The Endeavour to Control National Cyber Security Interests

An exploration of Strategic Autonomy in a Dutch Cyber Security Context

Leiden University – Faculty of Governance & Global Affairs

Program: Crisis and Security Management, MSc

Author: Robbin Begeer

Student No. 2106221

Date of admission: 08-06-2019

Word Count: 21.366 words (excl. bibliography, footnotes and annexes)

Thesis Supervisor: Dr. T. van Steen

It has been a true endeavour indeed. First and foremost, thank you very much, Liesbeth. For I would not have been able to do this research without your knowledgeable insights and your help in finding the right persons for my interviews. Also, thank you, Sergei, for having an inspirational cup of coffee and helping me out. I would like to thank all interviewees, who have cleared their busy schedules for the sake of science.

Special gratitude goes to dr. Tommy van Steen for taking over supervision and supporting me in finishing this thesis.

Autonomy

‘we aim at it because we want it and because we know that other people want it’

Castoriadis

Table of Contents

List of Abbreviations

ABDO	Algemene Beveiligingseisen Defensie Opdrachten General Security Requirements for Defence Contracts
BZ	Buitenlandse Zaken (Ministerie van) Foreign Affairs (Ministry of)
CERT	Computer Emergency Response Team
ENISA	European Union's Agency for Network and Information Security
EU	European Union
EZ	Economische Zaken (Ministerie van) Economic Affairs (Ministry of)
ICT	Information and Communication Technology
IT	Information Technology
NATO	North Atlantic Treaty Organisation
NCSC	National Cyber Security Centre
NCSRA	National Cyber Security Research Agenda
NCTV	Nationaal Coördinator voor Terrorismebestrijding en Veiligheid National Coordinator for Security and Counterterrorism
NDN	National Detection Network
PESCO	Permanent Structured Cooperation
SCSA	Strategic Cyber Security Autonomy

Abstract

This thesis analysed how prominent experts view strategic autonomy in the context of cyber security in The Netherlands. To answer this question, in-depth interviews with public and private security experts were conducted regarding national cyber security strategy and, more specifically, the takeover of Fox-IT by the NCC Group. After analysing relevant data, the results revolved around four categories: the ability to (1) build cyber security capacity & capabilities, (2) manage cooperation, (3) control national cyber security interests, which were all inherently limited by (4) influencing factors. From a strategic autonomy perspective, this study emphasises some important limitations to the country's self-sufficiency and self-rule towards cyber security. At the same time, it has provided relevant insights about how vital interests can be managed and controlled through strategic partnerships and regulation, as well as how an acceptable level of control can be identified through a risk management rationale.

1. Introduction

During the last decades, society has changed in unimaginable ways. Especially, the rise of electronic communication technologies has had an enormous impact. Besides our physical reality, a world of cyberspace has emerged around us. By now, our daily lives have become dependent upon this new cyber reality. From financial transaction, to power grids and transportation, most vital societal functions are becoming more and more digitalised and are connected to the internet. Although the vast digitalisation is responsible for large-scale innovation and other positive effects on society, it does not only come with a bright side. Fundamental issues related to public values started to arise as our lives become more intertwined with the digital reality (CSR, 2018; NCTV, 2018). Just like the physical world, cyberspace is a place in which human rights and public values need to be secured.

Consequently, over the past few years, governments increasingly picked up a more prominent role in cyber security. However, unlike other more traditional security issues wherein governments hold a so-called monopoly on violence, cyber security is unique in a way that it has not been a government responsibility from the start. Best reflection of this increased role can be seen when analysing the evolution of data protection laws. While the European Union's data protection act of 1998 described cyber security for public and private organisations as good practice, under the new General Data Protection Regulation (GDPR), security measures are a legal requirement – the GDPR's 'security principle' (ICO, 2018).

While the governments influence has increased, it can be noticed that cyberspace is governed in a different way compared to traditional security domains. Quickly, cyberspace became largely owned by private actors. Although cyberspace largely functions independently from governments, the way in which products, norms and common practices are created, has a great impact on government processes and even on international peace and security (Klimburg & Faesen, 2018).

Growing concerns about security of cyberspace and increased demand towards the government to protect fundamental values, has led states to formulate cyber security strategies. On European Union level, all member states have formulated such a National Cyber Security Strategy (NCSS) as required by the NIS Directive (ENISA, 2016). Moreover, cyber security is now part of most military doctrines and multiple countries are now openly – or covertly – developing offensive cyber capabilities. However, there are fundamental differences between traditional national security strategies and cyber security strategies. First, as mentioned earlier, private sector and civil society play a much greater role in the actual implementation of cyber security strategies. This created the need for new ways of governance – such as the multi-stakeholder models – whereas a traditional government-centric models were unable to cope with the interdependent and complex reality of cyberspace (Hofmann, 2016). Hence, cyber security is intertwined in every aspect of our society and requires a comprehensive approach, involving national and international public-private cooperation, as well as extensive information sharing. In the Netherlands, there has been a call for more investments in cyber security and digital resilience. More specifically, investments in better information sharing capabilities, both for the critical and non-critical sectors, are said to be required (Kamp, 2017).

Moreover, national cyber security concerns are not about protecting borders but about protecting values (CSR, 2018). This presents a challenge for government, private sector and society in general. In cyberspace, national borders have become irrelevant and the distinction between state and non-state actors have become blurred. Hence, most traditional – often state centric – governance models have become obsolete. Cyber security requires close cooperation between various actors, both on national and international level, to develop adequate policies, laws and technologies to effectively protect societal values. However, this need for cooperation has also introduced issues regarding dependency and interdependency. For example, for the development of cyber technology, the European Union – and consequently The Netherlands – is largely dependent upon the United States. This does not

only have an effect in financial-economic terms, it decreases the freedom of action and decision on strategical level (Holslag, 2017). Moreover, a great deal of the Dutch digital infrastructure is owned by large global or foreign companies. Although these companies often have better resources to protect their services and products, this is at odds with the desire to be an autonomous state (CSR, 2018). This raises fundamental questions about the degree of dependence on both the private sector and other states in terms of cyber security.

1.1. Research question and objective

Recently, due to the growing importance and impact of cyberspace on society, it has become common practice to view cyber security knowledge and technology as national or supranational (European Union) security interest. As Timmers (2018) puts it:

> '"Cyber" has become *a critical disruptor* [emphasis added] for the economy, society as well as the internal and external governance of states. However, it is also *a key force* [emphasis added] in defending these, and, more generally, mastery of digital technologies is an essential capability for future competitiveness [and] to protect society's values […]'

With cyber being both a threat to and a key force in defending society, it is of importance to gain more insight into the ability of states to act upon or make their own decisions on cyber security interest. How does the idea of autonomy play out in the anarchic global cyberspace, where interconnectivity creates interdependence and where cooperation and knowledge sharing seem to be the best defence? What balance is sought between dependence and independence in cyber interests? Although not much has been written about this relatively novel subject, it can be expected that prominent cyber security experts already possess (practical) knowledge about the way these dilemmas are dealt with. Therefore, the main research question that will be attempted to answer is: **'How do prominent security experts view strategic autonomy in Dutch cyber security policy?'**

First and foremost, this research aims to create a better understanding of the concept of strategic autonomy in the governance of cyber security. It will create a first step towards developing an academic understanding of Strategic Cyber Security Autonomy (SCSA) that will be helpful in explaining the national context but also within the European Union, of which The Netherlands is a member state. Furthermore, the second part of this study will explain how the characteristics of strategic autonomy materialise in empirical reality. The role of the concept will be analysed in the context of foreign ownership of important cyber

security organisations. Hence, the main research question will be divided into two sub-questions:

- How do security experts characterise SCSA in The Netherlands?
- To what extend has SCSA played a role in the takeover of a Dutch government contracted cyber security firm by a foreign actor?

1.2. Social Relevance

Due to its novelty, cyber is largely uncharted terrain, especially in the area of international relations. Although some attempts have been made to develop global norms in cyberspace – the most prominent example being the Tallinn manual 2.0 – global cyberspace remains rather anarchic and governed without any clear norms and rules in practice. As a result, many cases have shown that governments are willing to act in a controversial and provocative fashion in cyberspace. Whether this is through their own agencies or through their proxies. Recently, a group of Russian operatives were arrested in The Netherlands after attempting to launch a hacking operation against the OPCW in The Hague ('MIVD verstoort Russische cyberoperatie', 2018). Earlier, it was revealed that the United Kingdom's Government Communications Headquarter (GCHQ) infiltrated one of Belgium's largest telecom providers Belgacom, allowing them to exploit the firm's infrastructure (Britain's GCHQ Hacked Belgian Telecom Firm, 2013). This shows that institutions and national infrastructure are constantly being targeted through cyber operations by foreign nations, ranging from espionage to offensive sabotage, often undermining the target state's sovereignty.

Although espionage, sabotage and other ways of state interference are not new, the use of cyberspace has changed the dynamics and scale of the phenomena. Under the cloak of anonymity, with its relative low risk of being caught and thus relatively low political or diplomatic cost – compared to traditional warfighting and espionage capabilities – cyber operations can be deployed on a low-threshold with relative ease and speed. (Nye, 2010).

Be that as it may, to successfully carry out cyber operations or to defend against them, states must have the right capabilities and capacity, both in technical and organisational terms. Especially when it comes to technical knowledge and skills, governments often need to rely on private organisations to strengthen their capabilities. Governments have naturally been warried of outsourcing topics regarding national security. Therefore, the characteristics of the cyber domain presents challenges for public actors when it comes to securing society, as they often must rely on the private sector.

Moreover, state actors might try to interfere with other states' affairs through private companies. In the National Defence Authorisation Act for Fiscal Year 2018 (2017) United States Congress outlawed the use of all Kaspersky Lab software from civilian agencies and military networks. The anti-virus software developer was suspected to have ties with the Russian intelligence agency and was banned for concerns over (cyber) espionage. Similar concerns were voiced in amongst members of the European Union, where the European Parliament adopted a resolution calling upon the EU to 'ban the ones [programmes] that have been confirmed as malicious, such as Kaspersky Lab' (European Parliament, 2018, p.19). Accordingly, on national level, Dutch government stopped using Kaspersky Lab software and advised private critical suppliers to do the same (Nationaal Cyber Security Centrum, 2018)

The case of Kaspersky could be viewed as an example of broader moves on supranational and national level towards tighter control over government IT equipment and software supply chains. In 2013 América Movil, a company owned by Mexican billionaire Carlos Slim, tried to acquire The Netherlands' largest telecom provider KPN. Even though an independent – not government owned – foundation blocked the takeover ('Stichting beschermt KPN', 2013), the attempt by Movil led to questions in parliament whether the government should be better able to protect vital infrastructure and other IT related interests (Schellevis, 2013).

Although the issue has been on the political radar, it introduced a delicate dilemma between security on the one hand and free market values on the other. At the time of writing various countries are weighing the benefits against risks of using Huawei equipment in the development of 5G networks. Like in the case of Kaspersky, many voiced concerns over potential state interference and espionage towards Huawei, a large private Chinese based IT manufacturer (Kaska, Beckvard & Mináik, 2019).

Consequently, this and other increased cyber threats towards the Netherlands have no gone unnoticed. In collaboration with other actors, the National Coordinator for Security and Counterterrorism reported increasing risks when it comes to cyber espionage and attacks led by state actors (NCTV, 2018). Moreover, The Dutch Cyber Security Council (CSR), the main advisory body to the Dutch House of Representatives, has called upon the government to pay better attention to issues concerning the country's dependence, as well as the protection of public values when it comes to cyber security. By doing so, they have raised the questions to what extend The Netherlands wishes to be dependent upon other countries or large private firms for their own cyber security (CSR, 2018).

1.3. Academic Relevance

Autonomy is a widely used and broad concept. Depending of the level of analysis and field of research, autonomy can have different meanings. Within highly technical fields, for example, autonomy could refer to systems that can make decisions without the interference of humans, such as artificial intelligence (AI). From a philosophical perspective, autonomy might refer to an individual's capability to live autonomous and make its own decisions. Although autonomy has been a well-studied concept in other fields of research, such as in health care and moral philosophy, the concept has yet to receive attention from Security scholars. Most of the scholarly work, if not all, focus on strategic autonomy in the context of European defence and Transatlantic Cooperation (Biscop, 2016; Howorth 2017; Howorth, 2018; Drent, 2018). They primarily discuss European Union's (in)dependence from NATO or other third-party countries. Especially European Union's relation to the United States has been a topic of interest. Moreover, the works are often limited to traditional military capacity and decision-making.

Although EU-NATO discussion is a relevant one, implications of strategic autonomy may play out on more levels (national, supranational and global) and within various security domains. Looking at autonomy through a governance and security lens introduces themes, such as freedom, independence and sovereignty. Themes that have influenced state, regional and global security for years. As the Westphalian state system still represents the cornerstones of our modern society, autonomy is often seen as a mean to ensure state or regional sovereignty. Even so, the degree of autonomy, or the degree to which an actor wishes to be autonomous, may vary considerably (Osiander, 2001). Whereas it might be obvious that states seek autonomy over their nuclear weapons arsenal and scientific nuclear developments, within other fields of security, the desired degree of autonomy may be more ambiguous. This might especially be complex in the interconnected world of cyberspace. Here, interdependence and cooperation play a big role in both defensive and offensive capabilities. At the same time, cyber security is increasingly being considered vital to national and international security.

Therefore, to better understand strategic autonomy in the context of security, it is important to analyse its implications both on multiple governance levels (national and supranational) and within various security themes (conventional military, intelligence, cyber, nuclear, etc.). By analysing autonomy and related themes, such as independence, on a national level (the

Netherlands), this study will be relevant in two ways. First, as no real attempt has been made so far to conceptualise and define strategic autonomy[1], this research seeks to provide new insights into the dynamics of strategic autonomy within Dutch cyber security policy. Second, a Dutch perspective on the ideas related to autonomy in cyber could help initiate development of more general understanding of the concept and explain how it influences international and national cyber security governance. Since the Netherlands is a member of the European Union, the insights that are gained throughout this research might prove valuable in the existing debates about European strategic autonomy and its implications.

[1] As it is a highly politicised concept (Drent, 2018), strategic autonomy lacks a clear definition, especially regarding the cyber security realm. Some French efforts have been made to better conceptualise strategic autonomy (Kempin & Kunz, 2017; Drent, 2018). Also, Mauro's (2018) has attempted to integrate the literature into a more comprehensive definition. However, more work needs to be done in order to create a true theoretical concept.

2. Theory

Despite the explorative nature of this research, some important insights can be derived from existing literature. Providing this theoretical lens will help guide the study. In this chapter, an outline of relevant literature and theoretical ideas are presented. First, the meaning of autonomy in various academic fields is outlined. Second, an international relations perspective on the concept is illustrated. Third, the emergence of strategic autonomy thinking in security is described. Lastly, a preliminary idea about the notion of Strategic Autonomy will be provided at the end of the chapter, which will serve as guideline for this study, by providing a general sense of Strategic Cyber Security Autonomy.

2.1. The concept of Autonomy: a (very brief) introduction

The concept of autonomy has featured in many fields of research for over decades. Even so, up until today, it is covered in ambiguity. Although it does not fit the scope of this research to elaborate on the extensive history of autonomy, it is important to consider a short (historical) overview of how the concept emerged in academic fields, such as political and moral philosophy. It will help to better understand how notions of the concept emerged within International Relations and the political debate, which will be discussed later in this chapter.

Looking at the etymology of autonomy, it can be traced back to the early 17th century words *autonomous* and *autonomia*, contractions of Greek words *autos* 'self' and *nomos* 'law'(Autonomy, 2019.). Understandably, a broad concept leaves room for interpretation. Therefore, it is not surprising that autonomy became a concept of interest for prominent moral and political philosophers. Whereas Kant – and other scholars – focussed on personal level autonomy, the nature of autonomy is applicable to social and political spheres as well. For instance, it has been argued that Kant's interpretation of autonomy is closely associated to the concept of political freedom (Reath, as cited in Johnson & Cureton, 2019). This means that a free state can only be created when citizens are bound by 'laws that are in some sense of their own making' (Johnson & Cureton, 2019). Consequently, this means that a state is autonomous when it is governed by laws that reflect the free will of the people living in that state, rather than laws or decisions from people external to that state. This is opposed to heteronomy, in which the will of an agent is 'under the control of another' (Autonomy/heteronomy, nd).

Although Kant's view on autonomy has been influential, it presents only one interpretation of the concept. Autonomy has been broadly used by many authors. Over the years, the concept

has been related to freedom and liberty, or as an equivalent to sovereignty and self-rule. Also, self-reflection, self-knowledge and awareness of one's own interest and qualities, such as independence and responsibility have all been identified with autonomy (Dworkin, 1988). Thus, it could be derived from its broad use that autonomy cannot be comprehended in a single definition. As mentioned by Dworkin (1988, p. 7) it is rather 'a term of art introduced by a theorist in an attempt to make sense of a tangled net of intuitions, conceptual and empirical issues, and normative claims.' Therefore, this study will adapt the idea that 'a theory of autonomy is simply a construction of a concept aimed at capturing the general sense of "self-rule" or "self-government"' (Christman, 2018) This is an important preposition for the remainder of this research.

However, if we were to theoretically understand autonomy in cyber security strategy and governance context, it is important to study what role autonomy plays in that specific context. To do so, first, it is necessary narrow the scope of the concept to the field of Politics and International Relations.

