms of convenience sampling have been used to garner a good number of participants. We have made a significant effort to expand on the number of participants, and, to increase the participant diversity, we have tried snowballing: we asked all interviewees to nominate other suitable participants. However, not all interviewees were comfortable with giving details of colleagues, due to the sensitive nature of the subject.

Significant effort has been put into creating an open environment which would allow the participants to give detailed answers, yet as the discussion often contained sensitive topics, this might have led to participants not fully disclosing potentially interesting information. When consent forms were signed between the interviewer and participants, several participants chose to not allow including quotes from their interviews in the thesis. This means that potentially important quotes have been excluded from the research presentation.

Also, convincing certain organisations about the relevance of partaking in said interviews has been challenging. This means that even though we have made significant effort to incorporate all relevant Dutch ministerial organisations, we have not been able to include all organisations.

Due to the sensitivity of the topic, there are not that many relevant publicly available sources about the methods of countering (cyber) espionage. Most of the data available about specific modern espionage cases has come from grey sources. This makes it difficult to compare the results of this thesis to similar articles in scientific journals.

Another difficulty of researching espionage in a qualitative way is the bias that exists within the researcher and because of the choice of the interviewing method, also within the participants. The purpose of this research is to give more insights into the ways the Dutch government is monitoring espionage, and to find eventual pitfalls and successes. But as the researcher is also a Dutch national, some might argue that a Dutch or Western viewpoint might be prevalent in this thesis.

A difficult psychological effect we have to factor in for this thesis, is the social desirability bias. Chung and S. Monroe (2003), define the social desirability bias as: "the tendency of individuals to underestimate (overestimate) the likelihood they would perform an undesirable (desirable) action". Participants of the interviews are more likely to give desirable answers which might overestimate/underestimate certain parts of their work. To try and counter this effect, we used reflexive questions which allowed the participants to reflect on their answer and broader approach to certain problems. As a concrete example, we asked participants whether certain policy decisions they made, had the desired effect they originally had in mind. This will require the participant to reflect on certain parts of their work. This will not fully counter the bias that might exist, as we have not taken certain characteristics of participants into account, like their religion, as Chung and S. Monroe (2003), describe can be important when measuring this bias.

8 Conclusion

The Dutch national government has taken several steps to try and get in control of the various digital threats. With an ever-increasing digital attack surface, the difficulties in triaging initial cyber attacks and the massive number of organisations within important sectors that the government is looking out for, the future will hold several challenges when it comes to managing the national cyberspace. In this thesis, we describe 5 main challenges: 'difficulties to attribute an attack as cyber espionage´, 'lack of awareness at organisations, businesses, and people', 'political importance', 'educational freedom allows for less control by the government' and 'geopolitical changes cause a very dynamic environment'. We also denote 2 themes which describe certain successes: 'new development of tools, policies and legislation' and 'governance within the government; defined roles, and responsibilities'.

The last few years have proved quite successful in the number of tools and legislation the Dutch government has been able to push out. There also seems to be an increase in the amount of awareness for the espionage, economic- and knowledge security related topics within certain departments of the government. Even within the political spectrum there seems to be more attention for these topics, which will hopefully lead to more focused legislation, like the new criminalization of more (modern) espionage forms. Within the Dutch government the governance structure allows for clear responsibilities and the ministries themselves have clear portfolios which they focus on.

Due to the massive number of cyber attacks that are happening daily, it is important for organisations within the public- and private sector to properly protect their crown jewels. State actors such as China and Russia are notorious when it comes to their use of industrial and cyber espionage methods to gather intelligence. China and Russia are still using several TTP's to gather as much Western technology/information as possible, as in some sectors, they are still relatively dependent on it. Both cyber attacks as well as classical espionage acts via universities and research institutes are actively being exploited by these state actors to gain their sought-after information. Understanding the threat espionage creates and actively taking measures to protect company information, are imperative if organisations value their intellectual property and high-risk technology.

The Dutch government has also introduced plenty of new helpful tools that can be used to measure the current state of resilience and can also offer expertise where needed. To tackle espionage, economic- and knowledge security related problems/cases, organisations can contact either the business Desk (which focuses on economic security/espionage) or the Desk designed for knowledge institutions (which focuses on knowledge security/espionage). Within the government, there are usually close contacts between the ministries which allows for the fast transfer of information and expertise. Businesses and (research) organisations are however required to know about the existence of these Desks, and actively use the expertise that the government is offering. If they will not be used as originally designed, these tools might lose their inherent value. In the end, the government doers have clear responsibilities for their focus groups, just like the organisations within the vital sectors also have certain incident reporting responsibilities towards the government.

If needed, the Dutch public sector now has a growing amount of private sector partners, they can choose to involve. From SOC monitoring to threat intelligence information, governmental organisations can use this private sector experience if needed. The private sector has become more involved in researching nation state threat actors as well, which means governments have more options of finding their much-needed information about these actors. This also gives the governmental organisations more agency to try and be ahead of the curve when it comes to threat intelligence and actively preparing for cyber attacks. These public-private partnerships can become even more important as the capacity for security related FTE's can become more difficult to fill in the future with the ongoing competition within this industry.

There are several areas which could be expanded further upon, regarding the thesis topics. More research could go into the different knowledge institutions and the different ethical rules these organisations uphold, and the way knowledge security is currently being protected at these organisations. The way research is done could be quite interesting to investigate as it would require an internal critical reflection on current research ethics and methodologies. As universities all over the world are working together, investigating how this collaboration should take place could also prove quite beneficial. This means that for future iterations, organisations like the TNO could be included to see whether they agree with the findings and what kind of measures they are currently taking to prevent unwanted transfers of knowledge within certain phases of research. As we were also not able to speak to all the different universities and research organisations, there is still a gap in knowledge to take conclusion about all the different ways the universities implemented certain cyber security practices.

Another area which could be quite useful to further investigate would be the private companies holding a lot of the sensitive technology that the government aims to protect. Getting an insight into what these powerful companies are doing and what their challenges are, could help bring awareness to these problems within the public domain.