2.2. Autonomy in International Relations: The struggle for autonomy

One of the longest standing, but also heavily contested theories in International Relations (IR) is Realism. States, often referred to as units within a network, and their behaviour have been central objects in Realist studies (Donnelly, 2000). Early Realists have sought to explain state behaviour through unit motivation, by focussing on characteristics, such as the structure of anarchy in the international sphere, inherent human egoism, the need of self-preservation, fear of unequal distributions of gains, etcetera. Consequently, within the international sphere, units are involved in what Morgenthau (as cited in Harknete & Yalcin, 2012) calls 'the struggle for power'. Especially in the field of international security, Realist ideas have remained very influential up until today (Chatierjee, 2003).

Still, Realist theories have been heavily criticised amongst scholars. Neo-liberal, Constructivist and Post-Positivist scholars often voiced critique on Realists' narrow view. Realist Theories' explanatory value was, amongst others, doubted by Harknett & Yalcin (2012) because of its internal inconsistencies. However, while most criticism argue for full rejection of the Realist interpretations, Harknett & Yalcin (2012) have attempted to revisit and amend the Realist theories by introducing the concept of autonomy. They argue that 'Rather than a struggle over power, international politics is best understood, more purely, as a *struggle for autonomy*' (Harknett & Yalcin, 2012, p. 506). Here, autonomy is defined as:

‘[The] possession of the wherewithal for the organized capacity to act in a sustained fashion globally’ (Harknett & Yalcin, 2012, p. 506). In this perspective, autonomy revolves around an actor’s capabilities and the distribution of capabilities across the international system. Reason for units to seek autonomy is viewed as a structural generated necessity, rather than a motivation originating from within units. This necessity is based on the absence of a central authority – or anarchy – combined with dissimilarities in capacities amongst states – the distribution of power – in the international system. Hence, Harknett & Yaltcin (2012) suggest that in anarchic systems, units primarily rely on their own capabilities to govern their affairs. In pursuit of this fundamental motivation, States react to situations that may challenge their autonomy, or could potentially increase their autonomy by reposition their goals and strategy in line with their capabilities. Thus, the classic realist pursuit of power or security maximisation argument is in fact one of many strategic options a unit can choose from. Concludingly, States are primarily self-reliant units, motivated to promote their national autonomy and deny delegation of their autonomy to some other authority.

Another important note in the work of Harknett & Yalcin (2012) can be derived from their explanation of autonomy as a struggle. Although units are motivated to seek autonomy, the lack of concentration of power in the international system prevents a State from becoming fully autonomous. Therefore, the pursuit of autonomy is ‘in its purest sense an unattainable, but structurally necessary goal’ (Harknett & Yalcin, 2012, p. 510). Applied to the networked and interdependent world of cyberspace, States could choose to deploy cyber security strategies aimed at increasing their autonomy, but they will not be able to attain full autonomy. Hence, autonomy is not an all-or-nothing concept. Whereas absolute autonomy is theoretically an unattainable goal, relative autonomy can better explain strategic choices and actions of state actors. This study will take inspiration from this approach in explaining how autonomy of cyber security can be explained.

2.3. The emergence of Strategic Autonomy in security and defence policy

Due to rising global tensions, shifts in the international sphere and with an increasing amount of threats manifesting itself, EU’s defence and security policy and ambitions have seen a surge in interest over the last couple of years. Initial ideas about the EU being able to independently carry out military action were born during the UK-French St. Malo summit of 1998 (Mauro, 2018). As a result, the European Common Security and Defence policy (CSDP) was drafted, but it was the EU Global Strategy (European External Action Service,

2016) that extended their ambition of autonomous action to the more encompassing ambition of Strategic Autonomy.

The growing desire of the EU to take defence and security in their own hands was criticised by key NATO ally the United States, who voiced concerns over the risks it would impose in relation to the transatlantic alliance. Later, after being brought to a relative standstill, EU's defence and security ambitions became revitalised when the role of the US as backbone of European security was questioned by the Trump administration (Drent,2018).

Despite its history, the notion of Strategic Autonomy has been covered in ambiguity. Few attempts have been made to explain what strategic autonomy entails. Amongst the first attempts to conceptualise the notion was the report on the 'external security of France against new strategic challenges' (2000). Two principles of strategic autonomy were mentioned: the ability to rapidly gather (sensitive) data and information without any dependence, and the ability to deploy certain operational capabilities, in terms of last resort action – such as war – and in normal circumstances (Institut Montaigne as cited in Mauro, 2018). These principles were later incorporated into the French White Paper on defence and national security, which related strategic autonomy to three freedoms: freedom of assessment, freedom of decision and freedom of action (Ministry of the Armed Forces, 2017).

Later, introduced by French Institution for International Relations (IFRI), the concept became generally divided into three dimensions: Political, industrial and operational autonomy (Kempin & Kunz, 2017). This inspired later ideas about the notion of Strategic Autonomy, such as the ones by Dr. Paul Timmers, a research fellow at Oxford University. He defined strategic autonomy as: 'the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one's longer-term future in the economy, society and their institutions' (Timmers, 2018). Contrary to this broad definition, Mauro (2018) argued for a narrower definition. He argued for the necessity to confine the notion to military spheres only, to prevent conceptual confusion with the notion of independence. May that be a valid reason, limiting the definition of strategic autonomy to military spheres in the context of cyber security might be problematic. Due to the complex characteristics of cyberspace, it becomes difficult to provide a clear distinction between military and (national) security matters, as will be further discussed in the next section.

2.4. A new concept: Strategic Cyber Security Autonomy

For this research, it is crucial to evaluate how adding the prefix ‘cyber’ influences the concept of strategic autonomy. Until now, no research has been done on ideas of strategic autonomy in the context of cyber security. Cyber security in relation to national security has, however, increasingly appeared on research agendas over the last decade. As a broad concept, cyber security can be defined as: ‘the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, action 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, p. 97) This cyber environment is commonly referred to as cyberspace. Thus, cyberspace can be defined by ‘the interdependent network of information technology structures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries’ (The White House, 2008)

As the use of the world wide web rapidly expanded, societies now largely depend upon cyberspace and its underlying ICT infrastructures. Whereas this ICT might be utilised to make our lives easier, the same technology can be used for harmful purposes too. Vital infrastructure can be attacked or disrupted and classified information or intellectual property can be stolen. Therefore, today, cyber security has a prominent place in national security and critical infrastructure protection strategies of most countries (von Solms & van Niekerk, 2013). Also, within Dutch government, cyber security has taken a more prominent position in national security matter.

Most IT infrastructure is owned by the private sector and national borders in cyberspace are blurred. Even so, territorial governments and their system of rule law still hold a massive role in the control over the internet and how it is governed (Goldsmith & Wu, 2006). Consequently, as cyber security has become increasingly important in national security affairs, Timmer (2018) argues ‘There is no doubt that cybersecurity threats undermine strategic autonomy’. Be that as it may, it might do so in a unique way. Characteristics of ‘cyber’ and the internet are different from ‘traditional’ security matters. As suggested by Knoops (2010) the internet is inherently transborder, immediate and exists on a digital level. This presents unique opportunities for criminals, but also state or state sponsored actors, to commit crimes and to carry out cyber attacks. Unlike more ‘traditional’ attacks, cyber attacks can be carried out at a relative low threshold. They only require technical infrastructure and

qualified people to instigate them (NCTV, 2018). Moreover, depending on the attack method, it can remain undetected for months. When discovered, however, attribution is problematic, as perpetrators can hide their real identity and location (NCTV, 2018). Lastly, cyberspace landscape is largely owned and governed by private companies, in contrast to more physical domains. Thus, public-private partnership as often considered the corner stone to protect national security interest in cyberspace (NCTV, 2018).

From a military perspective, the mentioned characteristics of cyberspace presents unique opportunities and challenges for a country's defence. Most importantly, the cyber domain is manmade and volatile. Technology changes rapidly and cyberspace has a much more dynamic character than any other environment (Nye, 2010). Operations carry relatively low cost, as 'It is cheaper and quicker to move electrons across the globe than to move large ships long distance through the friction of salt water' (Nye, 2010, p. 4). Also, due to the constant development of technology, new vulnerabilities are created every day, which can be exploited by state and non-state actors. As a result, also cyber defence carries different characteristics compared to defence in the traditional physical domains.

Due to the relevance of cyber security, many governments have started to cultivate better cyber security capacity. According to a report by the Global Cyber Security Capacity Centre (2016), capacity building usually has five important dimensions: (1) Cyber security policy and strategy, (2) cyber culture and society, (3) cybersecurity education, training and skills, (4) legal and regulatory framework, and (5) standards, organisations and technologies. Hence, capacities include a government's ability to devise and implement cyber security strategy, to cultivate civil awareness, to develop cyber security knowledge, to create national legislation and regulation and to manage risks through standards.

When discussing cyber capacity in military terms, a division between offensive and defensive capacities is commonly made. According to the cyber strategy of the Dutch Ministry of Defence (2018), the latter includes intelligence to develop defensive measures and early detection methods to identify cyber espionage or sabotage, whereas the former relates to (military) action and their ability to disrupt urgent digital threats. Adjacent to cyber capacity, Nye (2010, p. 3) presents the notion of cyber power: 'the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyber domain'. Although power based on information is an older concept, cyber power is new. In the current information age, things often happen outside the control of states. Hence, unlike

traditional domains of (military) power, such as sea and air, dominance in cyberspace is highly unlikely due to its complexity and dynamics. In the realm of cyber, power and capacities seem to be diffused rather than concentrated (Nye, 2010).

Due to its global reach and extensive involvement of the private sector, cyberspace lacks clear borders. Traditional divisions, such as public-private, national-international or civil-military, become blurred and intertwined. Based on these premises and by linking them to previously mentioned knowledge about strategic autonomy in national security, a working definition of what strategic autonomy in the cyber security realm entails is drafted:

> *Strategic Cyber Security Autonomy (SCSA) is defined as a state's capability and capacity to decide and act upon both cyber defence and national cyber security interests in a sustainable way.*

Combining the various thoughts and writings on strategic autonomy and cyber security, leads to a preliminary idea about what the concept entails. As various ideas overlap each other, some main features can be pointed out. Essentially, it is about the self-governance in terms of assessment, decision and action, within the three spheres of cyber security: political, operational and industrial. As described throughout this chapter, characteristics of cyberspace introduce new challenges and opportunities. How this exactly influence strategic autonomy will be discussed in the remainder of this study.

3. Methodology

As this research aims to gain insight in the concept of strategic autonomy in the context of cyber security, the study will be designed through an inductive approach with an explorative goal in mind. In this chapter, the research design will be described and justified. Covered themes are the type of research design, case selection, the assessment of key concepts, the way in which data is collected, methods of data analysis and the assessment of potential validity issues, as well as how these will be addressed.

3.1. Research Design

To begin with, this study has been designed trough a theoretical post-positivist perspective, focussing on the interpretivist premises that the world exists of interpretations, rather than certainties (Grey, 2014). Following this logic, great value lies in how people interpret the world. Therefore, the study has been able to primarily focus on expert opinions and their experiences in cyber security (policy). As no empirical observations or studies had yet been conducted regarding strategic autonomy within the context of cyberspace, this study adopted an inductive approach. A deductive approach would not have been suitable, as it requires extensive pre-existing knowledge and theories that can be tested against empirical reality. Instead, using an inductive approach, empirical data was collected, after which it was analysed to find out whether categories, consistencies or inconsistencies emerged from the data (Grey, 2014). Conclusions were then drawn from these patterns to aid in creating better understanding of what strategic autonomy within cyber security entails. However, as generating a solid theory is far beyond the scope of this research, it should be regarded as a first step in contributing to a theory that can be validated through future empirical research.

Although the design focussed on drawing conclusions from the data, it did not completely disregard pre-existing ideas and theories. To help guide the research and explain the relevance of studying the concept in the context of cyber security, ideas about autonomy in various fields of science, as well as knowledge on the relatively new field of cyber security were covered as well. However, it is important to notice that this research was not set out to either falsify or corroborate theory, as explained earlier. Instead, grounded theory methodology was used to find an answer to the main research question. Grounded theory is a flexible, modifiable and open methodology that prompts discovery and development of theoretical ideas through the analysis of qualitative data (Corbin & Strauss, 2008). As data collection and data analysis happened simultaneously, new insights could be followed up

during the research period. Consequently, the research focus developed over time, starting with a more general inquiry based on indicators related to strategic autonomy and cyber security, towards a more specified case derived from experts' answers.

3.2. Case selection

Since strategic autonomy has mainly been discussed on the level of EU-NATO partnership, the study has taken inspiration from this prior knowledge. Some more general conceptualisations from working papers were used to guide the questions. However, in contrast to previous conceptualisation attempts, shifting the focus towards the Netherlands allowed for analysis of the concept on a national level, rather than supra-national level.

The Netherlands is one of the most important cyber hubs of Europe (i.e. Amsterdam Internet Exchange), with one of the best digital infrastructures of the world (Keijzer, Knops & Grapperhaus, 2018). Recognising that having a strong infrastructure provides opportunities, Dutch cabinet has announced their ambition to make The Netherlands the leading country of Europe in terms of digitalisation (Keijzer, Knops & Grapperhaus, 2018). Simultaneously, Dutch society has become highly digitalised. In 2017, 97% of the population had access to the internet and 86% of the population are believed to use the internet every day (CBS, 2018). However, no opportunity comes without risks. In this technology dependent society, impact of cyber threats carries high potential for social unrest or even disruption, both within and outside national borders. As digital developments put fundamental public values at stake, cyber security has become crucial in maintaining social stability. For these reasons, The Netherlands proves to be a relevant case for researching concepts of strategic autonomy and related themes such as freedom and independence within cyber security.

Moreover, to provide more detailed insights, a recent foreign takeover of Dutch cyber security firm Fox-IT and the implications for the government contracts were analysed. During the first interview round, several interviewees identified this takeover as a relevant case. Although other relevant cases were also mentioned, such as the attempted takeover of Dutch telecom company KPN, the termination of Kaspersky security products by the government and the discussion about risks related to Huawei's involvement in the development of 5G, this specific case was selected for two reasons. First, sufficient time has passed, since the Fox-IT takeover took place in 2015. This allowed a meaningful analysis to be carried out, whereas the Huawei discussion is still in full swing and the KPN takeover attempt is relatively outdated. Second, as Fox-IT HQ is located in The Netherlands, the

researcher was able to access key individuals who were involved in the takeover case. In contrast, this would have been difficult when compare to Kaspersky, as this is a Russian based firm. By examining the Fox-IT case in more detail through two additional interviews, the more general results could be complemented and strengthened.

3.3. Single case study

Not only has limiting the scope to The Netherlands led to insights on the national level, studying a single case has allowed for richer qualitative data to be acquired. Compared to a large 'n' or comparative study, a single case study allowed for multiple aspects and dimensions to be analysed, through which more in-depth data could be gathered. This qualitative data is especially valuable for the inductive creation of new knowledge, which is in line with the goal of this study. Although critics of the method have disregarded it as being interpretative and subjective, it is exactly this subjectivity that allows generating multiple explanations and new conceptualisations (Gerring, 2006). Regarding the timeframe, all data was collected at one point in time through a cross-sectional approach. As cyber security is a rapidly developing theme, the study focussed on collecting the most recent and up-to-date data. Even though longitudal analysis would theoretically have provided better reliability to the outcomes, because of limitations in the study's timeframe and budget, as well as potential validity issues caused by the use of historic data due to the fast-changing context, a cross-sectional approach was considered best suitable.

3.4. Methods of data collection

To collect the data, a semi-structured interview method was used, which has several advantages. As the concepts of interest are complex, relatively new and ambiguous, it could be argued that semi-structured interview provides the best balance between flexibility and structure (Gillham, 2005a). First, it allows for questions guided by pre-existing knowledge to be brought in. Second, it creates a possibility for new themes to emerge and for follow up questions to be asked. Both functions are considered important, as alignment with pre-existing knowledge enhances validity, while the open characteristic prevented the results from becoming unnecessary biased by this knowledge. Although, in terms of replication, the method is not as solid as a fully structured interview is. However, a fully structured interview would be a less ideal, since senior officials will form the main category of respondents. Hence, this so-called 'elite interviews', involve knowledgeable interviewees that will not easily submit to pre-structured questionnaires (Gillham, 2005b).

Eight expert or elite interviews were held from November 2018 till May 2019. The expert pool consisted of high placed officials, both within the public and private sector. Considered the study's focus on public cyber security policy, a slight emphasis was placed on government officials while selecting the interviewees. However, as the private sector is vital in cyber security, three representatives have been included as well. Amongst the public sector interviewees were government officials tasked with cyber security policy, representing the Ministry of Justice and Security, the Ministry of Defence, the Ministry of Economic Affairs and the Ministry of Foreign Affairs. In addition, the private sector was represented by the an official of the Confederation of Netherlands Industry and Employers (VNO-NCW), as well as by a cyber security expert from global consultancy firm Deloitte. Regarding the Fox-IT case, two insiders of the takeover process were interviewed. Both the contractor and supplier were included, respectively a Ministry of Defence official who was tasked with handling the case, and Fox-It's Chief Research Officer.

The selection of the experts was possible through accessing the researcher's personal professional network. In addition, a snowball sampling method was used to select more research subjects. This sampling method, which relies upon research subjects providing the researcher with other names of persons of interest, had some advantages (Atkinson & Flint, 2011). As the cyber security (policy) community consists of a relatively small and hard-to-find group of specialists, taking advantages of interviewees' social networks is a useful way to identifying new interviewees. Moreover, using this method, the selected research subjects could be cross-checked by each other. This verified the relevance and completeness of the collected data.