References

Abouzakhar, N., Jones, A. M., & Angelopoulou, O. (2017). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. *Green Computing and Communications*. https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2017.62

Adams, J., Johnson, J. A., & Grant, J. (2021). The rise of UK–China research collaboration: Trends, opportunities and challenges. *Science and Public Policy/Science & Public Policy*, *49*(1), 132–147. https://doi.org/10.1093/scipol/scab069

Adviesraad voor wetenschap, technologie en innovatie [AWTI]. (2022). Advies: Kennis in conflict - veiligheid en vrijheid in balans. In *AWTI* (ISBN: 978-90-77005-92-7). Adviesraad voor wetenschap, technologie en innovatie. Retrieved June 12, 2023, from https://www.awti.nl/documenten/adviezen/2022/11/29/index

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Ahmed, J., Gharakheili, H. H., Raza, Q., Russell, C., & Sivaraman, V. (2020). Monitoring enterprise DNS queries for detecting data exfiltration from internal hosts. *IEEE eTransactions on Network and Service Management*, *17*(1), 265–279. https://doi.org/10.1109/tnsm.2019.2940735

AIVD. (2023). AIVD Annual Report 2022. In *AIVD*. Retrieved July 27, 2023, from https://english.aivd.nl/publications/annual-report/2023/06/16/aivd-annual-report-2022

AIVD [AIVD]. (2022). Dreigingsbeeld Statelijke Actoren (DBSA 2). In *AIVD*. AIVD. Retrieved July 26, 2023, from https://www.aivd.nl/onderwerpen/spionage/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2

Al-Bataineh, A., & White, G. (2012). Analysis and detection of malicious data exfiltration in web traffic. *IEEE*. https://doi.org/10.1109/malware.2012.6461004

Ali, O., Shrestha, A., Chatfield, A. T., & Murray, P. A. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), 101419. https://doi.org/10.1016/j.giq.2019.101419

Anderson, C. (2010). Presenting and evaluating qualitative research. *American Journal of Pharmaceutical Education*, *74*(8), 141. https://doi.org/10.5688/aj7408141

Anggraini, N., Binariswanto, & Legowo, N. (2019). Cloud Computing Adoption Strategic Planning using ROCCA and TOGAF 9.2: A study in Government Agency. *Procedia Computer Science*, *161*, 1316–1324. https://doi.org/10.1016/j.procs.2019.11.247

ASML Says Ex-Employee in China Stole Chip Data. (2023, February 15). Bloomberg. https://www.bloomberg.com/news/articles/2023-02-15/asml-says-ex-employee-in-china-misappropriated-chip-data

Australische Strategic Policy Institute. (n.d.). *About: The China Defence Universities Tracker is a database of Chinese institutions engaged in military or security-related science and technology research. It was created by ASPI's International Cyber Policy Centre.* ASPI. Retrieved March 1, 2024, from https://unitracker.aspi.org.au/about/

Baker, S., & Edwards, R. (2012). How many qualitative interviews is enough. *National Centre for Research Methods Review Paper*. https://eprints.ncrm.ac.uk/id/eprint/2273/

Banks, W. C. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory Law Journal*, *66*(3), 513. https://law.emory.edu/elj/content/volume-66/issue-3/articles/cyber-espionage-electronic-surveillance-media-coverage.html

Bederna, Z., & Szádeczky, T. (2020). Cyber espionage through Botnets. *Security Journal*, *33*(1), 43–62. https://doi.org/10.1057/s41284-019-00194-6

Bellaby, R. W. (2023). The Ethics of economic espionage. *Ethics & International Affairs*, *37*(2), 116–133. https://doi.org/10.1017/s0892679423000138

Ben Moshe, N. B. (2022). Chinese Espionage Operations in the United States: And in Israel? *Institute for National Security Studies*, *1560*. https://www.inss.org.il/wp-content/uploads/2022/02/no.-1560.pdf

Bojanc, R., & Jerman-Blaič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

Boo, H. W. (2017, season-02). *AN ASSESSMENT OF NORTH KOREAN CYBER THREATS*. JSTOR. Retrieved July 27, 2023, from https://www.jstor.org/stable/44321274

Borak, D., Jiang, S., Gaouette, N., Cohen, Z., & Marquardt, A. (2019, February 1). *US intelligence warns China is using student spies to steal secrets*. CNN. Retrieved September 14, 2023, from https://edition.cnn.com/2019/02/01/politics/us-intelligence-chinese-student-espionage/index.html

Boroš, M., Boroš, M., & Halaj, M. (2019). REQUIRED COMPETENCIES OF SECURITY MANAGERS FOR DECISION-MAKING. *INTED Proceedings*. https://doi.org/10.21125/inted.2019.0992

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brewer, R. (2014). Advanced persistent threats: minimising the damage. *Network Security*, *2014*(4), 5–9. https://doi.org/10.1016/s1353-4858(14)70040-6

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26–31. https://doi.org/10.1016/j.istr.2005.12.001

Buchan, R. (2021). Cyber espionage and international law. In *Edward Elgar Publishing eBooks*. https://doi.org/10.4337/9781789904253.00021

Button, M. (2019). Editorial: economic and industrial espionage. *Security Journal*, *33*(1), 1–5. https://doi.org/10.1057/s41284-019-00195-5

Campbell, J. L., Quincy, C. D., Osserman, J., & Pedersen, O. K. (2013). Coding in-depth semistructured interviews. *Sociological Methods & Research*, *42*(3), 294–320. https://doi.org/10.1177/0049124113500475

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012). Cybersecurity Policy-Making at the Local Government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Journal of Homeland Security and Emergency Management*, *9*(2). https://doi.org/10.1515/jhsem-2012-0003

Cascio, M. A., Lee, E., Vaudrin, N., & Freedman, D. A. (2019). A Team-based approach to open coding: Considerations for creating intercoder consensus. *Field Methods*, *31*(2), 116–130. https://doi.org/10.1177/1525822x19838237

Chen, M., Yao, Y., Liu, J., Jiang, B., Su, L., & Lü, Z. (2018). A Novel Approach for Identifying Lateral Movement Attacks Based on Network Embedding. *IEEE*. https://doi.org/10.1109/bdcloud.2018.00107

Chung, J., & S. Monroe, G. (2003). Exploring Social Desirability Bias. *Journal of Business Ethics*, *44*(4), 291–302. https://doi.org/10.1023/a:1023648703356