3.5. Assessment of key concepts

To shape the interview questions, various documents about the meaning of autonomy in a general sense, the strategic component and cyber security were reviewed. The literature review served as a method of conceptualisation and contextualisation. Prior to the interviews, key features were identified, and a working definition was drafted. This involved incorporating the various proposed perspectives: IM's freedom of assessment, decision and action, as well as IFRI's political, industrial and operational autonomy. In addition, various related features of autonomy, such self-rule and self-reliance, were synthesised with characteristics of cyber security and cyber defence, creating an interpretive framework that illuminated some important components. Guided by this knowledge, interview questions

were drafted. However, with the research being primarily data driven, answers to open-ended and follow-up interview questions were leading in the assessment of concepts.

3.6. Methods of data analysis

To interpret the collected data, an inductive data analysis process was used. This qualitative data analysis process and the collection phase of the project happened simultaneously. To document the data awaited by the interviews, texts were transcribed using audio records. The transcripts were then used in the iterative process of coding, categorising and conceptualising the data. This process consisted of a continuous cycle of collecting data and interacting with the data. Newly discovered themes and cases were used to create new insights and to redirect and specify the data collection process. After various rounds, all data was organised using emergent codes and categorised into more abstract concepts. Data and categories were re-examined and redefined several times to better reflect respondents' answers.

3.7. Limitations and how they are addressed

All research projects have limitations and so does this study. Therefore, it is important to address potential reliability and validity issues. First, due to the small sample size of the expert interviews, the results of the study may have low external validity. Not only the sample size but also the sampling technique might pose an issue related to validity. Although regarded as an acceptable technique amongst most qualitative researchers, the use of snowball sampling inherits a risk of sampling bias. It may cause potential exclusion of research subjects that are not part of the social and professional network of the researcher, or that of other subjects. In addition, the single case design introduces some potential validity issues as well. Limiting the scope to a single case, rather than multiple cases, lowers the generalisability of the results, as specific conditions can deviate across cases. Amongst those deviations, but not limited to, are contextual differences between countries (demographical, economic, political, etc.) or across various levels (national, supranational and international). Consequently, it will not be possible to generalise the results to other populations or cases. Nonetheless, the research proves its relevancy through a deep understanding and explanation of the studied aspects of interest for the selected case. However, the interpretive character of the study can lower the reliability of the results. Ensuring reliability of the results becomes more difficult for two reasons. Firstly, caused by the ever-changing environment people are subjected to, (expert) opinions are dynamic and tend to change over time, rather than stay idle. Secondly, the open and flexible nature of the conducted interviews may lead to different

questions asked when the questionnaire is repeated. Hence, this will lead to a slight difference in results. In this sense, ever interview is unique and cannot be exactly replicated.

During the designing phase of the study, the mentioned limitations issues have been addressed. Considering the inherent limitations of qualitative design, the scope of the research is not to generalise the results. This does, however, present an opportunity for future research, as larger scale follow-up studies should be able to better generalise results. Even so, the study was limited to a small sample size, which allowed rich and in-depth data to be gathered, in line with the small amount of time and budget available to the researcher. Despite a small sample size, reputable experts were selected to increase the quality and internal validity of the results. The selection of interviewees was validated, not only by professionals in the field, but also by cross checking the sample with some of the research subjects themselves. In addition, the sample represented most relevant actors. Both experts from the private and public sector were included to further enhance internal validity. Using semi-structured interviews, the issue of replication and reliability was mitigated to an acceptable level. Moreover, by guiding the questions using pre-existing knowledge, validity was increased without causing biased results.

4. Findings

Through various rounds of inductive coding, data acquired from the interviews has been analysed. The dataset was examined to find patterns and insights relevant to the main research question how experts view strategic cyber security autonomy in The Netherlands. By analysing the results to a point where no new categories or themes would emerge from the data, the results were narrowed down to five main codes. These five themes could be divided into sub-themes, consisting of relevant information and insights to answer the main and sub-questions of the study. First, the general findings within each category will be presented. Next, relevant findings from the more detailed Fox-IT takeover case will be included.

For the convenience of the interviewees, the interviews were held in Dutch. For the purpose of this text, however, all quotes have been translated into English. The original quotes can be found in the footnotes.

4.1. Influencing Factors

Various ways in which government strategy and behaviour towards cyber security interests are being influenced are derived from the collected data. These factors of influence are related to features over which a low degree of control is experienced. In other words, these factors appear to carry a more fundamental character, in a way that they cannot easily be overcome. Therefore, they confine or define the context wherein a strategy can be chosen, essentially influencing the level of autonomy that can be reached. Three categories appeared to be relevant. First, influencing factors that can be found within the country's internal or *national* spheres are presented. Second, external or *global* factors that influence the state's control over cyber security affairs are shown. Third, the perceived balance between various *interests* may affect strategic options in various ways.

4.1.1. National influences

Some national characteristics are identified that are believed to affect strategic options. To begin with, the relatively limited size of the country is perceived to have an effect on different aspects of cyber security strategy. As financial investments require a budget, the national budget for cyber security is mentioned as one of the determining factors. Despite the Netherlands appears to have increased its budget for cyber security over the past years, it is still perceived to be relatively limited compared to other countries.

> *VNO-NCW Official: The United Kingdom is a nice example; they invested a few billions in it [cyber security]. That seems rather contrasting compared to the 95 million euros budget our government announced last year.*[2]

To explain why this contrast exists, references are made to the relative government security budget in general. For example, countries with large national cyber security budgets are believed to have more options available.

> *NCTV Official: When you compare us to countries like the United States, Israel and in a way France, countries that virtually have unlimited military and cyber research budgets. Yes… that would be very nice, but that is not the reality of a relatively small country.*[3]

Besides country and total budget size, another interviewee noticed budget are essentially defined through political decision-making processes.

> *Defence Official: In the end, how much resources you free up for cyber security is a political decision […] there needs to be a certain balance between threats and available financial means and capacity*[4]

Thus, the availability of resources is a described as balancing game. Political priority combined with the total available budget influence the possible courses of action. However, as mentioned earlier, a great deal of cyber resources is in the hands of the private sector. Consequently, the relative size and characteristics of the country's market for cyber security, and the way firms operate in this market, appear to influence the control over cyber capacity. The Netherlands is characterised as a trade nation, causing the cyber security market to be highly globalised. Two interviewees explain:

[2] Uk is wat dat betreft een goed voorbeeld, die steken er echt een paar miljard in, nou daarmee steekt die 95 miljoen die wij nu het afgelopen regeerakkoord voor cyber security hebben vrijgemaakt steekt wat scheel af.
[3] Kijk als je ons vergelijkt met landen als de Verenigde Staten, Israël en in zeker opzicht Frankrijk, landen die bijna ongelimiteerde defensie en cyber onderzoeksbudgetten hebben, ja… het zou heel mooi zijn om het te hebben, maar dat is niet de realiteit van een relatief klein land.
[4] Kijk uiteindelijk is het de politiek die besluit hoeveel middelen maak je voor iets vrij […] er moet altijd een zekere balans zijn tussen dreigingen, beschikbare financiële middelen en capaciteiten

> *BZ Official: In my opinion, the Dutch cyber security market is rather limited, simply because we are a small country. For example, it cannot be compared to America, a much bigger country with a larger technology sector.*[5]

> *EZ Official: On the global financial market, the Dutch economy is not a very extensive one. So, if a Dutch firm wants to grow, they will need to expand their operation globally. We cannot follow a logic of protectionism in The Netherlands, because we are just too small*[6]

Hence, it is argued that cyber security strategy in The Netherlands will always include an international aspect. Due to the market being limited in size, it is not possible to provide all the required capacity and capabilities on a national basis only.

4.1.2. Global Influences

In addition to county characteristics that were shown to influence cyber security options, global factors are considered to influence strategy too. To begin with, the impact of global IT itself are mentioned.

> *NCTV Official: The societal impact of technology has exceedingly developed during the last fifteen years, up to a point where security interests in various issues can no longer be ignored.*[7]

In other words, due to global technological development, it has increasingly become important to secure networks and the people who use them, because our society is dependent upon being connected to the digital world. Moreover, as a result of this global interconnectedness, most interviewees agree that the origin of many cyber threats can be found internationally. Most agree that cyber security influenced by the geopolitical or international security developments in general.

---

[5] Ik denk dat de markt in Nederland voor cybersecurity gerelateerde aspecten is vrij beperkt. Simpelweg omdat wij een klein land zijn. Met Amerika is het bijvoorbeeld niet te vergelijken, omdat het een groter land is en een grotere technologiesector

[6] Op de wereldmarkt is Nederlandse economie niet zo heel erg groot, dus een Nederlands bedrijf die überhaupt wil groeien moet over de landsgrenzen heen gaan kijken. Dus als je – want ik denk dat je bedoelde in termen van protectionisme van je eigen sector dat je daarna verwees – ja die logica gaat in Nederland gewoon niet op want we zijn gewoon te klein.

[7] de impact van technologie op de maatschappij is zo groot geworden, gegroeid ook de afgelopen vijftien jaar, dat je er niet meer aan ontkomt om de veiligheidsvraag constant in allerlei vraagstukken te stellen

EZ Official: At the highest level of cyber security, is still part of the geopolitical developments in the world.[8]

NCTV Official: When there are signs of unrest in the geopolitical world, there will be turmoil in the digital world too.[9]

BZ Official: Looking at cyber conflict like topics, such as cyber espionage or sabotage, international developments have great impact.[10]

Especially regarding the threat of cyber espionage and sabotage, the behaviour of other states might be of influence. Even more, these type or risks are only believed to exists, because other countries are motivated and willing to conduct this kind of operations. One interviewee argues:

BZ Official: I believe certain manifestations prove states are more willing to use certain instruments to serve their interests.[11]

Another interviewee brought up an example of a manifestations of the cyber espionage threat. The attempted hack on the OPCW in The Hague, which was attributed to the Russian military intelligence agency GRU, was mentioned. When discussing the incident, an interviewee argued:

Defence Official: It is a very serious incident but identified by our Minister of Foreign Affairs as a symptom of a broader problem, namely the deterioration the international security. Also, alliances that have become more uncertain, a different role of America on the international stage, a different stance of Russia, which was revealed by their behaviour in Eastern-Ukraine, Crimea and in the digital domain.[12]

Thus, position and behaviour of allies, as well as that of non-allied countries, appear to influence the national cyber security agenda. Materialisation of offensive cyber operations,

[8] Op het hoogste niveau van cyber security wordt nog steeds onderdeel van de geopolitieke ontwikkelingen in de wereld

[9] Als het in de geopolitieke wereld ergens onrust is, dan stormt het ook in de digitale wereld

[10] Als je het hebt over cyber conflict achtige dingen, als cyber spionage of sabotage, dan hebben internationale ontwikkelingen hier een grote impact op

[11] Ik denk dat je… absoluut zie je dat bepaalde manifestaties aantonen dat Staten meer bereid zijn bepaalde instrumenten in te zetten om hun belangen te dienen

[12] Dat is natuurlijk een heel ernstig incident, maar dat heeft onze minister, de minister van Buitenlandse Zaken, in een bredere context geplaatst als eigenlijk een symptoom van een breder probleem namelijk de chronische verslechtering van de internationale veiligheidssituatie. Denk aan allianties die niet meer zo vanzelfsprekend zijn, andere rol van Amerika op het wereldtoneel, een andere opstelling van Rusland wat zich uit in Oost-Oekraïne en de Krim en het gedrag in het digitale domein.

such as the one mentioned, is believed to have a motivating effect on government investments in national defensive cyber capacity.

> *NCTV Official: When there are other countries with less friendly intentions investing in offensive capacity, as a country, you are rather naïve if you do not at least invest in defensive capacity.*[13] *It would surprise me if there will be no further investments in cyber capacity and capabilities during the next few years, simply because the outside world is doing the same, so you need to keep up.*[14]

Hence, (political) willingness to devote resources to cyber security seems to be influenced by other actors' investments, as well as their motivations. A cyber power balancing game appears to develop itself due to the increased build-up of cyber capacity worldwide. Moreover, states that have more resources and capacity might be more attractive for skilled cyber security staff. Most interviewees acknowledge that competition for expertise could drain national expertise.

> *VNO-NCW Official: Germany has set up a large research institution and there is a risk that scientists may leave for Germany, where more budget is available.*[15]

> *Defence Official: When it comes to knowledge institutions and universities, I cannot properly assess but I get the impression we are at risk of falling behind other countries.*[16]

> *Deloitte Cyber Security Expert: Companies from the Middle East, the UK, Israel is popular regarding cyber security, America. There is a lot of recruitment for cyber security expertise going on, so I think it is very difficult to keep people inside. Once the climate deteriorates here or gets better somewhere else, I can imagine people will transfer to other places.*[17]

---

[13] als andere landen die je wat minder vriendelijk gezind zijn investeren in offensieve capaciteiten, dan ben je een heel naïef landje als je niet investeert in defensieve capaciteiten… op z'n minst.

[14] Het zou me stellig verbazen al je daar de komende jaren niet nog meer capaciteit in op gaat bouwen, omdat gewoon simpelweg de buitenwereld dat ook doet en je dus daarin ook een stap mee vooruit moet zetten.

[15] . Duitsland is met een heel groot kennisinstituut komen ze en je ziet dat er ook wel een risico bestaat dat bijvoorbeeld wetenschappers wegtrekken naar bijvoorbeeld Duitsland

[16] , op het gebied van kennisinstellingen, universiteiten, et cetera kan ik dat niet zo goed inschatten maar heb ik de indruk dat daar wel enig risico bestaat dat we achteropraken bij andere landen

[17] Een bedrijf uit het Midden-Oosten, uit het VK, uit Israël is een populair land op het gebied van cybersecurity, uit Amerika. Er wordt wel heel veel gerecruit naar cybersecurityexpertise, dus ja ik denk dat het lastig is om mensen binnen te houden. Zodra het klimaat voor de mensen, voor de experts, hier niet goed is of zodra het ergens anders veel beter is dan kan ik me zo voorstellen dat mensen ergens anders heen gaan.

BZ Official: There is a competitive element regarding [cyber security] knowledge between countries due to that scarce knowledge[18]

Consequently, other countries' investments may have an effect on the availability of expertise in the Netherlands, which is considered to be crucial for effective national cyber security.

4.1.3. Perceived interests

Various interests are at play that are related to the behaviour of actors in cyber security. In the broadest sense, the interplay between commercial or market interests and public or national security interests form a recurrent pattern in the data. One interviewee clarifies:

NCTV Official: In The Netherlands, we have always tried to find a balance […] We have always stood for an open and secure internet.[19]

Arguably, cyber security is believed to take on a more prominent role within the Dutch political agenda. Three interviewees clarify:

NCTV Official: Over the last couple of years, I noticed security more often appear on the political radar. I would never want to claim that The Netherlands has been naïve, but especially during the 90s we focussed on economic opportunities rather than security.[20]

Defence Official: I think the unrestrained need for a free open market without rules has come to an end. Aspects like sovereignty and national security have made their comeback.[21]

VNO-NCW Official: Maybe it is not directly noticeable in government behaviour yet, but security has increasingly become a more prominent theme.[22]

Especially in terms of public awareness and the willingness to devote means to cyber security efforts, the shifting focus from an economic perspective towards a national security

[18] er ook een competitief element tussen de verschillende landen op basis van die beperkt kennis
[19] Als Nederland hebben we altijd heel erg gekozen voor het zoeken van balans […] hebben we altijd gezegd we zijn voor een open en veilig internet
[20] De afgelopen jaren hebt gezien dat veiligheid als onderwerp meer op de politieke radar staat. Ik zou nooit willen beweren dat wij als Nederland naïef zijn, maar in Nederland hebben we zeker in de jaren negentig hebben we het heel veel gehad over de economie, kansen en misschien wat minder over veiligheid
[21] Die meer ongeremde, ongebreidelde drang naar een vrije open markt zonder regels waarin dat zichzelf wel regelt, dat die tijd wel voorbij is ja. Dat nu inderdaad aspecten als soevereiniteit, nationale veiligheid, terug zijn van weggeweest.
[22] je ziet het misschien nog niet direct in het acteren van de overheid maar je ziet wel dat veiligheid een steeds groter thema is

perspective may have an effect. However, the interviewees acknowledge that a competition between commercial and security interests can be challenging. Simultaneously, public and private interests do not always compete and overlap in some cases.

> *EZ Official: I mean, government and corporations have different interests, they exist for different reasons. Luckily, there is overlap to some degree and that's were public-private cooperation can be established.*[23]

Despite public actors and private actors exist and are motivate for different reasons, public-private cooperation can be established where interests overlap. Section 4.3 will discuss public-private cooperation in more detail.

4.2. National Cyber Security Capacity & Capabilities

National capacity and capability building was regarded as key element in the state's ability to decide and to act upon national cyber security interest, both now and in the future. Moreover, data from the interviews provided insights in the different aspects of cyber security capacity and capability building on a national level. In addition, various challenges were pointed out. The results show a differentiation between *characteristics* and *current challenges* related to capacity and capability building, as well as identified *sustainability challenges* for maintaining capacity and capabilities in the future. On the one hand, expertise knowledge, information sharing, and the availability of skilled experts were identified as characteristics. On the other, education and research were considered important for future sustainability.

4.2.1. Characteristics and current challenges

As presented by the data, cyber security is considered a knowledge intensive domain. Through a mix of public, private and scientific actors, a relevant body of knowledge is created, in order to strengthen the national cyber security capacity and capabilities (NCTV Official, personal communication, November 22, 2018). There is a consensus amongst the interviewees that a strong cyber security knowledge position exists in the Netherlands. Also, it is said to be a prime reason for the country's leading role and ability to act, not only within its national borders, but also outside it. Two interviewees explain:

[23] Ik bedoel de overheid en bedrijven hebben verschillende belangen, ze bestaan om verschillende redenen. Gelukkig is er dus ook overlap tot op een bepaalde hoogte, in die overlap kun je publiek-private samenwerking tot stand brengen.

Defence Official: They [PESCO] have cyber projects in which The Netherlands often has a leading role. I think this is due to our great knowledge position and excellent qualified staff. Also, our intelligence services have a good reputation when it comes to cyber security.[24]

Deloitte Cyber Security Expert: From a private perspective, I think The Netherlands has quite a progressive and a rather good level of expertise within the field of cybersecurity.[25] *[…] For example, our Deloitte experts literally travel around the world to help firms. I often visit Dutch subsidiary companies abroad or foreign firms to help them with cyber related issues*[26].

Although the quality of cyber security knowledge in The Netherlands is consistently regarded as relatively high, some pointed out quantitative challenge.

EZ Official: I think we have a great deal of high-quality knowledge in The Netherlands in the field of cybersecurity, but still too little.[27]

In addition, the challenge concerning the amount of knowledge that can be generated, is directly related to the availability of qualified experts. Although cyber security is a highly technical domain, it was explained that human capacity remains one of the most important aspects. Interviewees report that both private and public sector are struggling to find enough qualified cyber security experts due to an international shortage.

Defence Official: Capacity is scarce and within the cyber domain, capacity is primarily related to humans. We have computers and networks, but it's about the people who have to do something with it[28]

[24] 'Die hebben ook cyberprojecten waarin Nederland toch vrij vaak de voortrekkende rol speelt. Dat heeft te maken met, denk ik, een goede kennispositie en goede mensen die we hebben, goed gekwalificeerd personeel.'
[25] 'Ik heb zelf het meeste zicht op privaat. Ik denk dat we zeg maar in Nederland best wel een vooruitstrevend, best wel goed niveau van expertise hebben op het gebied van cybersecurity.'
[26] 'In mijn werk bij Deloitte zie je veel dat onze cybersecurityexperts letterlijk de hele wereld over gaan om allerlei bedrijven, met name te helpen op het gebied van cybersecurity. Ik ben ook regelmatig in het buitenland om bij dochterondernemingen van Nederlandse bedrijven dan wel buitenlandse bedrijven te helpen met cybersecurityvraagstukken.'
[27] Ik denk dat we in Nederland veel hoogwaardige kennis hebben op het gebied van cybersecurity, altijd nog steeds te weinig.
[28] Capaciteiten zijn schaars, in het cyberdomein zijn capaciteiten vooral mensen, computers die hebben we wel en netwerken, maar het gaat om de mensen die er iets mee moeten kunnen doen.

VNO-NCW Official: Talking about knowledge: we still have too little cyber security experts.[29]

Deloitte Cyber Security Expert: There are more and more people these days that call themselves cyber security experts and a great deal of firms that offer cyber security services. This is, however, commercially driven, because cyber security is a hot issue. At the same time, the group of experts is relatively small.[30]

As another way of increasing knowledge and expertise, cyber threat and vulnerability information sharing was mentioned. Especially the private sector and the 'global cyber security community' are believed to produce a great deal of information about vulnerabilities in systems that can be exploited. One interviewee explains most information can be found though communities on the internet:

Deloitte Cyber Security Expert: Let's say the bigger global community, it's not really one community, but there is a great deal of information available on the internet and every day, more information is added, such as new attack methods, new things. I think that's were the biggest share of knowledge comes from. There are people that produce information and there are people that consume it, so to say.[31]

Accordingly, much of this information sharing appears to be done through Computer Emergency Response Teams (CERTs). Various actors from different sectors can be engaged in knowledge sharing practices on those platforms.

NCTV Official: I think a lot of information is shared there [CERTs]. At the same time, a great deal of information is being shared by the private sector with the global CERT community, so that works quite well.

[29] 'Maar als je het hebt over kennis, ja: te weinig cyber security specialisten'

[30] Er zijn steeds meer mensen die zich cybersecurityexpert noemen en heel veel bedrijven die cybersecuritydiensten aanbieden, maar dat wordt heel erg gedreven vanuit commercieel perspectief, omdat cybersecurity heel hip en heel hot is springt iedereen erbovenop, terwijl de groep experts heel klein is ten opzichte van de groep mensen die dat soort diensten aanbieden aan de overheid en dan heb ik het vooral over vanuit het bedrijfsleven

[31] Dus meer uit laten we zeggen de grotere internationale community op dat gebied, het is niet echt één community maar op internet is er natuurlijk heel veel beschikbaar op dit gebied en er komt ook elke dag meer beschikbaar op dit gebied, nieuwe aanvallen, nieuwe dingen. Ik denk dat daar het grootste deel van de kennis vandaan komt. Je hebt zowel mensen die kennis consumeren als kennis produceren zeg maar.

Public actors can benefit from these structures by engaging in cooperation with private and civil actors. Due to the extensiveness of the discovered data related to cooperation, this category will be presented in more detail later in this chapter.

4.2.2. Sustainability

The cyber realm is a fast-developing domain. To ensure a consistent long-term level of cyber security capacity and capabilities, some interviewees have stressed the importance of suitable education, as well as advancement of research in cyber security related topics. Two interviewees from the private sector agree:

> *VNO-NCW Official: I think The Netherlands has a good knowledge position, but we need to remain thoughtful and we need to adequately invest to be to able maintain this position.*[32]

> *Deloitte Cyber Security Expert: There is a lot that needs to be developed, I think it [cyber security] requires a lot of research, both scientific academic research as well as applied practical research.*[33]

Here, private firms and knowledge institutions, such as (technical) universities are believed to have an important role, as most knowledge exists within and is created through these actors (BZ Official, personal communication, February 6, 2018). Even so, interviewees suggest that the government could have an important role in stimulating research and education as well. Financial incentives are named as an important tool for the government to facilitate education and research.

> *BZ Official: I think the government has or could have a stimulating role through financial investments.*[34]

> *Deloitte Cyber Security Expert: In my opinion, the role of the government should be to support companies and universities, so they can carry out new research to develop new products.*[35]

[32] Dus ik denk dat onze kennis positie wel goed is, maar we moeten wel heel attent blijven dat het zo blijft en dat we daar voldoende in blijven investeren.
[33] Er is nog heel veel ontwikkeling in nodig, ik denk dat nog heel veel onderzoek nodig is op dat gebied, zowel wetenschappelijk onderzoek als toegepast praktisch onderzoek.
[34] Ik denk dat de overheid ook een stimulerende rol speelt of kan spelen met het geven van geld, investeringen.
[35] Ik zie zeg maar de rol van de overheid in het ondersteunen van bedrijven en van universiteiten wellicht, om daar onderzoek naar te doen en producten te ontwikkelen

However, when asked whether financial investments alone could be enough in stimulating knowledge building, one interviewee replied:

> *BZ Official: It boils down to questions like: is there a need for knowledge you want to create? Will there be clients who want to buy it? Can we keep, place and maintain it? So, it's not just a matter of handing over a bag of money, that won't solve the problem, but it is one of the most important requirements for creating incentives.*[36]

Thus, in order to increase effectiveness, investments must be guided by a strategic plan. The government has initiated the National Cyber Security Research Agenda (NCSRA), which was argued to add this strategic layer to government investments. The example was brought up by various interviewees as the Dutch government's approach to centralise scientific and research needs. One interviewee explains the goal of the NCSRA:

> *EZ Official: We want to stimulate science and research, and we want to do that in a broader context. Not just individuals with some ideas, but to have a framework for it*[37]

With the NCSRA being collectively drafted by public and other actors, various actors have identified gaps in knowledge and established research subjects (NCTV Official, personal communication, November 22, 2018). While the ability to keep up with development and evolving cyber threats is considered imperative, the NCSRA is used to guide and fund new initiatives, such as the National Detection Network (NDN) (JB, personal communication, 2019).

Overall, government's investments in knowledge, information sharing and expertise are considered important characteristics for maintaining a strong capacity to establish national cyber security resilience. Despite the current position being described as mostly positive, ensuring The Netherlands' long-term knowledge position, as well as maintaining the availability of skilled experts, requires continuous research and educational development, interviewees argued.

[36] Uiteindelijk komt het voor een groot deel, kun je die kennis, is er behoefte aan die kennis die je wil creëren, dus is daar een afnemer voor? En kun je die ook behouden, plaatsten en borgen? Dus het is niet alleen een zak geld geven, dat lost het probleem niet op, maar het is wel een van de belangrijke voorwaarde om vanuit overheidsperspectief dingen in gang te zetten.

[37] Het is ook zo dat je wetenschap wil stimuleren en je wil kijken hoe kan je dat in een soort breder verband doen dat niet iedereen een ideetje heeft, maar dat er ook een soort kader is.

4.3. Public-private & international cooperation in cyber security

By analysing the data, it has become evident that cooperation is essential in cyber security. A wide range of cooperative opportunities were brought forward, such as cross-dimensional cooperation between public sector, private sector and civil society, as well as international cooperation. Accordingly, the interviewees have identified various *benefits of cooperation*. Although none of them challenged the importance of national and international cooperation, collected data also suggest cooperation may have some *limitations.*

4.3.1. Benefits

To begin with, cooperation is considered to be a useful way for creating better effectiveness in cyber security. Two possible ways of cooperation are mentioned. It can be done in the context of research, but also on more operational levels.

> *NCTV Official: We cooperate quite intensively with countries like the United States, Singapore and Australia, to jointly carry out academic research, as well as more operationally focussed collaboration or threat intel sharing*[38]

Especially cyber threat information sharing was believed to induce a synergising effect on cooperation in cyber security. The interviewees explained that, due to the globalised network of cyberspace, the same attacks can be carried out countless times. Moreover, they are not bound by branches or physical location. Therefore, sharing information does not necessarily weaken one's position, but it could strengthen each other's resilience, as one interviewee added:

> *NCTV Official: Information about threats and incidents in member state A, can also be useful to enhance cyber resilience in member state B.*[39]

In practice, these international collaborations take on different forms. To begin with, some cooperative efforts are presented that work through existing structures and alliances, such as the EU and NATO:

> *Defence Official: Especially in the cyber domain, international cooperation is essential. NATO has labelled cyber as one of their military operational domains.*

[38] Dan heb je het bijvoorbeeld over landen als de Verenigde Staten, Singapore, Australië, Nou daarin hebben wij een redelijk intensieve samenwerking om mee academisch onderzoek te doen of operationele samenwerking of informatie over dreigingen

[39] Informatie over dreigingen en incidenten in lidstaat A die ook belangrijk kunnen zijn om de weerbaarheid van lidstaat B te verhogen

Therefore, NATO must be capable of effectively acting in the digital domain. This can only be done when individual allies have cyber capabilities and are willing to contribute this to allied missions and operations.[40]

BZ Official: Through the European Union, investments are being made in ENISA and similar institutions to increase the ability to build and maintain knowledge on a European level.[41]

NCTV Official: From the perspective of the NCTV, the European Union is an important partner which has invested in a directive that enables a landscape of CERT- organisations.[42]

Based on these examples, it seems that international cooperation in cyber security is flourishing. The idea of 'stronger together' in cyber security appears to be a valid assumption. For the effectiveness of collective cyber defence within NATO, but also to strengthen cyber security of all member states through the European Union.

Even more, cooperation is argued not to be limited to pre-existing security cooperation only. A noticeable cooperative structure that is often referred to is Computer Emergency Response Teams, which can be public-private cooperation itself. CERTs are said to cooperate on national level, supra-national level and even internationally (NCTV Official, personal communication, November 22, 2018). By doing so, they provide a national and international landscape of different CERTs where various actors, such as security and intelligence agencies, government departments and private firms, can share information with each other. The national Dutch CERT, known as the National Cyber Security Centre (NCSC), was brought forward as a successful example.

[40] Vooral in het cyberdomein is samenwerking internationaal essentieel. Om bij de NAVO die je noemt te beginnen, ook NAVO heeft cyber als operationeel domein als domein van militair opreden bestempeld, dus ook in het digitale domein moet de NAVO effectief kunnen optreden. Dat kan alleen maar als de afzonderlijke bondgenoten cybercapaciteiten hebben en bereid zijn die aan te dragen bij bondgenootschappelijke missies en operaties

[41] Anderzijds zie je wel dat bijvoorbeeld via de Europese Unie er wordt geïnvesteerd in ENISA en dat soort instellingen om op Europees niveau die kennis beter te verwerven en te borgen.

[42] Als ik vanuit het Nationaal Cyber Security Center en de NCTV kijk, zien we juist dat de Europese Unie als onze belangrijke partner de afgelopen jaren heeft geïnvesteerd in een richtlijn die een landschap van CERT organisaties verplicht.

> *EZ Official: Many companies have information about system contaminations that happened at their own firm. They can share this with the NCSC, and they will determine if this could be relevant information for someone else too*[43]

With public-private partnership being a core element of the NCSC's existence, the involvement of both public and private actors was further analysed. The necessity was explained in twofold. On the one hand, involvement of the government in cyber security affairs was related to their responsibility regarding national security.

> *Defence Official: Threats in the cyber domain are part of a broader national security context*[44] *[…] National security involves different threats and various [government] actors that must do something with it*[45].

On the other hand, it was pointed out that many of today's IT is privately owned. Hence, a large amount of information and knowledge is situated within the private sector. Especially large-tech companies, such as Google or Microsoft, are perceived to be crucial partners.

> *NCTV Official: By 2020, probably 98% of our vital infrastructure will be owned by the private firms*[46] *[…] You will always have a partner relationship with large tech-firms, because you are also, to some extent, dependable on the information and knowledge they possess about vulnerabilities or potential problems in their products.*[47]

Moreover, partnerships were believed not only to increase effectiveness of cyber security but were also considered necessary for complementing one's own cyber security capacity and capabilities. Despite the need to invest in the ability to self-sufficiently develop cyber capacity and capabilities, taking on extensive and complex subjects within cyber security solo, is considered undesired and even impossible.

---

[43] Heel veel bedrijven hebben informatie over besmettingen die ze zelf hebben gehad of zo, dat zijn dingen die ze kunnen delen met het Nationaal Cyber Security Center, die dan vervolgens gaan kijken is dat relevant voor iemand anders.

[44] Je moet dreigingen zien – dreigingen in het cyber domein – als onderdeel van dreigingen in de nationale veiligheid.

[45] Kijk je hebt verschillende soorten dreigingen voor de nationale veiligheid en verschillende soorten actoren die daar iets mee moeten doen

[46] Anno 2020 is eerder 98 procent van de vitale infrastructuur in handen van bedrijven

[47] zeker als je naar het internet kijkt heb je ook altijd een samenwerkingsrelatie met de grote tech-reuzen waar je natuurlijk wel in die zin ook in belangrijke mate van afhankelijk bent van informatie en kennis die zij hebben over kwetsbaarheden en problemen in hun eigen producten.

> *Defence Official: The basis that the military can no longer do it on its own […] that is something we definitely acknowledge in policy documents.*[48] *Regarding developments, such as Artificial Intelligence, Quantum Computing, Big Data, etcetera […] those are things we cannot autonomously stay up-to-date with.*[49]

In sum, cooperation is considered an inevitable aspect of effective and adequate cyber security capability. As public-private cooperation on a national scale might be useful for this purpose, it is considered to have a limited reach. Therefore, to look for cooperation with actors outside the country's national borders is regarded to be a necessity. However, both public-private partnerships and international cooperation appear not to be without restraints.

4.3.2. Limitations

Despite cooperation was consistently called beneficial and necessary for effective cyber security policy, some limitations were put forward. First, from a government perspective, willingness to accept a certain balance of dependency appears to be relevant. Therefore, it is argued that international cooperation should always be accompanied by investments in one's own capacity and capabilities, as one interviewee explains:

> *NCTV Official: It is needless to say that regarding cyber security, which is essentially an international affair, one should invest in international research […] However, you should also be allowed to invest in your own country, as building a strong knowledge basis is considered to be a strategic interest.*[50]

Investing in international capacity is also considered problematic as some countries seem to more advanced national capacity than others. As a result, some countries are said to gain more from cooperating, while other might not.

[48] Dat is ook wel iets wat wij onderkennen in beleidsstukken […] het principe dat je het niet meer als defensie zelf kan

[49] Als je denkt aan ontwikkeling op het gebied van Artificial Intelligence en Quantum Computers, noem maar op, Big Data […] als defensie gaat je dat niet lukken om daar autonoom up-to-date te blijven

[50] Wat mij betreft is het geen discussie dat je bij een onderwerp als het internet cybersecurity, wat van nature grensoverschrijdend is, dat je daar ook in internationaal verband in onderzoek *investeert* […] maar ja je mag ook best in je eigen land investeren om te zorgen dat daar ook een hele stevige kennisbasis is omdat je ook strategische belangen hebt om daar een eigen positie te hebben.

> *Defence Official: [in NATO partnerships] there are countries that have better developed capacities than others. When talking about sharing those cyber security capacities, some countries might benefit more from it than others.*[51]

Also, freeriding is considered a risk to successful cooperation. Encouraging countries to develop national capacity of their own is believed to be more effective in some cases, the interviewee added:

> *Defence Official: What you try to prevent is that countries will get discouraged to invest in their own capacities, because of the idea that they will get sufficient means from allied countries anyway. This determines our approach in EU context, but also in the PESCO system: cooperation is a good thing, but every country also has their own responsibility regarding national capacity building.*[52]

Consequently, it is argued that not all forms of cooperation might lead to better effectiveness of cyber security on a national level. Hence, deciding when and when not to cooperate is perceived to be essential. Although many opportunities to start projects and other forms of collaborations exist, the government should carefully select what cooperation structures to engage in.