Clarke, V., & Braun, V. (2016). Thematic analysis. *The Journal of Positive Psychology*, *12*(3), 297–298. https://doi.org/10.1080/17439760.2016.1262613

Clingendael. (2021). Technologische samenwerking met China: Risico's voor en belangen van Nederland op de terreinen halfgeleiders, fotonica en medicijn-/vaccinontwikkeling. In *Clingendael*. https://www.clingendael.org/publication/technologische-samenwerking-met-china

CSRC Content Editor. (n.d.). *Cyber Security - Glossary | CSRC*. https://csrc.nist.gov/glossary/term/cyber_security

Cutcliffe, J. R. (2000). Methodological issues in grounded theory. *Journal of Advanced Nursing*, *31*(6), 1476–1484. https://doi.org/10.1046/j.1365-2648.2000.01430.x

Dann, G., & Haddow, N. (2007). Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! and the Business of Censoring China's Internet. *Journal of Business Ethics*, *79*(3), 219–234. https://doi.org/10.1007/s10551-007-9373-9

De Bruijn, A., Booij, D., Emanuel, H., Sys, M., & Eikelenboom, S. (2023, November 21). Drones en beton tegen kogels: ook samenwerken met 'gewone' Chinese universiteiten levert risico's op. *Follow the Money - Platform Voor Onderzoeksjournalistiek*. https://www.ftm.nl/artikelen/semenwerken-met-gewone-chinese-universiteiten-eveneens-riskant

Deibert, R., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. (2009). Tracking GhostNet: investigating a cyber espionage network. *University of Oxford*. https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651/download_file?safe_filename=Gh0stNet.pdf&file_format=application%2Fpdf&type_of_work=Report

Dilek, E., & TalİH, Ö. (2022). Overview of Cyber Espionage Incidents and Analysis of Tackling Methods. *IEEE*. https://doi.org/10.1109/iscturkey56345.2022.9931893

DPG Media Privacy Gate. (n.d.). https://www.parool.nl/amsterdam/erdogan-krijgt-in-de-rai-meer-dan-66-procent-van-de-turks-nederlandse-stemmen~be8c04b7/

EU Council. (n.d.). *EU sanctions against Russia explained*. European Council. Retrieved July 26, 2023, from https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/

European Commission [EC] & Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs,. (2019). The scale and impact of industrial espionage and theft of trade secrets through cyber. In *Publications Office of the European Union* (10.2873/528416). Publications Office of the European Union. Retrieved April 11, 2023, from https://op.europa.eu/en/publication-detail/-/publication/b3b5fcfb-4541-11e9-a8ed-01aa75ed71a1/language-en/format-PDF/source-90181868

Fraumann, E. (1997). Economic Espionage: Security Missions redefined. *Public Administration Review*, *57*(4), 303. https://doi.org/10.2307/977311

Gilli, A., & Gilli, M. (2019a). Why China has not caught up yet: Military-Technological superiority and the limits of imitation, reverse engineering, and cyber espionage. *International Security*, *43*(3), 141–189. https://doi.org/10.1162/isec_a_00337

Gilli, A., & Gilli, M. (2019b). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*, *43*(3), 141–189. https://doi.org/10.1162/isec_a_00337

Gooijer, L., & Veiligheid, A. N. (2019). *Geïntegreerde risicoanalyse Nationale Veiligheid*. https://repository.tno.nl/islandora/object/uuid%3A9d14f4c9-7c3c-4dc4-a986-8f1409352efe

Grabiszewski, K., & Minor, D. (2018). Economic espionage. *Defence and Peace Economics*, *30*(3), 269–277. https://doi.org/10.1080/10242694.2018.1477400

Guillemin, M., & Gillam, L. (2004). Ethics, reflexivity, and "Ethically Important moments" in research. *Qualitative Inquiry*, *10*(2), 261–280. https://doi.org/10.1177/1077800403262360

Handcock, M. S., & Gile, K. J. (2011). Comment: On the concept of snowball sampling. *Sociological Methodology*, *41*(1), 367–371. https://doi.org/10.1111/j.1467-9531.2011.01243.x

Hannah, D. M., & Robertson, K. (2015). Why and How Do Employees Break and Bend Confidential Information Protection Rules? *Journal of Management Studies*, *52*(3), 381–413. https://doi.org/10.1111/joms.12120

Hannas, W. C., Mulvenon, J. C., & Puglisi, A. B. (2013). Chinese Industrial Espionage. In *Routledge eBooks*. https://doi.org/10.4324/9780203630174

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, *43*, 165–172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, *29*(3), 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

Hooghe, D., & Dekker, B. (2020). China's invloed op onderwijs in Nederland: een verkenning. In *Clingendael*. Clingendael. Retrieved April 4, 2023, from https://www.clingendael.org/sites/default/files/2020-07/Rapport_politieke_beinvloeding_in_het_onderwijs_juni_2020.pdf

Hove, S., & Anda, B. (2005). Experiences from Conducting Semi-structured Interviews in Empirical Software Engineering Research. *IEEE*. https://doi.org/10.1109/metrics.2005.24

Hruschka, D. J., Schwartz, D., StJohn, D. C., Picone-Decaro, E., Jenkins, R. A., & Carey, J. W. (2004). Reliability in Coding Open-Ended Data: Lessons Learned from HIV Behavioral Research. *Field Methods*, *16*(3), 307–331. https://doi.org/10.1177/1525822x04266540

Hsu, C., Wang, T., & Lu, A. (2016). *The Impact of ISO 27001 Certification on Firm Performance*. https://doi.org/10.1109/hicss.2016.600

ICO Wizard - bio-overheid. (n.d.). https://www.bio-overheid.nl/ICO-Wizard/

Informatie- en communicatietechnologie (ICT). (2022, June 30). Tweede Kamer Der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2023D16182&did=2023D16182

Inkster, N. (2015). Cyber espionage. *Adelphi/Adelphi [Series]*, *55*(456), 51–82. https://doi.org/10.1080/19445571.2015.1181443

Johnson, L. K. (2019). American universities, the CIA, and the teaching of national security intelligence. In *Routledge eBooks* (pp. 79–93). https://doi.org/10.4324/9780203702086-3