> *VNO-NCW Official: There is a high willingness to cooperate, but a difficult question is: what do we invest in, what do we leave aside and how do we choose the things that will really help The Netherlands?*[53]

This concept of selectivity is analysed by another interviewee. For cooperation to remain a feasible and effective tool, partnerships are often limited to a select group, as argued:

[51] Je hebt toch landen die met capaciteitsopbouw een stuk verder zijn dan andere landen, dus als je het dan hebt over bijvoorbeeld het poolen van capaciteiten op cybersecuritygebied waarvan andere landen dan gebruik kunnen maken daar heeft het ene land daar meer belang bij dan het andere land

[52] Dus je wilt niet dat landen achterover gaan leunen op het gebied van capaciteitsopbouw omdat ze die toch wel krijgen van een ander land, dus dat blijft ook wel onze insteek in EU verband, ook in de PESCO systematiek want ja, tuurlijk samen, dat is goed, elk land heeft afzonderlijk ook een eigen verantwoordelijkheid om eigen capaciteiten op orde te hebben

[53] Dus de bereidheid om samen te werken is groot, ik denk dat het lastigste is: waar zetten we wel op in, waar zetten we niet op in, wat zijn nou echt de krenten uit de pap die Nederland echt verder helpen

> *NCTV Official: As within every domain, a nation must decide what countries it wishes to primarily cooperate with, simply because it is not possible to maintain intensive partnerships with every single country in the world.*[54]

While it is not possible to cooperate with everyone, one interviewee explains how the government can select useful partnerships. An assessment on how the potential partners can be of value towards national cyber security interests is ought to be the leading motivation in selecting partners.

> *Defence Official: Everyone wants to cooperate with everyone: states with other states, within the context of the EU, firms are queuing up, so you have to be selective and ask yourself: ok, how will this further our national interest, the security of The Netherlands and how the military can attribute to this.*[55]

It has become evident that international and public-private cooperation in cyber security is inevitable and necessary. Effectivity of national cyber security abilities can be boosted and, where needed, cooperation appears to be able add capacity where needed. However, not all forms of cooperation seem to further national cyber security interests. As unlimited cooperation is considered impossible and not all collaborations might be useful, the interviewees stress the need for the government to be selective while engaging in partnerships.

4.4. Strategies to control cyber security interests

Collected data from the interviews suggest various ways in which national cyber security interest are being managed in the Netherlands. These findings show how the government seeks to cope with fundamental limitations or influences in the cyber security domain. Three different approaches recur that explain how resources are effectively and efficiently being marshalled, and how the government seek to control its national cyber security interests. First, the country's *governance structure* appears to play a significant role in efficiently organising cyber security. Second, *regulation and oversight* were described as important tools for the government to control cyber security interests. Lastly, the data outlines a *risk*

[54] Eigenlijk zoals in elk domein bepaal je als land met welke landen je prioritair samen wil werken, gewoon simpelweg omdat je niet met alle landen in de wereld tegelijk goed kunt samenwerken, intensief kunt samenwerken.

[55] Kijk iedereen wil wel met iedereen in zee; landen met elkaar, landen in EU-verband, bedrijven staan aan de poort, dus je moet daar wel heel goed in selecteren van oké hoe brengt dat ons verder en op nationaal gebied hoe brengt dat de veiligheid van Nederland verder en de bijdrage die defensie daarin kan leveren.

management approach that serves as a guiding theme in most decision making regarding cyber security control.

4.4.1. Governance Structure

Most interviewees seem agree that the cooperative nature and horizontal alignment within Dutch cyber security governance structure provide The Netherlands with unique benefits. Even so, due to their responsibility for national security in general, the NCTV, as part of the ministry of Justice and Security, is said to have a coordinating role in national cyber security matters. In practice, general cyber security responsibility is distributed over all government departments.

> *Defence Official: Although the NCTV plays a central role, they require knowledge and input from other actors, such as safety regions, intelligence agencies, ministry of defence. So, it is pretty decentralised, which works quite well. It's a sort of networked environment, wherein everyone contributes using their own expertise.*[56]

> *NCTV Official: The Netherlands is not really a country that works through hierarchical lines where only one person is responsible […] we are good at cooperating, connecting and coordinating.*[57]

The willingness to involve non-government actors in cyber security policy echoes a decentralised approach. Two interviewees referred to the Dutch 'polder model' in cyber security, an approach used in Dutch politics that is based upon consensus building.

> *NCTV Official: I think there is one unique thing about The Netherlands compared to other countries: we have very short lines of communication… let's call it the Dutch polder model in cyber security […] Through collaboration between science, public and private, I think we are quite successful when it comes to determining new research subjects.*[58]

---

[56] Dus op zich is het… heeft de NCTV die centrale rol, maar kan ook niet zonder de kennis en input van andere instellingen, zoals Veiligheidsregio's, inlichtingendiensten, defensie, dus het is hier best wel uitgesmeerd en volgens mij werkt dat wel prima, een soort van genetwerkte omgeving krijgen waarin ieder vanuit zijn eigen expertise zijn bijdrage levert.

[57] We zijn in Nederland niet echt een land wat werk vanuit hiërarchische lijnen waarbij één iemand verantwoordelijk is […] we zijn goed in samenwerken, verbinding en coördinatie.

[58] Dat je één ding hebt wat Nederland wel heel uniek maakt ten opzichte van andere landen, is de hele korte lijnen, zeg maar… noem het maar even het Nederlandse poldermodel op het gebied van cybersecurity […] het feit dat het met z'n alle best goed is – en daar mogen we best trots op zijn – goed in slagen om samen in een

> *EZ Official: This is where out Dutch culture comes in: we are from the polder and that's why we cooperate with anyone who might contribute […] this means governments, companies, as well as civil society, are all involved in finding solutions together.*[59]

However, potential issues regarding this approach were noticed as well. Two interviewees warned that distribution of responsibility might also lead to ambiguity and compartmentalisation of expertise.

> *Defence Official: Within the ministry of defence, there are four organisational units […] In my opinion, our work has become rather compartmentalised and, as a result, all units have been building cyber capacity separately. This is not always very efficient, as most organisational units will more or less require people with similar knowledge and capabilities*[60]

> *VNO-NCW Official: Cyber security policy responsibility is dispersed over various ministries, which causes it to become very complex sometimes, especially for private companies.*[61]

Recognising these issues, the way cyber security efforts are organised are mostly seem to have a strengthening effect on Dutch cyber security position. The cooperative and decentralised nature is perceived to be capable of efficiently and effectively make use of available cyber security resources, despite of some fundamental limitations and influencing factors that have been mentioned earlier in this chapter.

4.4.2. Regulation & Oversight

Besides financial incentives, regulation and oversight were mentioned as other public sector tools used to influence cyber security. Especially in this domain, where reliance upon essential private partners is perceived as rather high, laws and regulation were mentioned as

---

driehoek van wetenschap, publiek en privaat te kijken naar wat zijn nou onderwerpen waar we kennis op willen bouwen

[59] Hier zie je ook weer onze Nederlandse cultuur in: we zijn van de polder, dus we zeggen goh we gaan gewoon met iedereen om de tafel die wat kan bijdragen en dan komen we er samen wel uit […] dus je praat zowel met overheden als het bedrijfsleven als civil society en dat je met al die partijen bij elkaar tot oplossingen komt.

[60] We hebben vier verschillende organisaties […] Dus wat je wel hebt gezien naar mijn mening is dat we best wel verkokerd zijn gaan werken en al die vier takken van sport binnen defensie hebben hun eigen capaciteitsopbouw gedaan op cybergebied en dat is niet altijd even efficiënt, omdat het uiteindelijk gaat met min of meer mensen met vergelijkbare kennis en capaciteiten die je zoekt in alle takken van sport

[61] Wat je ziet is dat cyber security heel erg verdeeld is over diversen ministeries en dat maakt het af en toe wel lastig

useful tools to control public cyber security interests. Moreover, to effectively use regulation as a tool, government oversight is considered to increase. One interviewee explained:

> *VNO-NCW Official: Eventually, you will notice that oversight of companies will increase, especially for companies that are part of the critical infrastructure, but also of digital service providers.*[62]

As one way of using regulation as a tool, the use of existing laws was mentioned. References were made to one case where already existing laws were applied to cyber security considerations. To manage private firms that handle classified digital data and secret information, the Ministry of Defence makes use of their ABDO (General Security Requirements for Defence Contract) regulation, as one interviewee experienced:

> *Fox-IT CRO: The use and handling of classified information is already quite strictly regulated*[63]

Whereas some aspects of the existing regulation were considered applicable, it did not appear to be suitable in all circumstances. Therefore, existing legislation was said to be amended to better incorporate cyber security matters.

> *Defence Official: The old ABDO regulation originated from the year 2006. Since a year or two, we have new regulation in place that is, for example, better focussed on digital security and cyber security aspects*[64]

However, the regulation used in this example is only applicable to military contracts. In a broader perspective, general legislation to control interests in other areas is believed to be lagging. An interviewee speculated about the need for additional regulation.

> *BZ Official: The question that needs to be answered by the government is: what subjects are considered important enough to deploy other means to organised them, such as additional laws and regulation.*[65]

[62] Uiteindelijk ja en wat je gaat zien is dat er meer toezicht gaat komen, in het bijzonder op bedrijven in de vitale infrastructuur, maar ook op digitale dienstverleners.
[63] Het hele gegeven van gerubriceerde informatie en de omgang daarmee, daar zit al behoorlijk strenge wet- en regelgeving op.
[64] De oude ABDO-regels kwamen uit 2006, we hebben nu nieuwe regels, inmiddels een jaar of twee, die bijvoorbeeld veel meer aandacht hebben voor digitale veiligheid en cybersecurity aspecten.
[65] Dan is ook de vraag vanuit de overheid vanuit welk onderwerp vinden we het zo belangrijk dat we dus ook andere middelen in gaan zetten, bijvoorbeeld wet- en regelgeving, om iets te organiseren

Especially regarding the country's critical infrastructure, a lack of regulation to control cyber security interest is noticed. The risk of undesired foreign influence over critical infrastructure, is argued to be amongst those subjects for which additional regulation is needed. Moreover, one interviewee noticed the government is working on more generic laws to control foreign interference in all relevant cyber security areas:

> *Defence Official: The Ministry of Economic Affairs and the Ministery of Justice and Security are almost done drafting a law allowing the government to stop foreign takeovers and investments, or even to reverse them. This law is focussed on telecom, but they are already talking about drafting more generic laws.*[66]

While more general laws are still being developed, potential workarounds have been identified. One example has shown that existing emergency laws might be initiated. When partners who are vital to national cyber security are at risk of falling into the wrong hands, emergency laws can be used as a last resort option, as one interviewee explained:

> *Defence Official: This [using emergency laws] is already possible: the ministry of finance has a standard law that can be adjusted to fit a specific situation. Then, in case of a real emergency, both chambers [first chamber and parliament] can decided whether to adopt this law within one day time.*[67]

Besides legislation, contractual agreements between government actors and private suppliers are perceived to be able to fill in the gaps of current laws. An example was brought forward in which the Ministry of Defence, together with one of their private contractors, agree to formally add additional security requirements to the contract.

> *Defence official: Legislation and ABDO regulation are rather broadly formulated […] as a result, the focus may not be specific enough for a certain situation.*[68]

Hence, current regulation may need to be supplemented with additional agreements to maintain an adequate level of control over vital cyber security interests. However, national regulation, emergency laws and even contractual agreements, fall under national jurisdiction.

[66] Volgens mij zijn ze er wel vrij ver vanuit EZK en JenV met het maken van een wetgeving die de regering in staat stelt om ongewenste overnames uit het buiteland of investeringen tegen te houden of zelfs terug te draaien. Die wet ziet specifiek op telecom, op de telecommarkt, maar er wordt ook al gesproken over meer generieke wetgeving

[67] Dat kan nu al, het ministerie van financiën kan gewoon een soort standaardwet uit de plank trekken, die even schrijven naar de situatie en dat kan in één dag door beide kamers als dat echt een noodgeval is

[68] Ik denk dat wet- en regelgeving en het ABDO zijn heel breed opgesteld […]Dus waar je wel eens tegenaan kunt lopen is dat dat niet heel specifiek toegesneden is op één bepaalde situatie.

As most private firms are said to operate globally (BZ Official, personal communication, November 28, 2018), legislation from a foreign state may in some cases be applicable instead. Examples have shown that foreign laws can have a problematic effect. Regarding the ban of Russian anti-virus software Kaspersky from government networks, it was stated that:

> *Defence Official: we are still worried about Russian legislation and other mechanisms that could potentially prevent this firm [Kaspersky] from operating independent from Russia*[69]
>
> *NCTV Official: There are laws and regulations in another country that can force private firms to cooperate with the authorities of that other country […] this influence how you think about cooperating*[70]

As a solution, investing in supra-national regulation might be essential to overcome this limitation in the future, one interviewee suggested:

> *BZ Official: By having an open economy and by being member of the EU, we have, or we will have to organise regulation on EU level for many things, including cyber security.*[71]

In sum, some legislative tools to control vital cyber security interests are currently available to the Dutch government. Despite no general laws has been drafted so far, the interest in developing such laws show the need for more legislative tools to control cyber security interests. Meanwhile, more sector focussed regulation, such as ABDO, contractual agreements or, as a last resort, emergency laws, are used. Even so, some firms might fall under foreign jurisdiction, which sometimes may cause concerns, as Dutch regulation and oversight appears to be limited to national spheres only.

4.4.3. Risk Management Approach

Recurring references have been made to the use of risk management logic in decisions to act in national cyber security affairs. Most considerations are primarily seen as balancing act

[69] Maar we zijn toch bezorgd vanwege Russische wetgeving en andere mechanismes dat dit bedrijf wellicht niet geheel onafhankelijk van Rusland kan opereren.
[70] er is sprake van wet- en regelgeving in een ander land die dat bedrijf dwingt om meet te werken met de autoriteiten van dat andere land
[71] We zijn een open economie en onderdeel van de Europese unie, dus voor best wel veel zaken zullen we dus ook regulering op EU-niveau moeten gaan organiseren of er is al EU-regulering van op EU-niveau van toepassing die ook op cybersecurity eventueel van toepassing kan zijn.

between potential risks and benefits. Based upon the threat-level and potential impact on society, resources to act are distributed over various cyber security issues.

> *BZ Official: Looking at the variety of cyber threats, there are different gradations, ranging from simple annoyances to the most severe cyber conflict kind of situations […] Looking at current priorities, cyber espionage and sabotage clearly carry great potential impact. The manifestation of this potential impact causes these themes to receive a higher priority than other phenomena.*[72]

Likewise, cyber threats to what is called 'critical infrastructure' are perceived to have a higher priority over other concerns. Due to the impact a disruption of critical infrastructure might have on society, risks are considered to be high.

> *VNO-NCW Official: Critical sectors provide products and services that are crucial for our society, often utilities. Failure of vital infrastructure can result in social disruption.*[73]

Even so, due to the international characteristic of cyber security, it is seemingly common for products and services that are provided by an international supplier to be used, even in critical infrastructure. However, the introduction of this international aspect appears to be of influence on the risk assessment. When asked to explain how the government decides what cyber security products to use or in what partnerships to engage, similar answers were given that indicate the use of risk management rationale.

> *BZ Official: When deciding to exclude certain services or products, a risk analysis is carried out to see whether the costs can be balanced against the benefits.*[74]

The ban of a Russian based firm's anti-virus software from government networks appeared to be a typical example. In this case, the government chose to terminate all use of the software, based off their risk analysis. One interviewee explained:

---

[72] Als je kijkt naar de verscheidenheid van de cyberdreigingen, heb je een maatstaf van vervelende nuisances tot aan de hoogste cyber conflict achtige situaties […] Kijk je naar waar nu veel aandacht voor is, naar cyberspionage of sabotage dat is duidelijk een onderwerp wat veel potentiele impact heeft en waardoor zeg maar, de manifestatie en de potentiele impact maakt het dusdanig dat daar hoger op geprioriteerd wordt dan andere verschijnselen

[73] De kritische sector leveren natuurlijk vaak producten en diensten die cruciaal zijn voor onze samenleving, vaak zijn dat nutsvoorzieningen. Als deze nutsvoorzieningen uitvallen kan dat leiden tot sociale onrust.

[74] Nou, als je kiest om bepaalde producten en diensten uit te sluiten heb je een risicoanalyse gedaan, dus of de kosten opwegen tegen de baten.

> *NCTV Official: The Dutch government has put forward three arguments: the hard and software has far-reaching access to computer systems, foreign legislation is applicable that can force a company to cooperate with authorities, and specifically that country has an offensive strategy towards the Netherlands.*[75]

Hence, risk management logic can be observed, as both a cyber threat and its potential impact were mentioned. The perceived willingness of a foreign country to conduct cyber espionage, combined with the potential impact it can have on critical computer systems – due to the software's high level of authorisation – allows for a risk analysis to be carried out.

In another frequently featured example, the risk assessment of the situation is believed to have led to different decisions. The takeover of Fox-IT, a company that develops encryption products and services for the Ministry of Defence, by a British company, was mentioned as another case which led the government to reassess their risks (Defence Official, personal communication, November 22, 2018). Although ownership by a foreign parent company added risks regarding government control over Fox-IT, it was told that they decided to remain using the firm's services, though additional requirements were put in place.

> *Defence Official: Well, when such a company is being bought by a foreign actor, that will lead to a reassessment of your relationship with such a firm. In this case, it has not, however, lead to termination of the relationship, but it has caused it to become better ensured.*[76]

A more detailed analysis of the considerations and measures that were put in place will be discussed in the next section of this chapter.