Jones, A. (2008). Industrial espionage in a hi-tech world. *Computer Fraud & Security*, *2008*(1), 7–13. https://doi.org/10.1016/s1361-3723(08)70010-1

Jonsson, M. (2023). Espionage by Europeans: treason and counterintelligence in post-Cold war Europe. *Intelligence and National Security*, 1–16. https://doi.org/10.1080/02684527.2023.2254020

Jung, S., & Jung, C. (2020). Classification of Industrial Espionage Cases and Countermeasures. *IEEE*. https://doi.org/10.1109/bigcomp48618.2020.00-18

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

KNAW. (2021). Academische vrijheid in nederland: Een begripsanalyse en richtsnoer. In *KNAW* (ISBN 978-90-6984-745-0). Koninklijke Nederlandse Akademie van Wetenschappen. Retrieved March 1, 2024, from https://storage.knaw.nl/2022-05/20210217-webversie-advies-Academische-vrijheid.pdf

KNAW. (2023, October 10). *KNAW waarschuwt voor voorgenomen wet kennisveiligheid - KNAW*. Koninklijke Nederlandse Akademie Van Wetenschappen. Retrieved March 5, 2024, from https://www.knaw.nl/nl/nieuws/knaw-waarschuwt-voor-voorgenomen-wet-kennisveiligheid

Knowledge security | NWO. (n.d.). NWO. https://www.nwo.nl/en/knowledge-security

Lee, J. J., & Haupt, J. P. (2020). Winners and losers in US-China scientific research collaborations. *Higher Education*, *80*(1), 57–74. https://doi.org/10.1007/s10734-019-00464-7

Lee, R. W. (1982). Political absorption of western technology: The Soviet and Chinese cases. *Studies in Comparative Communism*, *15*(1–2), 9–33. https://doi.org/10.1016/0039-3592(82)90003-5

Leviathan, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope, Group G0065 | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/groups/G0065/

Lewis, J. A. (2013). CYBER ESPIONAGE AND THE THEFT OF U.S. INTELLECTUAL PROPERTY AND TECHNOLOGY. In *JSTOR*. Center for Strategic and International Studies (CSIS). Retrieved May 23, 2023, from https://www.jstor.org/stable/resrep37659

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Libicki, M. C. (2017). The coming of cyber espionage norms. *IEEE*. https://doi.org/10.23919/cycon.2017.8240325

Libicki, M. C. (2018). Drawing inferences from cyber espionage. *IEEE*. https://doi.org/10.23919/cycon.2018.8405013

Liebetrau, T. (2022). Cyber conflict short of war: a European strategic vacuum. *European Security*, *31*(4), 497–516. https://doi.org/10.1080/09662839.2022.2031991

Lindsay, J. R. (2015). The impact of China on cybersecurity: fiction and friction. *International Security*, *39*(3), 7–47. https://doi.org/10.1162/isec_a_00189

Livingston, S. (2022). *The Chinese Communist Party Targets the Private Sector*. https://www.csis.org/analysis/chinese-communist-party-targets-private-sector

Mackieson, P., Shlonsky, A., & Connolly, M. (2018). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work*, *18*(6), 965–980. https://doi.org/10.1177/1473325018786996

Majed, H., Noura, H., & Chehab, A. (2020). Overview of Digital Forensics and Anti-Forensics Techniques. *IEEE*. https://doi.org/10.1109/isdfs49300.2020.9116399

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *IEEE*. https://doi.org/10.1109/cymaen57228.2023.10051114

Mandiant, Mandiant, Mandiant, Mandiant, Mandiant, Mandiant, Mandiant, & Mandiant. (n.d.). APT40 | Examining a China-Nexus espionage Actor | Mandiant. *Mandiant*. https://www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor

Mazurczyk, W., & Caviglione, L. (2021). Cyber reconnaissance techniques. *Communications of the ACM*, *64*(3), 86–95. https://doi.org/10.1145/3418293

Messaoud, B. I. D., Guennoun, K., Wahbi, M., & Sadik, M. (2016). Advanced Persistent Threat: New analysis driven by life cycle phases and their challenges. *IEEE*. https://doi.org/10.1109/acosis.2016.7843932

Ministerie van Algemene Zaken. (2024, February 15). *Hoofdlijnen Wet open overheid*. Wet Open Overheid (Woo) | Rijksoverheid.nl. https://www.rijksoverheid.nl/onderwerpen/wet-open-overheid-woo/hoofdlijnen-woo

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2022, December 20). *Strafbaarstelling van moderne spionagevormen*. Spionage | AIVD. https://www.aivd.nl/onderwerpen/spionage/strafbaarstelling-van-moderne-spionagevormen

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2023, March 21). *Kabinet ontraadt gebruik spionagegevoelige apps voor ambtenaren Rijksoverheid*. Nieuwsbericht | Rijksoverheid.nl. https://www.rijksoverheid.nl/actueel/nieuws/2023/03/21/kabinet-ontraadt-gebruik-spionagegevoelige-apps-voor-ambtenaren-rijksoverheid

Ministerie van Economische Zaken en Klimaat. (2024, January 19). *Wet veiligheidstoets op investeringen, fusies en overnames*. Het Stelsel Van Investeringstoetsing | Bureau Toetsing Investeringen. https://www.bureautoetsinginvesteringen.nl/het-stelsel-van-toetsen/wet-veiligheidstoets-investeringen-fusies-en-overnames

Ministerie van Justitie en Veiligheid. (2019, December 16). *Wetsartikel computervredebreuk*. Cybercrime | Openbaar Ministerie.

https://www.om.nl/onderwerpen/cybercrime/hack_right/wetsartikel-computervredebreuk

Ministerie van Justitie en Veiligheid. (2022, December 2). *Vervolging en rechtszaak*. MH17 Vliegramp | Openbaar Ministerie. https://www.om.nl/onderwerpen/mh17-vliegramp/vervolging-en-rechtszaak

Ministerie van Onderwijs, Cultuur en Wetenschap. (2023a, September 8). *Home - Loket Kennisveiligheid*. https://www.loketkennisveiligheid.nl/

Ministerie van Onderwijs, Cultuur en Wetenschap. (2023b, October 17). *Kamerbrief bij Sectorbeeld kennisveiligheid universiteiten*. Kamerstuk | Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/kamerstukken/2023/10/16/sectorbeeld-kennisveiligheid-universiteiten