Due to the extensiveness of some risks and limited means to solve them, a risk management approach appears to help prioritise the distribution of capacity and capabilities. Not to cover all risks but to mitigate the most pressing ones. Through this rationale, a system of gradation emerges that can be linked to the desired control over cyber security related interests. The higher the perceived risks, the bigger the desire to control these interests. On the one hand, it can mean partnering with national suppliers only, as well as completely excluding services or

[75] De Nederlandse overheid op grond van drie argumenten heeft gekozen: a) de hard- en software heeft diepgravende toegang tot computersystemen, b) er is sprake van wet- en regelgeving in een ander land die dat bedrijf dwingt om meet te werken met de autoriteiten van dat andere land en specifiek dat andere land, dat heeft een offensief programma wat ook gericht is op Nederland

[76] Ja als zo'n bedrijf overgaat naar een buitenlandse partij, dan leidt dat wel tot een heroverweging van je relatie met zo'n bedrijf. En nu heeft dat in het geval van Fox niet zo zeer geleid… juist niet geleid tot bijvoorbeeld het verbreken van de verbanden, maar juist tot het veel meer verankeren van je relatie

products. On the other hand, certain risks can be mitigated to acceptable levels by taking a more careful approach towards international cooperation.

4.5. Fox-IT case

This section will discuss the acquired results from two interviews regarding the takeover of Fox-IT by the NCC Group. The case involved two private and one public stakeholder, respectively: The NCC Group, Fox-IT or more specific Fox Crypto, and the Dutch Ministry of Defence. The latter two stakeholders are represented in the dataset. First, a short case introduction will be provided. Next, relevant results are presented following the identified codes and one emergent code: strategic partnership.

4.5.1. Case Description

Fox-IT is a Dutch cyber security company based in Delft, specialised in IT-security and encryption. The Dutch government, amongst other the Ministry of Defence, is one of Fox-IT's biggest clients. They deliver essential applications for secure communication, which is particularly important in the context of military operations and intelligence (Defence Official, personal communication, November 22, 2018). In 2015, Fox-IT announced the acquisition of the firm's shares by the NCC Group, a listed British company. The acquisition quickly raised questions amongst government officials, who were concerned about the potential effects of the takeover on Dutch national security. Negotiations between the Ministry of Defence, Fox-IT and NCC Group were initiated to discuss those concerns and to come up with solutions (Leijten & Rosenburg, January 24, 2017; WODC, 2017). Currently, the shares are still owned by NCC Group but Fox-IT's crypto division has formally been split from Fox-IT and turned into a Fox Crypto BV, a private subsidiary of the NCC Group based in The Netherlands.

4.5.2. Influencing factors

Collected data shows how some relevant factors influenced the range of potential actions and decisions of the government. First, comments were made regarding the market of encryption products and services. Both interviewees described the market as a 'knowledge intensive' and 'small'.

> *Fox-IT CRO: From the perspective of The Netherlands, there is only a very small market […] it is debatable whether that is interesting for a commercial actor.*[77]

> *Defence Official: I can imagine, from an entrepreneur's perspective, that you might not be very motivated to invest in such a small knowledge intensive market. Moreover, often you cannot force a larger market to emerge. In that sense, the government cannot always control this*[78]

Both sides view this as a challenge. On the one hand, it reduces the government's options to choose an alternative supplier. On the other, as one of their biggest sources of income, government contracts generate a large share of Fox Crypto's revenue.

4.5.3. Capacity & Capabilities

Although not being part of the nation's critical infrastructure, Fox-IT delivers essential products to secure government communications. In general, cryptography is believed to be an important fundamental in cyber security.

> *Fox-IT CRO: It is not the same as critical infrastructure, however, we are very aware that we provide security what really matters.*[79]

Regarded as being essential for secure lines of communication, strong encryption is crucial to 'safely, securely and effectively' carry out military operations. Besides military communication, most crucial government information is saved digitally. Thus, the encryption is considered a vital aspect of securing top secret information, not only in terms of business, but also for state secrets.

> *Fox-IT CRO: Products we develop that allow our clients, especially the government, to protect top secret or classified information.*[80]

[77] Als je vanuit de Nederlandse overheid en vanuit nationaal belang kijkt en je beperkt dat tot Nederland, dan heb je maar een hele kleine markt en dat is voor een commerciële partij… dat hangt er erg vanaf of dat dat commercieel interessant is

[78] Maar ik kan me voorstellen als niet-ondernemer zijnde, ik kan we wel voorstellen dat er, juist omdat de markt zo klein is, dat het animo in zo'n super kennisintensieve markt te springen als aanbieder, dat het niet overloopt van enthousiasme om daarin te springen. Dus je dwingt een grote markt ook niet altijd af. Dus in die zin heb je dat ook lang niet altijd in de hand als Rijksoverheid.

[79] Maar dat is niet hetzelfde als kritieke infrastructuur, maar wel het bewustzijn dan we met beveiliging bezig zijn die er echt wel toe doet

[80] Producten die wij maken die onze afnemers, met name de overheid kunnen gebruiken om zeer geheimen informatie, dus gerubriceerde informatie, te beschermen

Cryptography, however, requires rather specialised knowledge, which is not in great supply. Subsequently, crypto knowledge and expertise is regarded to be an important national cyber security asset. As mentioned during earlier interviews:

> *NCTV Official: Regarding cyber security, encryption is certainly a very important element for which one would want to have a knowledge basis in The Netherlands, without being completely dependent on others.*[81]

This argument is reaffirmed in the case of Fox-IT. Data showed that it was essential to maintain the knowledge and expertise in which Fox-IT and the government had jointly invested in over the years.

> *Defence Official: During the years [of cooperation], a great deal of expert knowledge has been developed. For the military, retaining this knowledge is essential to continue to be provided with this kind of cryptographic applications in future.*[82]

4.5.4. International and public-private cooperation

Data suggests government cooperation with the private sector is beneficial but also necessary. It is argued that Fox Crypto possess high quality expertise knowledge on encryption. However, this vital expertise about secure communications and data protection but does not seem to be owned by any government agency itself. When asked if the government has reconsidered to provide their own encryption applications, instead of outsourcing it, an official argued:

> *Defence Official: Yes, that is an option, but the military, and I think this applies to all the government, does not possess this kind of knowledge […] We are not capable to develop and create those things on our own.*[83]

This does, however, appear to be regarded as a suboptimal situation. Having a close partnership – instead of being fully self-sufficient – was named to be 'the next best thing' in case of military grade encryption, according to the interviewed official.

---

[81] Encryptie is natuurlijk wel een – als je kijkt naar cybersecurity – een heel belangrijk fundament waar je ook in je eigen… in Nederland wilt zorgen dat je een eigen kennisbasis blijft houden, waarbij je niet voor alles afhankelijk bent van anderen

[82] Daarnaast natuurlijk dat je heel veel kennis hebt opgebouwd in de loop der jaren, heel veel specialistische kennis, die je ook nodig hebt om in de toekomst voorzien te blijven als defensie van dit soort cryptologische toepassingen.

[83] Ja dat is een optie, maar ook de overheid, defensiedienst, maar volgens mij geldt dat voor de hele Rijksoverheid heeft die kennis niet in huis […] we zijn niet in staat om zelf het spul te ontwikkelen en te maken.

Even more, the introduction of an international component to the partnership appears to have influenced to the structure of the cooperation. The effect of foreign ownership of a private partner was brought up in more detail, as it might pose a problem.

> *Defence Official: If Fox Crypto BV impends to move to a foreign country, it would definitely be a problem.*[84]

While moving Fox-IT to a foreign country appears to be problematic in general, the issue would become even greater if the acquiring party has a basis of operation in a country that has poor diplomatic ties to The Netherlands. Both interviewees explain what the effect could be:

> *Defence Official: I will not mention specific countries but assume there is a company based in a country you are in conflict with. Also, you know the firm has good ties with their country's government and they want to takeover Fox Crypto BV. That's a no-go, it's not going to happen.*[85]

> *Fox-IT CRO: Look, it is in no one's interest if we would be taken over by a Russian actor. In that case, not only our customers but also our employees will probably leave […] the government is a very good customer and an important partner for us, so in is not in our interest to look for an [acquiring] organisation that will cause everything to fall apart.*[86]

Thus, despite public-private cooperation being inevitable for developing encryption, international cooperation appears to be limited by diplomatic ties and the potential of foreign government relation with the firm. However, depending on how the structure of the firm changes, this does not completely exclude partnerships with international actors. Far-reaching restructuring might be an issue, while slight changes may be acceptable. One interviewee adds:

[84] Als Fox Crypto BV zou dreigen te verhuizen naar het buitenland, ja dan heb je een probleem.
[85] Nou ja stel, ik zal waken voor het noemen van specifieke landen, maar stel je bent met een land in een conflict en een bedrijf uit dat land, waarvan je weet dat het goede banden heeft met de overheid, wil Fox Crypto BV overnemen, dan lijkt me dat een no-go, dan gaat dat niet gebeuren.
[86] Kijk niemand heeft er belang bij dat wij door een Russische partij worden overgenomen, want dan gaan onze klanten ook weg misschien en dan gaan onze mensen weglopen […] de overheid is een hele goede klant van ons en ook een hele belangrijke partner van ons, dus we hebben er ook zelf geen belang bij om naar een partij op zoek te gaan waarvan je van tevoren al weet dan klapt de boel

Defence Official: A company that is taken over by a foreign holding company while everything remains the same, or a company is taken over, dismantled and moved to another country, those are two very different situations. So, there are gradations.[87]

4.5.5. Strategies to control cyber security interest

Allowing the government some degree of control over Fox-IT is considered crucial to ensure adequate encryption of classified communications. Data shows the government engaged in various efforts to maintain this control. In line with previous identified themes, the interviewees explain how national cyber security interest have been managed during the takeover process of Fox-IT.

4.5.5.1. Governance

Although negotiations between the government, Fox-IT and the NCC Group are mentioned to have been 'constructive', it is also described as being complex due to the Dutch government's governance structure.

Fox-IT CRO: It [negotiation] is rather complex because the Dutch government is formally one actor but consists of many different interest […] there are not just two actors sitting at the negotiating table.[88]

As cyber security is distributed amongst several ministries, in this case too, multiple ministries were included in the talks. While the private and public interest were sometimes competing, so were the interests between the ministries, the interviewee added.

4.5.5.2. Regulation & Oversight

The services and products provided by Fox Crypto BV are subject to ABDO regulations. As mentioned in the general findings, this set of regulations impose various generic security measures on private contracts. From an technical perspective, the ABDO is argued to have set important general security arrangements.

[87] Het maakt nogal een verschil of een bedrijf wordt overgenomen en alles blijft bij het oude met alleen een nieuwe holdingmaatschappij, of een bedrijf wordt overgenomen en ontmantelt, of naar het buitenland verplaatst, of het wordt doorverkocht. Dus je hebt natuurlijk verschillende gradaties.

[88] Het is best ingewikkeld omdat de Nederlandse overheid dat is natuurlijk formeel één rechtspersoon, maar dat bestaat uit allemaal verschillende belangen […] het is dus niet zo dat je twee partijen aan tafel hebt en dat maakt het best wel ingewikkeld

Fox-IT CRO: On operational level, many arrangements were already in place, security [in accordance with] ABDO regulation. Not much has changed.[89]

In addition, government oversight can be arranged through ABDO. When talking about how the government performs quality and compliancy checks on the delivered services and products, the interviewee answered:

Fox-IT CRO: This is possible due to ABDO regulation, because code can be reviewed, there are secret rooms, those are all technical matters.[90]

However, two issues regarding regulation were brought up. First, ABDO regulations was told to be conflicting with other regulation, such as market regulations. One interviewee mentioned an example:

Defence Official: For example, according to regulations for listed companies, information about oncoming changes in ownership, such as share transactions, cannot be shared, whereas the ministry of defence may require this information based on the ABDO regulations.[91]

Second, although existing regulation appeared to be sufficient for controlling post-takeover national security interests, it was explained that ABDO could not be tailored to cover some risks that specifically applied to a takeover scenario. To maintain control, the existing rules had to be supplemented by additional contractual agreements.

Defence Official: Yes, ABDO provides sufficient or suitable tools in theory but practically it appears to be lacking sometimes. Therefore, in the new structure with Fox, we have added additional contractual guarantees that are supplementary to ABDO[92]

[89] Waarbij je natuurlijk op operationeel vlak heel veel dingen al geregeld hebt, want die waren al geregeld, dat gaat gewoon beveiliging, ABDO-regeling, eigenlijk is er niet zo veel veranderd.
[90] Dat doe je omdat je dus ABDO-regelingen hebt, dat doe je omdat code gereviewd kan worden, dat zijn allemaal technische dingen, dat doe je door, in de ABDO zijn allemaal regelementen van hoe je… weet je, je hebt geheimen ruimten
[91] Soms heb je informatie die over aanstaande wijzigingen in het eigenaarschap, bijvoorbeeld aandelentransacties die je vanuit de wetgeving hebt omdat je beursgenoteerd bent, nog niet kunt delen, maar die wij vanuit onze regelgeving, de ABDO – Algemene Beveiligingseisen voor Defensie Orderbedrijven – wel willen weten
[92] Dus in die zin, ja de ABDO geeft je daarin genoeg of passende instrumenten in theorie, maar in de praktijk wil het wel eens wringen. Maar goed daarom hebben we nu ook in het nieuwe construct met Fox additionele contractuele waarborgen toegevoegd aan het ABDO-stelsel.

The most important motivator for including these additional rules was not only the takeover itself, but to control the fate of the company after the takeover. Especially, rumours of a possible takeover of the parent company NCC Group were of great concern to the government. If this scenario would become reality, the capability to exert control in favour of Dutch interest would become particularly difficult (Defence Official, personal communication, May 12, 2019)

In general, control over jurisdictions and sphere of influence required consideration. National legislation and regulation are only applicable and can only be enforced within national borders, one interviewee told. As a result, for regulation and oversight to be effective, it is argued that the firm needed to be kept under Dutch jurisdiction to assure sustainable control over cyber security interests.

> *Defence Official: To control oversight, to control agreements, to control security, only with companies that are based in your own country a structure of future assurances can be devised, as it cannot be enforced at a foreign based country.*[93]

4.5.5.3. Risk Management Approach

A risk management approach was commonly referred to as driver behind decisions being made and measures being taken. First, the need for a thorough assessment of the acquiring actor showed this rationale being applied. One interviewee explains how possible risks were assessed and evaluated:

> *Defence Official: First, there is a sort of assessment of the acquiring firm: Who is it? What are the intentions behind the takeover? From what country? What kind of government is involved? Which strategy? How are the ties between government and private firms in that specific country? What is their track record in, amongst other things, espionage, unfair competition?*[94]

To carry out a risk assessment, intelligence and security agencies are perceived be crucial actor in providing the right information. Especially in case of a foreign takeover, this seems

[93] Toezicht heb je in eigen hand, de afspraken die je met zo'n bedrijf kan maken heb je in eigen hand, het aspect van veiligheid, wat in je eigen land gebeurt kun je beter in de gaten houden dan wat er in het buitenland gebeurt, zekerheden inbouwen voor de toekomst, dat kun je ook alleen met een bedrijf in je eigen land, dat kun je niet afdwingen in het buitenland

[94] Er is er natuurlijk eerst een soort van assessment van de overnemende partij: wie is dat? Met welke intentie wordt de overname gedaan? Uit welk land komt de overnemende partij? Wat voor een regering zit daar? Welke strategie? Wat zijn de banden tussen overheid en bedrijven in dat land? Wat is het trackrecord van dat land op het gebied van, nou noem eens wat, spionage, oneerlijke concurrentie

crucial, as one may assume that the involvement of a foreign actors always introduces new risks.

> *Fox-IT CRO: Depending on the acquiring actor, whether it is about services or technology, or where they are located… It is probably fair to say, in case of a takeover, there will always be additional risks, because it involves a foreign actor taking ownership.*

However, the interviewee continues by explaining that not all risks can be fully eliminated. Fox-IT is a private firm that operates through rules of the global market, rendering it impossible to exclude or prevent foreign involvement completely and the risks that come with it. The interviewee adds:

> *Fox-IT CRO: The question should not be: are there additional risks involved, but to what extend are they a problem and can we mitigate them, are we able to quickly notice when something goes wrong, are we able to penalise wrongdoing? It really is a risk management effort.*[95]

Thus, the significance of applying a risk management approach is perceived to be, not in eliminating, but in mitigating risks to an acceptable level. While total self-sufficiently in IT is argued to be 'an illusion', some cases might require stronger mitigation than others. In this case, mitigation allows the government to hold an adequate level of control over Fox Crypto BV, without having to nationalise the firm.

Consequently, various possible gradations of control can be created. When vital interests are at risk, rather significant measures are considered to be necessary. Requiring Fox-IT's crypto department to formally become a Dutch based subsidiary, is argued to be a significant measure. One interviewee puts it in a broader context:

> *Fox-IT CRO: I think some of our products are in that category [vital interests] but there are many other products that can be assigned to that category as well. Products which should be adequately controlled. This means that in some cases you may want*

[95] De vraag is natuurlijk vaak niet zijn er extra risico's, maar in welke mate is dat een probleem en kunnen we ze mitigeren, kunnen we tijdig zien als er iets fout gaat, hebben we een stok om mee te slaan ofzo, dat is eigenlijk risicomanagement. Niet de risico's willen uitbannen, als het kan wel, maar als het niet kan moet je ze hanteerbaar maken.

it to be Dutch from cradle-to-cradle. In such case, not even a chip should be made in China.[96]

However, it might not always be necessary – neither possible – to keep this degree of control over suppliers regarding national cyber security. Subsequently, when less vital interests and lower risks are involved, less severe measures can be taken to reach an acceptable level of control.

4.5.6. Formal strategic partnership

Notably, a specific form of cooperation between Fox-It and the Dutch government is presented in the data. The unique circumstances regarding Fox-IT and the government led both parties to engage in what is called a strategic partnership. One interviewee explains what this form of partnership entails:

Defence Official: Signed on high level, we guarantee a certain revenue at Fox. This way, we enable them to invest in a very small market with better assurances towards the future […] normally, this would be against rules on anticompetitive behaviour, but in this case, considering involved national security interests, especially the proper functioning of the military, it is legitimised to engage in such partnership with only one company.[97]

Also, this example was brought up to by the other interviewee. While, acknowledging the strategic partnership can be very beneficial regarding government interests, it was said to be helpful for Fox-IT too.

[96] Een aantal producten van ons, die passen daar wel in denk ik, maar er zijn nog wel meer producten in Nederland die daar echt wel in horen, waar ook over nagedacht moet worden van oke maar dat, dat is wel zo belangrijk dat moeten we echt goed onder controle houden. Dan kan het in sommige gevallen dus zijn dat… ja van cradle-to-cradle zeg maar Nederland moet zijn. Dat moet je dus ook niet een chipje in China laten bouwen

[97] Het is ook niet voor niks dat wij uiteindelijk als defensie een formeel strategisch partnerschap met Fox-IT hebben afgesloten, gewoon ook ondertekend op hoog niveau, waarin we bepaalde omzet garanderen bij Fox, zodat Fox met iets meer toekomstzekerheid investeringen kan doen in een hele kleine markt […] normaliter zou dat misschien ingaan tegen de regels van de open markt en mededingingsregels. Maar in dit geval, ook gezien het belang van de nationale veiligheid, met name het veilig functioneren van defensie, is het geoorloofd om zo'n partnerschap aan te gaan met één specifiek bedrijf.

> *Fox-IT CRO: We have engaged in a strategic partnership with the Ministry of Defence for the development of crypto products. This shows that [Defence-Fox-IT] collaboration is just very good.*[98]

As explained, the partnership was enabled through the alignment of commercial and public interests. Both the Ministry of Defences, as well as Fox-IT, acknowledged their mutual dependence and therefore decided to formally engage in as strategic partnership. From a government perspective, this interdependence is said to have strengthened the government's ability to control. It has enabled them to create a 'constructive' dialogue during the takeover and has helped to reach agreements over vital aspects regarding Fox-IT. Although both interviewees acknowledge the benefits of their mutual dependence, one interviewee doubts whether this form of public-private partnership would also be applicable or possible in other circumstances.

> *Defence Official: It might be different if it would have been a large market with many suppliers and potential clients. This would perhaps change the context, causing us to be able to exert less influence on the process.*[99]

[98] Los daarvan, en dat heb je misschien gelezen in het nieuws eind vorig jaar als ik het goed heb, hebben we een strategisch partnerschap gesloten met het ministerie van Defensie over het ontwikkelen van cryptoproducten.

[99] Het was waarschijnlijk anders geweest als het een hele grote markt was geweest met heel veel spelers, dan is de context heel anders en wellicht heb je dan minder invloed op dit proces

5. Discussion & Conclusion

In this chapter, the meaning of the outcomes of this study will be discussed. Both the general findings and the findings from the Fox-IT case will be synthesized to conclude the study. First, by analysing the findings, the sub-questions will be discussed. After that, an answer to the main research question will be provided. The final part of this chapter considers the limitations to this study, as well as suggestions for future research into this topic.

5.1. Discussion of the Results

Sub-question 1: How do security experts characterise SCSA in The Netherlands?

Recurring patterns in the findings suggest that Strategic Cyber Security Autonomy in the Netherlands is characterised by three intertwined aspects: strategies to control vital security interests, methods to build and sustainably maintain cyber capacity & capabilities, and ways to assess and to balance the benefits and limitations of international and public-private cooperation. The range of possible decisions in all three categories appear to be pre-determined by national and global factors of influences, as well as a balancing game between private and public interests.

5.1.1. Influencing factors

In this study, experts identified aspects that fundamentally influence and therefore shape SCSA in the Netherlands. These influences arise from the context wherein SCSA is established and include national resources, international security situation and perceived importance of security interests. Although this might not represent an exhaustive list of contextual influences, for the purpose of this study, these findings have been categorised under ‘influencing factors’, as they cannot be, or are not easily controlled by actors involved but do seem to determine a range of available options regarding SCSA. Hence, they are indirectly limiting the Netherland’s strategic decisions but do not entirely prevent them from pursuing strategies to increase cyber security autonomy. It does, however, imply that, complete total or near-total self-sufficiency is virtually impossible in the case of The Netherlands.

To begin with, globalisation of IT is amongst the main causes that prevent the country from becoming fully self-sufficient, as functioning of the internet depends on being interconnected. However, the most important factor appears to be the limited size of the Netherlands as a country. Reduced national resources in terms of security and defence budget, but also the

relatively small size of the cyber security market inherently limits possible courses of action and, subsequently, the country's cyber security autonomy. This is in line with Harknett & Yalcin (2012) idea of 'autonomy as a struggle', as they mention that pure autonomy is unattainable due to the absence of sufficient concentration of power. Instead, governments seek relative autonomy, which is supported by the finding that the Netherlands tries to balance their investments in cyber capacity against global threats and other states' investments in (offensive) cyber capabilities. However, smaller sized countries like the Netherlands are faced with a challenge posed by countries with larger sized budgets. One effect is argued to be a drain of expertise from the Netherlands towards countries with more copious means.

In addition, political beliefs play a role. It influences how threats are perceived and how they should be mitigated. Over the last years, increased materialisation of cyber threats and more unpredictable international relations have gradually shifted the Dutch government's focus on economy to a focus on national security, a trend that appears to run parallel to the shift in the EU's focus towards European security. Even so, being important partners in national cyber security affairs, private firms mainly have a commercial interest, which the government also has to take into account to maintain effective public-private cooperation. Here too, a balancing effort between the various interests is believed to influence the country's strategic autonomy decisions.

5.1.2. Capacity & capabilities

By examining the dataset, cyber security capacity and capabilities emerged as an essential theme regarding the ability of the Netherlands to act on cyber security interests. References to capacity and capabilities echoed the idea of freedom to act in cyberspace as put forward by Institut Montaigne (as cited in Mauro, 2018), while also providing a more detailed image of what it means. The availability of qualified cyber security experts, or more specifically, the quality of the knowledge they create, is perceived to be key in understanding what cyber security capacity entails. Therefore, it could be argued that knowledge is, indeed, power within the domain of cyber security. Unfortunately, results are inconclusive to fully explain what cyber security capacity entails and especially or if private knowledge should be considered national cyber security capacity. However, what has become evident is that possessing a certain level of capacity at one point of time is only half the story. While high qualitative knowledge appears to be present in the Netherlands, experts are scarce.

Resonating with the theoretical definition of strategic autonomy, the ability to maintain capacity on the long-term was underlined.

Accordingly, education of skilled experts and advancement of cyber security research was regarded important for sustainable capacity building. Unlike one might expect in more traditional security domains, investing in more governmental capacity does not appear to be the solution. Although knowledge can be created within government agencies, it is primarily found in the private and civil sector. Therefore, the government is ought to facilitate capacity building rather than the leading its development. Subsidies and investments into education and research are mentioned as important government tools. Education resembles one of the important categories mentioned by the Global Cyber Security Capacity Center (2016) but based on the findings, it is possible to conclude that research investments are another important way of building and maintaining capacity. To increase effectiveness of the financial research incentives, together with all sectors, guidelines for future research have been set out in the National Cyber Security Research Agenda.

5.1.3. Public-Private & international cooperation

Results show that cooperation with public and private actors, both nationally and internationally, is a vital aspect of acting on cyber security matters. Like reported by various literature sources, the interview outcomes reaffirm the government has an important role in cyber security regarding national security. Simultaneously, the crucial role of the private sector as owners of the underlying infrastructure of cyberspace and as basis of innovative cyber security technologies, was acknowledged as well. Consequently, public-private cooperation appears to be a cornerstone of effective decision-making and acting on cyber security related interests. As assumed, the Dutch National Cyber Security Centre was presented as the Netherland's most prominent public-private cooperation example in practice.

Both for research efforts and more operational information sharing structures, cooperation is explained to have a synergising effect on knowledge or cyber security capacity building. Methods of attack are not bound by any physical border and may be deployed all over the world and across all sectors. Sharing and obtaining this knowledge can help public and private actors to protect their own interests or assets against attacks that happened in another country or in another sector. Whereas knowledge is power, it essentially builds on (international) knowledge sharing. This turns cooperation into a crucial prerequisite for

capacity building. At the same time, however, it creates a dependency on international and commercial actors for Dutch national cyber security.

Results have shown the necessity to manage this dependency by acknowledgement of and acting upon the limitations of cooperation. Essentially, it is argued that international cooperation should be seen as supplementary to national capacity rather than determinative. Though cooperation can be helpful, it is argued that first and foremost, every nation has its own responsibility to build capacity. Even so, in practice, willingness to cooperate seems high but capacity strength appears to be distributed. Consequently, the Netherlands may not benefit from all kinds of cooperation. Therefore, it is crucial to select what cooperation to engage in and what partnership to leave aside. However, the results remain rather inconclusive regarding how this selectivity could decrease dependency towards private actors in terms of national cyber security.

5.1.4. Strategies to control cyber security interests

As emerged from the data, creating and maintaining control over cyber security interests appears to be at the core of managing autonomy. This relates to the country's overall ability to develop cyber security strategy, as featured in the GCSCC (2016) model. The adopted strategy in the the Netherlands presented the ability to use some of the country's unique features to their advantage. The decentralised cyber security governance structure allowed The Netherlands to overcome one of its fundamental limitation: size. Thorough the application of what is called the 'poldermodel' on cyber security affairs, it was argued that the Dutch government is effectively capable of uniting actors, including knowledge and skills form relevant actors. Essentially, by combining unique resources from all sectors, overall cyber security and resilience can be improved at a national level. Interestingly, it was generally regarded an effective strategy but some experts stated an opposing view. As multiple departments are responsible for cyber security, they are all recruiting their own cyber security experts, while the availability of qualified experts is already scarce. In the end, this may significantly lower efficiency of capacity and capability development.

In addition, regulation and oversight can be used to control critical cyber security interests. Existing regulations does offer some opportunities and are in some cases amended to better suit cyber security topics. While this is an ongoing process, foreign investments and takeover attempts showed that, under these circumstances, current legislation on its own give the government insufficient control over cyber security interests. Although emergency laws

could be used in case of an immediate threat to cyber security interests, outcomes suggest there is a need for more generic laws. Especially the country's critical infrastructure is expected to become increasingly regulated. Other services and product outside the critical infrastructure prove to be strongly related to national security as well. Regarding firms with a heavy cyber component, such as Fox-IT, adequate control does seem to require tailored case-by-case regulation. Also, effective control through any kind of regulation or legislation does require an involved actor to fall under Dutch jurisdiction. Capturing the essence of 'self-rule', data has shown that regulation and oversight can only be effective under one's own sphere of influence. However, foreign actors may use their own national legislation to further their interests, which could position Dutch interests at risk. Without supra-national or international alternatives, the 'traditional' importance of the government's rule of law, as stated in the literature, was confirmed. As most firms operate globally, this proves to be a rather challenging issue, as some vital functions provided by those firms require strict control. Examples have shown that, to preserve this control, the government can choose to completely terminate contracts with companies that fall under foreign legislation or require them to stay under Dutch legislation. However, the severity of measures depends on various risk factors.

Consequently, risk management proves to be a crucial rationale in determining the required degree of control over cyber security interests. As a high level of control requires more means, it can only be established over the most essential security interests. Some cyber threats might be accepted, whereas others high impact risks, such as cyber espionage and sabotage, requires mitigation. Overall, the goal is to create an acceptable degree of control rather than a maximum degree of control over cyber security interests. Although risk management is a useful technique, it could be argued that even the desired level of control might sometimes not be reached. Either due to a lack of wherewithal or due to fundamental limitation. However, the current dataset contains insufficient information to confirm the latter, as it is an indirectly derived interpretation.

Sub-question 2: To what extend has SCSA played a role in the takeover of a Dutch government contracted cyber security firm by a foreign actor?

The takeover of Dutch cyber security firm Fox-IT by the British NCC Group presented a challenge for the Dutch government's SCSA. Maintaining the business relationship with the firm was considered a vital national cyber security interest for three reasons: (1) High-end encryption was considered essential for secure government and military communications, (2)

a lack of alternative suppliers due to the small market, (3) inability of the government to develop this technology on their own.

Although existing regulation was applied, it required additional contractual agreements to secure an adequate level of control. Decentralised responsibility for cyber security affairs within the government proved to be challenging during negotiations. Nevertheless, a constructive dialogue between the Dutch government and Fox-IT was possible due to the perceived strong mutual dependence. Consequently, for the agreements to be effective and to keep a knowledge base regarding encryption in The Netherlands, Fox Crypto BV remained under Dutch jurisdiction, as well as geographically located in the Netherlands. Risk assessment of the involved foreign based private acquiring, the nature of the products and the significance of it – and Fox-IT in general – for vital government functions, affected the required degree of control and measures. As a result of the process, both sides engaged in a strategic partnership to ensure long-term supply and demand.

5.1.5. The Role of Influencing Factors

As described in the SCSA characteristics, the size of the Dutch cyber security market significantly influenced the available alternatives. Developing high-end encryption is a knowledge intensive process and there is limited demand in the Netherland. Consequently, only a few commercial actors desire to invest in this market. In this case, limiting the governments options due to complete lack of alternative suppliers. The reason for the government to have little control is that supply and demand are primarily balanced by market forces. The results did not present evidence for any of the other mentioned influencing factors, such as political beliefs, size of government budgets and geopolitical developments. However, the latter may have indirectly played a role, as encryption is essential for protecting data against cyber espionage.

5.1.6. The Role of Capacity & Capabilities

Especially for the government, encryption is an elemental aspect of cyber security, as it is essential for the protection and integrity of classified and top-secret digital data. Even so, a great deal of specialised knowledge – and skilled experts that produce this knowledge – is involved in the development of strong encryption products and methods. Despite not being directly supported by argumentation, the limited market presumes scarcity of these skilled encryption experts. To be able to sustainably and independently provide secure communications, it was considered important to maintain a knowledge base in the

Netherlands. Although it could be assumed that education and research play a role in this knowledge intensive and specialised topic, this was not brought up during the interviews regarding the Fox-IT takeover case and therefore remains inconclusive.

5.1.7. The Role of Public-private & International Cooperation

From the results it can be derived that cooperation between the government and Fox-IT was both essential and inevitable. With benefits being clear, limitations were presented regarding the internationality of this cooperation. Unlike earlier analysed results which focussed more on effectivity and capacity limitations of (international) cooperation, in this case, the effect of diplomatic relations was emphasized. Depending on the effect of foreign ownership on the future structure of the firm, it was regarded acceptable to a limited extend. For example, possible settlement of Fox Crypto BV in any foreign country was considered problematic. Moreover, a potential move to an adverse country was considered particularly unacceptable for both sides. From the perspective of Fox-IT, the potential loss of the Dutch government as a client was presented as a commercial interest not to engage with firms based in adverse countries. From a government perspective, a national security argument based on prevention of adverse foreign interference through private actors was brought forward. However, it remains elusive what was regarded adverse and whether the arguments signified only a risk-based rationale or also a political motivation.

5.1.8. The Role of Strategies to Control Cyber Security Interests

With encryption being exclusively provided by Fox-IT, data showed that the government required tools to control this vital aspect of their cyber security. Especially the foreign takeover scenario presented additional challenges for the Ministry of Defence. Even so, existing security regulation, referred to as ABDO, was already applicable to Fox-IT's contract with the Ministry of Defence. This set of regulations was told to control most of the pre-takeover technical risks and measures related to the public-private partnership, while enabling the government to have oversight on these quality and security requirements.

However, it was argued that the takeover, particularly the post-takeover situation, introduced unforeseen challenges and new risks. On the one hand, it proved that some requirements were conflicting with other legislation, such as market regulations. On the other hand, ABDO appeared to be too generic. Consequently, negotiations were set up to develop supplementary contractual agreements to mitigate the added risks and ensure an acceptable degree of control over the firm's future. Despite negotiations being regarded as complex due to the

involvement of many stakeholders, all agreed to a set of additional requirements, enabling firmer government control over Fox Crypto BV's organisational affairs. These arrangements were chiefly formalised in by-laws.

The severity of the measures to ensure control were legitimised by a risk management approach. Although it was mentioned that an assessment of the costs and benefits of the chosen strategy was carried out, an exact picture of the risk assessment could not be demonstrated during the interviews. In general, the goal of risks mitigation was stressed, as complete elimination was regarded an impossible solution in practice. As a long-term measure, a very specific form of strategical public-private partnership was introduced. As identified characteristic of SCSA, commercial or market and national security interest play a role. In this case, the significance of the national security interest was said to overweigh open market interest and laws, such as anticompetitive behaviour regulations, which allowed the government to guarantee a share of Fox Crypto BV's revenue. Thus, lowering Fox Crypto BV's commercial risks associated to large investments in encryption technology, while ensuring a firmer grip on the company. Subsequently, by building on the actor's mutual dependence, the strategic partnership facilitated a more sustainable and stable partnership for both sides.