Ministerie van Onderwijs Cultuur en Wetenschap [OCW]. (2020). Verkenning wetenschappelijke samenwerking Nederlandse en Chinese kennisinstellingen. In *Rijksoverheid*. Ministerie van Onderwijs Cultuur en Wetenschap. Retrieved April 11, 2023, from https://www.rijksoverheid.nl/documenten/rapporten/2020/11/16/rapport-verkenning-wetenschappelijke-samenwerking-nederlandse-en-chinese-kennisinstellingen

MIVD. (2023). Militaire Inlichtingen- en Veiligheidsdienst (MIVD): Openbaar Jaarverslag 2022. In *Rijksoverheid*. Rijksoverheid. Retrieved June 26, 2023, from https://www.rijksoverheid.nl/documenten/jaarverslagen/2023/04/19/openbaar-jaarverslag-2022-mivd

Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing Attack Models for IT Systems: Lockheed Martin’s Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. *IEEE*. https://doi.org/10.1109/isse54508.2022.10005490

Navarro, P. (2020, February 23). US: don’t give China control of intellectual property group. *Financial Times*. Retrieved April 11, 2023, from https://www.ft.com/content/91addb98-532b-11ea-a1ef-da1721a0541e

Nederland beklaagt zich over MH17-spionage door Oekraïne. (2018, July 5). RTL.nl. https://www.rtl.nl/nieuws/nederland/artikel/4272856/nederland-beklaagt-zich-over-mh17-spionage-door-oekraine?redirect=rtlnieuws

NOS. (2022, November 30). Spionnen hebben het op Nederlandse technologie voorzien, “we waren naïef.” *NOS*. https://nos.nl/nieuwsuur/artikel/2454626-spionnen-hebben-het-op-nederlandse-technologie-voorzien-we-waren-naief

NWO, KNAW, Vereniging Hogescholen, NFU, TO federatie, Rijksoverheid, & Universiteiten van Nederland. (2022). Nationale leidraad kennisveiligheid: Veilig internationaal samenwerken. In *Open Overheid*. Rijksoverheid. Retrieved March 1, 2024, from https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid

Poreba, J. (2012). Neutralizing China’s Student-Spy Network. *International Journal of Intelligence and Counterintelligence*, *25*(2), 260–291. https://doi.org/10.1080/08850607.2012.623037

Putra, I. M. M., & Mutijarsa, K. (2021). *Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005*. https://doi.org/10.1109/eiconcit50028.2021.9431865

Putra, S. J., Gunawan, M. N., Sobri, A. F., Muslimin, J., Amilin, & Saepudin, D. (2020). *Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company*. https://doi.org/10.1109/citsm50537.2020.9268845

Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden. (n.d.). PIANOo - Expertisecentrum Aanbesteden. https://www.pianoo.nl/nl/regelgeving/crisis-en-inkoop/nationale-veiligheid/quickscanrisicomitigatie-nationale-veiligheid-bij

Roy, S., Sharmin, N., Acosta, J. C., Kiekintveld, C., & Lászka, Á. (2022). Survey and taxonomy of adversarial reconnaissance techniques. *ACM Computing Surveys*, *55*(6), 1–38. https://doi.org/10.1145/3538704

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56–62. https://doi.org/10.1016/j.cose.2006.10.008

Ruim 900 Nederlandse bedrijven in handen van Chinezen: "Risico op spionage." (2022, September 28). RTL Nieuws. https://www.rtlnieuws.nl/onderzoek/artikel/5335199/china-nederlandse-bedrijven-eigendom-invloed-spionage

Shi, Y. (2018). Data Security and Privacy Protection in Public Cloud. *IEEE*. https://doi.org/10.1109/bigdata.2018.8622531

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88–115. https://doi.org/10.1016/j.jnca.2016.11.027

Singh, N. (2009). The Khan Proliferation Network. *JSTOR*, *13*(4). https://www.jstor.org/stable/48505219

Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., & Park, J. H. (2016). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. *The Journal of Supercomputing*, *75*(8), 4543–4574. https://doi.org/10.1007/s11227-016-1850-4

Sinha, S. (2012). Understanding industrial espionage for greater technological and economic security. *IEEE Potentials*, *31*(3), 37–41. https://doi.org/10.1109/mpot.2012.2187118

Snetselaar, D. (2022). Dreams Lab: assembling knowledge security in Sino-Dutch research collaborations. *European Security*, *32*(2), 233–251. https://doi.org/10.1080/09662839.2022.2127317

Steadman, J., & Scott-Hayward, S. (2018). DNSxD: Detecting Data Exfiltration Over DNS. *IEEE*. https://doi.org/10.1109/nfv-sdn.2018.8725640

Sulmasy, G., & Yoo, J. (2007). Counterintuitive: intelligence operations and international law. *Michigan Journal of International Law*, *28*(3), 625–638. https://lawcat.berkeley.edu/record/1120718/files/fulltext.pdf

Suresh, N. R., Malhotra, N., Kumar, R., & Thanudas, B. (2012). An integrated data exfiltration monitoring tool for a large organization with highly confidential data source. *IEEE*. https://doi.org/10.1109/ceec.2012.6375395

Susanto, H., Nabil Almunawar, M., & Chee Tuan, Y. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences IJECS-IJEN*, *11*(5), 21–27.

Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department | CISA. (2021, July 20).

Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200a

Teer, J. (2022). China's militaire opkomst en Europese technologie. In *The Hague Centre for Strategic Studies*. HCSS. Retrieved April 4, 2023, from https://hcss.nl/report/chinas-militaire-opkomst-en-europese-technologie/

Thakur, K., Qiu, M., Gai, K., & Ali, L. (2015). *An Investigation on Cyber Security Threats and Security Models*. https://doi.org/10.1109/cscloud.2015.71

Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S., & Lee, M. (2012). Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat. In *Lecture Notes in Computer Science* (pp. 64–85). https://doi.org/10.1007/978-3-642-33338-5_4

Thorleuchter, D., & Van Den Poel, D. (2013). Protecting research and technology from espionage. *Elsevier*, *40*(9), 3432–3440. https://doi.org/10.1016/j.eswa.2012.12.051

Tian, Z., Shi, W., Wang, Y., Zhu, C., Du, X., Su, S., Sun, Y., & Guizani, N. (2019). Real-Time lateral movement Detection based on evidence reasoning network for edge computing environment. *IEEE Transactions on Industrial Informatics*, *15*(7), 4285–4294. https://doi.org/10.1109/tii.2019.2907754

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, *101*, 18–54. https://doi.org/10.1016/j.jnca.2017.10.016

Unger, J. (1996). Bridges: Private Business, the Chinese Government and the Rise of New Associations. *The China Quarterly*, *147*, 795–819. https://doi.org/10.1017/s0305741000051808

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

Van Os, E., & Kole, L. (2020). 5G en het Paard van Troje. In *JSTOR* (No. 44). JSTOR. Retrieved April 4, 2023, from https://www.jstor.org/stable/48600553

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, Y. (2023, March 24). The Problem with TikTok's Claim of Independence from Beijing. *Human Rights Watch*. https://www.hrw.org/news/2023/03/24/problem-tiktoks-claim-independence-beijing

Wangen, G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, *6*(2), 183–211. https://doi.org/10.3390/info6020183

Weston, C., Gandell, T., Beauchamp, J., McAlpine, L., Wiseman, C., & Beauchamp, C. (2001). Analyzing Interview Data: The Development and Evolution of a Coding System. *Qualitative Sociology*, *24*(3), 381–400. https://doi.org/10.1023/a:1010690908200

Willemsen, P. (2023, August 2). *Follow The Money: ook samenwerken met 'gewone' Chinese universiteiten levert risico's op*. HCSS. https://hcss.nl/news/follow-the-money-ook-samenwerken-met-gewone-chinese-universiteiten-levert-risicos-op/

Williams, I. (2022, September 14). How China spies on the West. *The Spectator*. https://www.spectator.co.uk/article/how-china-spies-on-the-west/

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45–55. https://doi.org/10.1057/ejis.2011.51

Yan, Z., Robertson, T. S., Yan, R., Park, S. S., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

Yavuz, M. H. (2021). Erdoğan. In *Edinburgh University Press eBooks*. https://doi.org/10.1515/9781474483278

Yoo, C. S. (2015). Cyber espionage or Cyber war?: International Law, Domestic Law, and Self-Protective Measures. *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2596634

Zapf, A., Castell, S., Morawietz, L., & Karch, A. (2016). Measuring inter-rater reliability for nominal data – which coefficients and confidence intervals are appropriate? *BMC Medical Research Methodology*, *16*(1). https://doi.org/10.1186/s12874-016-0200-9

Annex A

General Question list – subject to changes for specific interviews

Questions espionage Dutch Government

Introduction and interview rules + expectations (Yes/No recording, confidential yes/no.)

RQ1 How does the Dutch government monitor (cyber) espionage within the Dutch industry and educational sector?

1. How does the government monitor/manage certain cyberthreats/espionage threats?
2. What methods can you disclose to us that the government uses to monitor certain cyber espionage?

RQ2 How big does the Dutch government perceive the danger of espionage to be in general, and what are the trends?

1. What is the trend or change in behaviour that you observe recently concerning historic nation state threat actors?
2. Is the Dutch government aware of the dangers of espionage within the Dutch industry?
3. Do organisations report certain cyberthreats towards the government?
4. How does the government research/monitor the trends regarding espionage behaviour?
5. What are the current trends regarding industrial/cybersecurity espionage practices?

RQ3 What are the main challenges for the Dutch government regarding managing national cyberspace against espionage?

1. Is the government currently well equipped to monitor espionage within critical infrastructure/sectors?
2. How does the government assist organisations with combatting espionage?
3. Could you give an estimation of the amount of espionage attempts that you monitor? (Digital or physical attempts)
4. Does the Dutch government help organisation with defending themselves against certain espionage threats?
5. How would you rank the threat of cyber espionage compared to other cyber threats to the Netherlands as a state and to Dutch organisations?

RQ4 What are the recommended practices and procedures for organizations to defend themselves against espionage?

1. Are there standards organisation can use as a baseline of security against espionage specifically?
2. Does the government make organisations within the technological sector aware of the dangers of espionage for the organisation and national interests.

3. How does the Dutch government maintain connection with important organisations after creating the policies these organisations will use?
4. How often does the government create/implement new policies regarding cybersecurity?
5. How do you think NIS2 will help governments to combat cyber espionage threat? And are there other relevant current or upcoming laws and regulations that are relevant here?

Cybersecurity related questions:

1. How many attacks are actively happening daily on average?
2. Does the government make organisation within the technological sector aware of the dangers of espionage for the organisation itself, but also for the Netherlands?
3. Does the Dutch government help organisation with defending themselves against certain espionage threats?
4. How does the Dutch government maintain connection with important organisations after creating the policies these organisations will use?
5. Does the government promote active communication between the organisation and the correct ministry?
6. How often does the government create new policies regarding cybersecurity?
7. How actively is the Dutch government involved with new EU policies like the NIS2?
8. Does the government actively track how successful the policy is they create?
9. Do organisations report certain cyberthreats towards the government?
    a. If yes, what does the government do with this information?

Questions for economic security:

1. Is the Dutch government aware of the dangers of espionage within the Dutch industry?
2. Does the government monitor the amount of espionage attempts in any way?
3. How big do you reckon is the danger of espionage within the technological sector?
4. What are the current trends regarding industrial/cybersecurity espionage practices?
5. What are currently the main challenges for the government regarding managing the national cyberspace against espionage?
6. What kind of challenges does the government face against espionage from a physical perspective? For example, international students/workers?
7. How many of the organisation within the technology sector maintain their security against Economic security (Economische veiligheid)?
    a. Does the government monitor this level?
8. Does the government make organisations within the technological sector aware of the dangers of espionage for the organisation itself, but also for the Netherlands?

9. Does the Dutch government help organisation with defending themselves against certain espionage threats?
10. How does the Dutch government maintain connection with important organisations after creating the policies these organisations will use?
11. Does the government promote active communication between the organisation and the correct ministry?
12. How actively is the Dutch government involved with new EU policies like the NIS2?
13. Does the government actively track how successful the policy is they create?