5.2. Conclusion

While the results have been discussed to both sub-questions have been discussed, the main research question can now be answered, which was stated as follows: **How do prominent security experts view strategic autonomy in Dutch cyber security policy?**

The results of this study have provided new valuable insights by capturing an initiate general sense of Strategic Cyber Security Autonomy in the Netherlands through the collection and analysis of experts' ideas. Moreover, the examined takeover case of Fox-IT has provided relevant practical insights. As a result, the strategic notion of cyber security autonomy was explained using four categories: (1) The country's ability and methods to build cyber security capacity and capabilities, (2) the way benefits and limitations regarding public-private and international cooperation are being managed and, (3) the adopted strategies to control essential cyber security interests through governance, regulation and oversight, and a risk management approach. These categories appear to be interrelated, as one might have an effect on the other. Moreover, together they were affected by (4) internal and external

influencing factors and perceived interests. Table 5.1 provides a schematic representation of these findings.

First, in line with the theorised working definition, sustainable cyber capacity and capabilities are believed to have crucial role in SCSA. Relevant cyber information, knowledge and skilled experts who create it, is at the core of this aspect. To have a strong knowledge position can be of strategic essence, as was shown in relation to encryption. Capacity and capabilities can be found amongst private, civil and, to a lesser degree, public actors. However, the government holds important tools to help sustain expertise: investing in and facilitation of cyber security education and research.

Second, cyber security can often only be effective through public-private and international cooperation. Strong private presence in the cyber security sector and its global characteristics render cooperation beneficial and often inevitable. In the examined case, the government's dependence on private encryption technology and Fox-IT's dependence upon the military as one of their largest clients, resulted in a strategic partnership. However, each country has its own responsibility to develop capacities and this cannot – and should not – be internationalised. Moreover, it remains important for the government to stay selective what cooperation to engage in.

Thirdly, national cyber security interests should be adequately controlled. Decentralised responsibility and 'poldermodel' governance, aids the Dutch government to effectively control general cyber security interests. For each case, however, the gravity of the desired self-sufficiency requires a risk management assessment, creating a system of gradations where only the most critical interest should be kept under full control. Even in cyber security, most important control tools are regulation and oversight. However, as experienced in the takeover case, generic or conflicting regulations may in some cases need to be supplemented with additional agreements for remain effective, and new legislation might be required in the future. Moreover, regarding the notion of 'self-rule, the Fox-IT case has explained that any form of regulation and oversight can only be effective under Dutch jurisdiction. Turning it into an essential aspect regarding foreign takeovers.

Finally, influencing factors pose fundamental limitations to all of the above-mentioned aspects. On a national level, the size of the Netherlands is the most significant influencer, both in terms of national security budget and the cyber security (labour) market. While this inherently prevents the creation of full cyber autonomy, in overcoming this limitation,

relative autonomy appears to be more a feasible ambition. International factors, such as increasing manifestation of global cyber threats, more uncertain international relations and a build-up of offensive cyber capacity around the world, seem to influence government behaviour in cyberspace as well.

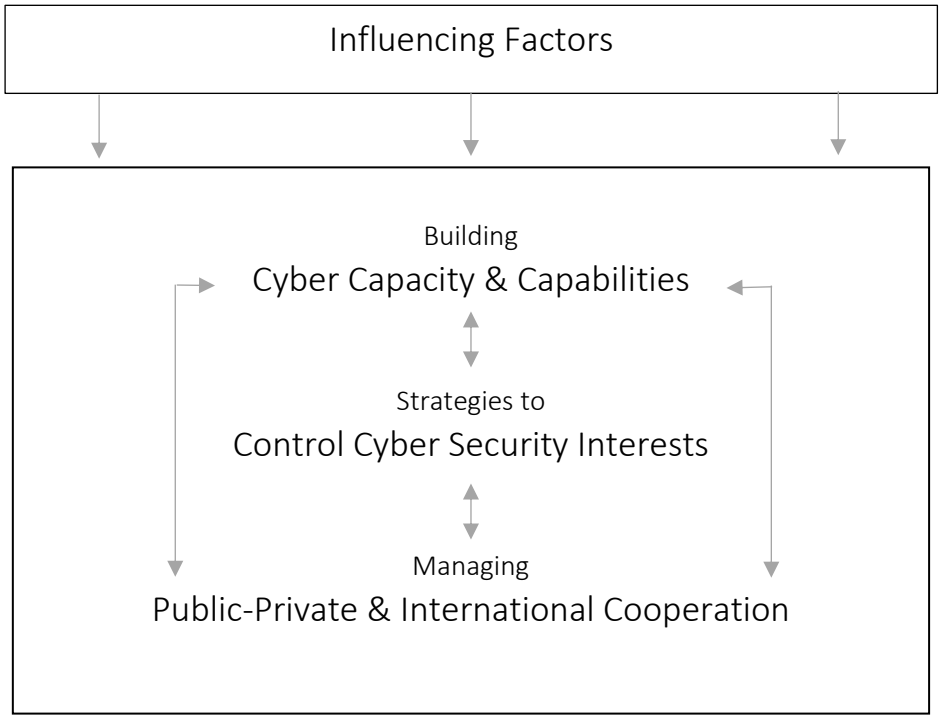

Table 5.1: schematic representation of Strategic Cyber Security Autonomy in The Netherlands

5.3. Limitations & Future Research

While the research question has been answered, it is important to discuss some limitations of the results. First, as this research focusses on valuable expert opinions, one should be aware that these opinions might not represent the view of all the relevant stakeholders in the Netherlands. To prevent personal bias as much as possible, various actors from different organisations were included. However, due to resource and time limitations, as well as the used sampling technique, this list is not exhaustive. For example, intelligence agencies appear to play a significant role in cyber security but were not represented in the dataset. Although the research focussed mainly on cyber security government officials, there is a great political aspect to the question of strategic autonomy that has not been fully considered. In addition,

data was collected at one point in time. Subsequently, it should be acknowledged that experts' opinions prove valuable but may, to some degree, fluctuate over time.

Secondly, national cyber security is highly complex field to analyse comprehensively. Especially within the policy domain, the subject is relatively new, and there is no clear common understanding what national cyber security interests entails. During this study's data collection, no specific division was made between different cyber security themes, such as between different security domains, e.g. military spheres and critical infrastructure. Although this choice was made deliberately to advance the exploratory nature of the study, it left room for interpretation by each individual interviewee. Therefore, it should be considered that this may have caused opinions and explanations to be influenced by personal notions of cyber security.

Moreover, applying strategic autonomy to national cyber security affairs essentially combines two relatively new subjects for which more research is needed to provide the required scientific substantiation. Specifically, in the light of a general theory. Therefore, the results should not be regarded as such. While, generalisation of the results to national level already proves difficult due to the use of interviews, most findings may only be applicable to circumstances in the Netherlands and cannot be stretched to other cases. One interviewee suggested possible differences regarding much larger countries with sizable technology sectors, like the US. Also, this same limitation applied to the examined takeover case. Even though it provided insights in the role of strategic cyber security autonomy, at the same time, the results only representing this role in a very specific scenario. As the military naturally has more means to ensure national security interests, it can be questioned if the same applies to other cases. Even so, big things have small beginnings and the initial explanations derived from this research might prove valuable for future research.

Therefore, an interesting path for future research might be to examine the role of strategic autonomy in other cases, such as telecom or energy. Currently, many countries are discussing if they should allow Chinese firm Huawei to help them build 5G networks. Main concerns are about potential backdoors that can be built in their equipment, only to be used by Chinese intelligence agencies for the purpose of espionage. This case and many other cases, such as the ban on anti-virus software from the Russian company Kaspersky, or the takeover attempt of Dutch telecom provider KPN by a Mexican actor, may provide relevant insights regarding autonomy and dependence in the complex and globalised cyber security realm.

In terms of a more general understanding of the concept, it might be useful to research ideas about strategic cyber security autonomy in a country with a large market and an extensive government budget, such as the US, the UK or Israel. Adjacent to this suggestion, the role of unions and alliances may prove another interesting venue to research. As suggested by one interviewee, for small countries like The Netherlands, economic blocks, such as the European Union, might prove to be a more useful level to become strategically autonomous. While strategic autonomy has already entered the (political) agenda of the EU, its relation to cyber security has yet to gain attention.

5.4. Final Thoughts

Concludingly, this study has emphasised some important aspects of strategic autonomy in national cyber security affairs, as well as how it can be limited. The globalised and interconnected world of cyberspace and society's, as well as the government's, great dependence upon secure access to it, exposed a significant challenge for national security. Whereas cyber security self-reliance is key in protecting vital national interests, the country cannot keep its interests adequately cyber secure in a full self-sufficient way. On the contrary, a nation's cyber security is often strengthened by public, private or public-private cooperation, whether that may be international or national. At the same time, The Netherlands should also be able create enough cyber security capacity on their own. In practice, it has shown that cooperation can either be the best or, due to a dependency on private actors, a second-best option in cyber securing vital interests.

However, it is not about the government's ability to create complete self-sufficiency, but rather about their ability to self-control critical interests. Despite only a small amount of cases might qualify, complete control over the most essential cyber security elements can be legitimised, but it requires adequate tools to control them. The classical idea of 'self-rule' or 'self-governance' appears to play a large role, even in this modern context. National jurisdictions are critical to control cyber security suppliers through regulation and oversight. However, maintaining control can be costly and difficult. Therefore, 'strategic autonomy' is essentially about accepting a certain degree of 'heteronomy' in nonessential features, while introducing measures to sustainably control the most critical national cyber security interests.

List of References

Atkinson, R & Flint, J (2011) Snowball Sampling in Lewis-Beck, M. S., Bryman, A. and Liao, T. F. (Eds.), *The SAGE Encyclopedia of Social Science Research Methods* (p. 1044). Thousand Oaks: Sage Publications Inc.

Autonomy (2019). In *Oxford Online Dictionary*. Retrieved from https://en.oxforddictionaries.com/definition/autonomy

Autonomy/heteronomy. *Oxford Reference.* Ed. Retrieved 5 Apr. 2019, from http://www.oxfordreference.com/view/10.1093/oi/authority.20110803095436286.

Biscop, S. (2016) All or nothing? The EU Global Strategy and defence policy after the Brexit, *Contemporary Security Policy*, 37(3), pp. 431-445. DOI: 10.1080/13523260.2016.1238120

Centraal Bureau voor de Statistiek (2018) *Internet: toegang, gebruik en faciliteiten*. Available at: https://statline.cbs.nl/

Chatterjee, S (2003) Neo-realism, Neo-liberalism and Security, International Studies, 40(2), pp. 125-144

Christman, J. (2018) Autonomy in Moral and and Political Philosophy, The Stanford Encyclopedia ofPhilosophy (Spring Edition). Retrieved from https://plato.stanford.edu/entries/autonomy- moral/

Corbin, J., & Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Donnelly, J. (2000) The Realist tradition in Donnelly, J. *Realism and International Relations* (pp. 6-42). Cambridge: Cambridge University Press.

Drent, M. (2018) *European strategic autonomy: Going it alone?* (Policy Brief August 2018), Clingendael. Retrieved from https://www.clingendael.org/publication/european-strategic-autonomy-going-it-alone

Dworkin, G. (1988) The nature of autonomy in Dworkin, G. (Ed.), *The Theory and Practice of Autonomy* (pp. 3-20), Cambridge: Cambridge University Press. DOI: 10.1017/CBO9780511625206.002

European Parliament (2018). *Report on cyber defence*. Committee on Foreign Affairs. Available at: http://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.pdf

European Union External Action Service (2016) *Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign And Security Policy*. EEAS. Available at: https://eeas.europa.eu/topics/eu-global-strategy_en?page=3

Gerring, J. (2011) The Case Study: What it is and What it Does. In Goodin, R. E. *The Oxford Handbook of Political Science*. DOI: 10.1093/oxfordhb/9780199604456.013.0051

Gillham, B. (2005a) The semi-structured interview. In Gillham, B. (Ed.) *Research Interviewing: The range of techniques* (pp. 70-79), Berkshire: McGraw-Hill Education.

Gillham, B. (2005b) The élite interview. In Gillham, B. (Ed.) *Research Interviewing: The range of techniques* (pp. 70-79), Berkshire: McGraw-Hill Education.

Global Cyber Security Capacity Centre (2016) Cyber Capacity Maturity Model for Nations (CMM). Oxford: Oxford University. Online available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

Goldsmith, J. L., & Wu, T. (2006). *Who Controls the Internet? : Illusions of a Borderless World*. New York: Oxford University Press. Retrieved from http://search.ebscohost.com.ezproxy.leidenuniv.nl:2048/login.aspx?direct=true&db=nlebk&AN=169236&site=ehost-live

Grey, D. E. (2014) Doing Research in the Real World. London: Sage Publications Ltd.

Howorth, J. (2017) European defence policy between dependence and autonomy: A challenge of Sisyphean dimension, *The British Journal of Politics and International Relations*, 19(1), pp. 13-28. DOI: 10.1177/1269148116685296

Howorth, J. (2018) Strategic autonomy and EU-NATO cooperation: threat or opportunity for transatlantic defence relations? *Journal of European Integration*, 40(5), pp. 523-537. DOI: 10.1080/07036337.2018.1512268

Johnson, R. & Cureton, A. (2019) Kant's Moral Philosophy, in Edward N. Zalta (ed.) *The Stanford Encyclopedia of Philosophy* (Spring Edition), Available at: https://plato.stanford.edu/archives/spr2019/entries/kant-moral/

Kaska, K., Beckvard, H. & Minárik, T. (2019) *Huawei, 5G and China as a Security Threat.* NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/

Keijzer, M.C.G., Knops, R.W. & Grapperhaus, F.B.J. (2018, June 15) Nederlandse digitaliseringsstrategie [government letter]. *Ministry of Economic Affairs and Climate*. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/06/15/kamerbrief-over-nederlandse-digitaliseringsstrategie

Kempin, R. & Kunz, B. (2017) *France, Germany, and the Quest for European Strategic Autonomy in A New Era* (Notes du Cerfa No.141), Institut Français des Relations Internationales (IFRI). Retrieved from https://www.ifri.org/sites/default/files/atoms/files/ndc_141_kempin_kunz_france_germany_european_strategic_autonomy_dec_2017.pdf

Koops, E. J. (2010). The internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), *Transnational Criminology Manual* (pp. 735-754). Nijmegen: Wolf Legal Publishers (WLP).

Leijten, J. & Rosenberg, E. (2017, January 24) Wakker geschrokken na Britse overname Fox-IT, *NRC*. Retrieved from https://www.nrc.nl/

Mauro, F. (2018) *Strategic Autonomy under the Spotlight: The New Holy Grail of European Defence,* Brussels, Group for Research and Information on Peace and Security (GRIP)

Ministry of Defence (2018) Defensie Cyber Strategie 2018. Online available at: https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018

Ministry of the Armed Forces (2017) *Strategic Review of Defence and National Security.* Ministère des Armées. Available at: http://www.defense.gouv.fr/

MIVD verstoort Russische cyberoperatie bij de Organisatie voor het Verbod op Chemische Wapens. (2018, October 4). Rijksoverheid. Available at: https://www.rijksoverheid.nl/actueel/nieuws/2018/10/04/mivd-verstoort-russische-cyberoperatie-bij-de-organisatie-voor-het-verbod-op-chemische-wapens

Nationaal Cyber Security Centrum (2018) *NCSC Briefing: Uitfasering antivirussoftware Kaspersky Lab bij Rijksoverheid en advies aan vitale- en ABDO-bedrijven*. Available at https://www.ncsc.nl/

National Coordinator for Security and Counterterrorism (NCTV) (2018) Cyber Security Assessment Netherlands (CSAN), NCTV. Available at https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html

National Defence Authorisation Act for Fiscal Year 2018, Pub. L. No. 115-91, Stat. 1283 (2017). Available at https://www.congress.gov/bill/115th-congress/house-bill/2810/text?r=17

Nye, J. S. (2010) Cyber Power. Cambridge: Belfer Center for Science and International Affairs. Online available at: https://www.belfercenter.org/publication/cyber-power

Osiander, A. (2001) Sovereignty, International Relations and the Westphalian Myth, *International Organization*, 55(2), pp. 251-287. DOI: 10.1162/00208180151140577

Schellevis, J. (2013, August 29) Ondernemingsraad KPN: politiek moet overname verhinderen. *Tweakers*. Available at: https://tweakers.net/nieuws/90980/ondernemingsraad-kpn-politiek-moet-overname-verhinderen.html

Stichting beschermt KPN tegen América Móvil. (2013, August 29) *de Volkskrant*. Available at: https://www.volkskrant.nl/economie/stichting-beschermt-kpn-tegen-america-movil~bd41f85b/

The White House (2008) National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23. The White House. Available at: https://fas.og/irp/offdocs/nspd/nspd-54.pdf

Von Solms, R. & Van Niekerk, J. (2013) From information security to cyber security, *Computer & Security 38*, pp. 97-102. DOI: http://dx.doi.org/10.1016/j.cose.2013.04.004

WODC (2017) *Vitale Vennootschappen in Veilige Handen*. Onderzoekscentrum Onderneming & Recht. Available at: https://www.rijksoverheid.nl/documenten/rapporten/2017/05/22/tk-bijlage-vitale-vennootschappen-in-veilige-handen

Annex: Codes

Themes	Sub-themes
1. Influencing Factors	**Internal/national** National Cyber Security budget/ Political decisions Size of Cyber Security or financial market Geopolitical influence Cyber Security characteristics (interconnectedness technology, private ownership) **External/global** Tangibility of global cyber threats/ experienced cyber threats Competing investments in capacity & capabilities/ balancing of power **Perceived interests** Commercial – security Open market – security
2. National Cyber Security Capacity & Capability	**Current characteristics & challenges** Knowledge Information sharing Skilled experts **Sustainability challenges** Education Research
3. Across-border & Public-Private Cooperation in Cyber Security	**Necessity & benefits** Increased effectivity Private sector dependence Strengthening of capacity and capabilities **Limitations** Selectivity Practical limitation in cooperation