Annex B

ICA table for coder 2:

Agreement Coefficient:	Krippendorff's c-Alpha-binary				
Legend					
Applied*	Number of times the code has been applied				
Units*	Number of units* the code has been applied				
Total Units*	Total number of units* across all selected documents				
Total Coverage*	% Coverage within the selected documents				
Coders					
	Coder 2				
	T VDV				
ID11 Transcription					
Semantic Domain:	behaviour: geopolitical events behaviour: increasing awareness				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
behaviour : geopolitical events					
	Coder 2	4	248	15681	1,58%
	T VDV	2	515	15681	3,28%
behaviour : increasing awareness					
	Coder 2	6	510	15681	3,25%
	T VDV	3	403	15681	2,57%
			Reliability Coefficient		
				Krippendorff's c-Alpha-binary: 0.733	
Semantic Domain:	communication: sharing threat intel				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
communication:					

sharing threat intel					
	Coder 2	11	949	15681	6,05%
	T VDV	15	2067	15681	13,18%
			Reliability Coefficient		
				Krippendorff's c-Alpha-binary: 0.453	
Semantic Domain:	cyber resilience: integral security cyber resilience: risk management				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
cyber resilience: integral security					
	Coder 2	2	149	15681	0,95%
	T VDV	1	40	15681	0,26%
cyber resilience: risk managem ent					
	Coder 2	3	220	15681	1,40%
	T VDV	1	149	15681	0,95%
			Reliability Coefficient		
				Krippendorff's c-Alpha-binary: 0.642	
Semantic Domain:	educational sector: cyber security				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
educational sector: cyber security					
	Coder 2	1	47	15681	0,30%
	T VDV	1	46	15681	0,29%
			Reliability Coefficient		

				Krippendorff’s c-Alpha-binary: 0.989	
Semantic Domain:	government: confidential government: cooperation government: defined responsibility government: information position government: law or regulation government: public private cooperation government: publications				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
government: confidential					
	Coder 2	1	90	15681	0,57%
	T VDV	2	273	15681	1,74%
government: cooperation					
	Coder 2	6	542	15681	3,46%
	T VDV	11	1582	15681	10,09%
government: defined responsibility					
	Coder 2	5	459	15681	2,93%
	T VDV	8	873	15681	5,57%
government: information position					
	Coder 2	1	75	15681	0,48%
	T VDV	2	254	15681	1,62%
government: law or regulation					
	Coder 2	2	75	15681	0,48%
	T VDV	2	218	15681	1,39%
government: public private cooperation					
	Coder 2	3	293	15681	1,87%
	T VDV	4	556	15681	3,55%
government: publications					
	Coder 2	6	495	15681	3,16%
	T VDV	6	511	15681	3,26%

			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 0.532	
Semantic Domain:	NIS2: positive				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
NIS2: positive					
	Coder 2	1	81	15681	0,52%
	T VDV	1	80	15681	0,51%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 0.994	
Semantic Domain:	organisation: role				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
organisation: role					
	Coder 2	3	120	15681	0,77%
	T VDV	2	53	15681	0,34%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 0.611	
Semantic Domain:	Private sector: responsibility				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
Private sector: responsibility					
	Coder 2	1	193	15681	1,23%
	T VDV	1	191	15681	1,22%
			Reliability Coefficient		

				Krippendorff’s c-Alpha-binary: 0.995	
Semantic Domain:	threats: criminal threats: cyber security threats: economic security threats: espionage threats: hacktivism threats: nation state actors threats: trends threats: triage				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
threats: criminal					
	Coder 2	6	295	15681	1,88%
	T VDV	6	454	15681	2,90%
threats: cyber security					
	Coder 2	5	402	15681	2,56%
	T VDV	3	360	15681	2,30%
threats: economic security					
	Coder 2	2	348	15681	2,22%
	T VDV	1	192	15681	1,22%
threats: espionage					
	Coder 2	2	66	15681	0,42%
	T VDV	2	78	15681	0,50%
threats: hacktivism					
	Coder 2	2	106	15681	0,68%
	T VDV	1	25	15681	0,16%
threats: nation state actors					
	Coder 2	7	576	15681	3,67%
	T VDV	7	1415	15681	9,02%
threats: trends					
	Coder 2	3	416	15681	2,65%
	T VDV	2	416	15681	2,65%
threats: triage					
	Coder 2	4	348	15681	2,22%
	T VDV	3	373	15681	2,38%
			Reliability Coefficient		

				Krippendorff’s c-Alpha-binary: 0.546	
Semantic Domain:	tools: auditing tools: control tools: law and legislation tools: network monitoring tools: threat research				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
tools: auditing					
	Coder 2	1	140	15681	0,89%
	T VDV	1	140	15681	0,89%
tools: control					
	Coder 2	1	76	15681	0,49%
	T VDV	1	76	15681	0,49%
tools: law and legislation					
	Coder 2	1	82	15681	0,52%
	T VDV	1	81	15681	0,52%
tools: network monitorin g					
	Coder 2	7	525	15681	3,35%
	T VDV	6	352	15681	2,25%
tools: threat research					
	Coder 2	7	602	15681	3,84%
	T VDV	10	1398	15681	8,91%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 0.528	
			Total		
				Krippendorff’s c-Alpha-binary: 0.631	

Table 2: Krippendorff's C-Alpha-binary table coder 2.

Annex C

ICA Table for coder 3:

Agreement Coefficient:	Krippendorff’s c-Alpha-binary				
Legend					
Applied*	Number of times the code has been applied				
Units*	Number of units* the code has been applied				
Total Units*	Total number of units* across all selected documents				
Total Coverage*	% Coverage within the selected documents				
Coders					
	coder 3				
	T VDV				
ID3 Transcription					
Semantic Domain:	behaviour: geopolitical events				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
behaviour: geopolitical events					
	coder 3	4	1149	18116	6,34%
	T VDV	2	447	18116	2,47%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 0.540	
Semantic Domain:	communication: sharing threat intel				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
communication: sharing threat intel					
	coder 3	10	2902	18116	16,02%
	T VDV	7	1548	18116	8,55%
			Reliability Coefficient		

				Krippendorff’s c-Alpha-binary: 0.653	
Semantic Domain:	cyber resilience: incident management				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
cyber resilience: incident management					
	coder 3	1	186	18116	1,03%
	T VDV	1	186	18116	1,03%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 1.000	
Semantic Domain:	government: cooperation government: defined responsibility government: political influence government: publications				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
government: cooperation					
	coder 3	15	5425	18116	29,95%
	T VDV	7	2049	18116	11,31%
government: defined responsibility					
	coder 3	8	2724	18116	15,04%
	T VDV	1	249	18116	1,37%
government: political influence					
	coder 3	2	645	18116	3,56%
	T VDV	2	344	18116	1,90%
government: publications					
	coder 3	1	233	18116	1,29%
	T VDV	1	233	18116	1,29%
			Reliability Coefficient		

				Krippendorff’s c-Alpha-binary: 0.425	
Semantic Domain:	NIS2: positive				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
NIS2: positive					
	coder 3	1	383	18116	2,11%
	T VDV	1	383	18116	2,11%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 1.000	
Semantic Domain:	organisation: role				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
organisation: role					
	coder 3	3	62	18116	0,34%
	T VDV	2	64	18116	0,35%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 0.427	
Semantic Domain:	threats: criminal threats: cyber security threats: economic security threats: espionage threats: knowledge security threats: nation state actors threats: national security threats: trends threats: triage				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
threats: criminal					
	coder 3	2	323	18116	1,78%
	T VDV	2	418	18116	2,31%
threats: cyber security					
	coder 3	3	306	18116	1,69%
	T VDV	4	546	18116	3,01%

threats: economic security					
	coder 3	3	485	18116	2,68%
	T VDV	1	141	18116	0,78%
threats: espionage					
	coder 3	7	892	18116	4,92%
	T VDV	1	141	18116	0,78%
threats: knowledge security					
	coder 3	4	1025	18116	5,66%
	T VDV	1	81	18116	0,45%
threats: nation state actors					
	coder 3	3	655	18116	3,62%
	T VDV	3	641	18116	3,54%
threats: national security					
	coder 3	2	341	18116	1,88%
	T VDV	4	606	18116	3,34%
threats: trends					
	coder 3	5	815	18116	4,50%
	T VDV	2	159	18116	0,88%
threats: triage					
	coder 3	3	1922	18116	10,61%
	T VDV	3	1693	18116	9,35%
			Reliability Coefficient		
				Krippendorff's c-Alpha-binary: 0.714	
Semantic Domain:	tools: cyber security tools: knowledge security tools: monitoring tools: security standards tools: threat research				
Code	Coder	Applied*	Units*	Total Units*	Total Coverage*
tools: cyber security					
	coder 3	9	2929	18116	16,17%
	T VDV	5	1390	18116	7,67%

tools: knowledge security					
	coder 3	5	3229	18116	17,82%
	T VDV	1	227	18116	1,25%
tools: monitoring					
	coder 3	12	4784	18116	26,41%
	T VDV	7	2746	18116	15,16%
tools: security standards					
	coder 3	6	1842	18116	10,17%
	T VDV	3	751	18116	4,15%
tools: threat research					
	coder 3	7	1887	18116	10,42%
	T VDV	2	234	18116	1,29%
			Reliability Coefficient		
				Krippendorff’s c-Alpha-binary: 0.636	
			Total		
				Krippendorff’s c-Alpha-binary: 0.722	

Table 3: Krippendorff's C-Alpha-binary table coder 3.

Annex D

Codebook

Code	Gr	Co	Code	Gr	Co
A. Behaviour			**F. NIS2**		
A.1. behaviour: cultural differences	3	2	F.1. NIS2: positive	26	10
A.2. behaviour: geopolitical events	15	8	F.2. NIS2: potential negative	3	2
A.3. behaviour: increasing awareness	33	11	**G. Organisation**		
A.5. behaviour: lack of awareness	25	8	G.1. organisation: department	13	7
B. Communication			G.2. organisation: role	29	11
B.1. communication: business sector	2	2	**H. Private sector**		
B.2. communication: educational sector	11	3	H.1. responsibility	4	2
B.3. communication: sharing threat intel	48	8	**I. Threats**		
C. Cyber resilience			I.1. threats: criminal	21	8
C.1. cyber resilience: incident management	18	10	I.2. threats: cyber security	43	9
C.2. cyber resilience: integral security	19	8	I.3. threats: economic security	29	10
C.3. cyber resilience: preventing hacks	4	3	I.4. threats: espionage	41	11
C.4. cyber resilience: risk management	24	10	I.5. threats: hacktivism	1	1
C.5. cyber resilience: security policy	7	3	I.6. threats: knowledge security	39	10
D. Educational sector			I.7. threats: nation state actors	69	12
D.1. educational sector: academic freedom	13	5	I.8. threats: national security	36	9
D.2. educational sector: cooperation	15	6	I.9. threats: strategic dependencies	5	4
D.3. educational sector: cyber security	3	3	I.10. threats: trends	7	3
D.4. educational sector: ethics and rules	3	3	I.11. threats: triage	11	5
D.5. educational sector: lack of cooperation	1	1	I.12. threats: TTP's	2	2
D.6. educational sector: tensions	1	1	**J. Tools**		
E. Government			J.1. tools: auditing	11	6
E.1. government: confidential	5	3	J.2. tools: control	4	4
E.2. government: cooperation	51	12	J.3. tools: cyber security	45	10
E.3. government: defined responsibility	54	11	J.4. tools: Desk	13	4
E.4. government: information position	8	5	J.5. tools: economic security	20	4
E.5. government: knowledge institutions ties	1	1	J.6. tools: espionage	13	6
E.6. government: lack of mandate	4	3	J.7. tools: knowledge security	24	10
E.7. government: lack of tools	6	3	J.8. tools: law and legislation	31	10
E.8. government: law or regulation	7	4	J.9. tools: monitoring	37	10
E.9. government: policy creation	21	8	J.10. tools: policies	21	9
E.10. government: political influence	28	9	J.11. tools: security standards	35	9
E.11. government: public private cooperation	22	7	J.12. tools: threat research	41	9
E.12. government: publications	18	19			

Table 4: Codebook with grounding and coverage.
Gr = Groundedness (amount of times the code has been used in total)
Co = Coverage (the number of participants mentioning the code)