NAVIGATING THROUGH CYBERSPACE WITH THE NATIONAL CYBER SECURITY STRATEGIES

A comparison between the United Kingdom and the Netherlands

E.S.Langevoort

Studentnumber: s2628996

Submission: 28-06-2023

Bachelor Thesis Management, Society and Technology

University of Twente, Enschede

Supervisors: Guus Meershoek and Ola El-Taliawi

Wordcount: 11809

Abstract

One of the main governmental instruments in the cybersecurity system for a lot of countries are the National Cyber Security Strategies. These strategies contain a vision about the ideal position in cyberspace which are to be achieved by goals that are described in these strategies. This study compares the national cybersecurity strategies of the United Kingdom and the Netherlands. It focuses on how these strategies aim to influence cybersecurity, it compares the two strategies and it analyses their differences and similarities. This is done by answering the following research question: ‘’How do the national cybersecurity strategies aim to influence the cybersecurity in the Netherlands and the United Kingdom? ‘’ This question is answered by combining a coding analysis in Atlas.ti of the strategies, relevant literature, and interviews with cybersecurity experts. This study concludes what the main institutions and policies in cybersecurity are and explains the differences of the strategies by discussing what elements influence cybersecurity. One of the main relevant insights from this study are what the main focuses and aims of the strategies are, how much attention each focus point is given, and how the NCSS aims to handle and implement the actions.

Keywords: Cybersecurity, National cybersecurity strategy, United Kingdom, Netherlands, NCSC

Table of contents

Abbreviations

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BBNI	Ministerial Decision on Network and Information Systems Security
CMA	Computer Misuse Act
DPA	Data Protection Act
ENISA	European Union Agency for Cybersecurity
EU	European Union
GCHQ	Gouvernement Communications Headquarters
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NCTV	National Coordinator Terrorisme en Veiligheid
NIS Regulations	Network and Information Systems Regulations
NPSA	National Proactive Security Authority
UK	United Kingdom
WBNI	The network and information systems security act

List of tables & figures

1. Introduction

Cybercrime. This is a definition that has unfortunately worked its way into our society over the past decades. Cybercrime is becoming an increasing threat to a lot of countries in the world. But what is cybercrime? Even though this has become a familiar term for a lot of people and organizations, there is still discussion about the exact definition of cybercrime. (Phillips, K., Davidson, C.K., Farr, R.R., Burkhardt, C., Caneppele, S., & Aiken, P.K. 2022). Since a separate thesis could be written about the entire concept of cybercrime, it will be very simply and shortly stated here. According to the Cambridge dictionary, cybercrime means the following: "crime or illegal activity that is done using the internet." (The Cambridge Business Dictionary). Since cybercrime can be described as all crime that is committed using or targeting a computer with the internet, it is a very broad definition. It includes crimes like hacking, phishing, and online fraud. (Phillips, K., Davidson, C.K., Farr, R.R., Burkhardt, C., Caneppele, S., & Aiken, P.K. 2022).

In the Netherlands, 16.9 percent of the inhabitants fell victim to cybercrime in the year 2021. This is approximately the same number of inhabitants that fell victim to traditional crime, like theft, violence, and burglary in that same year. (Centraal Bureau voor Statistiek, 2021). This is not very different in the United Kingdom since almost ten percent of the inhabitants of the UK that were older than fifteen were a victim of cyber fraud and scams in 2020. (Office for national statistics, 2020). Because cybercrime is a growing issue that needs to be addressed in the society of today in the Netherlands and the United Kingdom, both countries have formed and implemented different regulations, policies and strategies to prevent cybercrime. This forms the system of cybersecurity that is present in a country. (Asghar, M. Z., & Chen, D, 2019). Cybersecurity can be defined as: "Things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet". (The Cambridge Business Dictionary).

One of the main governmental instruments in the cybersecurity system for both the UK and the Netherlands are the National Cyber Security Strategies. Both these strategies contain a vision about the ideal position in cyberspace which are to be achieved by objectives and goals that are described in the strategies. The objectives and goals in the strategy from the UK and the Netherlands differ, but both include information on how to strengthen and implement certain elements of cybersecurity in order to realize the goals that are set out in the strategy. (National Cyber Strategy UK, 2022), (Nederlandse Cybersecuritystrategie 2022-2028). This study focuses on how these strategies aim to influence cybersecurity, it compares the two strategies, and it analyses their differences and similarities. There is a knowledge gap concerning this specific focus because it is still unclear how national cybersecurity strategies actually effect cybercrime and which national strategies work better than others. Even though this study does not specifically focus on the effect of the national cybersecurity strategies, it does compare two of these strategies of highly developed countries and explains the differences. Therefore this study aims to conclude what these strategies can learn from each other, which could be used in the development of future national cybersecurity strategies.

Even though there are a few previous comparisons of national cybersecurity strategies of countries around the world, in which this study can be mostly compared to the study of Luiijf, H.A.M., Besseling, K., Spoelstra, M., Graaf.d.P from 2011, (Ten National Cyber Security Strategies: A Comparison) and the study of Shafqat, N., Masood, A., from 2016, (Comparative Analysis of Various National Cyber Security Strategies), this study distinguishes itself because of a couple of reasons. This thesis creates scientific relevance since it is an in-depth investigation on the cybersecurity strategies of these specific two countries as well as an investigation of the newest versions of these strategies which has not been studied in this way before. This study combines a methodological comparison with societal relevance by finding and combining the differences and similarities with societal activities and issues. The explanation of this relation can be used when there is a will to change a certain aspect of the cybersecurity. In this thesis, a coding strategy is used to analyze the national cybersecurity strategies, which has not been done in a previous study as a way to draw conclusions about such a strategy. The aim of this particular method is to discover possible unexpected insights that can add to the state of the art in research about national cybersecurity strategies.

The choice of comparing the national cybersecurity strategies of these countries specifically is based on multiple aspects. The Netherlands and the United Kingdom are both developed countries with a very high Human Development Index. (Human Development Index, 2022). The UK and the Netherlands also share a very high score on the Global Cyber Security Index from 2020, which means they are evaluated as countries with a high cybersecurity. (Global Cybersecurity Index, 2020). However, the Netherlands is part of the European Union which has its own cybersecurity policies, and the United Kingdom is, since the Brexit, not a member of the EU, which could possibly lead to different cybersecurity systems. (Walden, I., Michels, J, D, 2021). These aspects contributed to the interest of finding out what differences and similarities there would be between the two strategies and why. Another reason for the choice of these two strategies is that they are both published in 2022, this is helpful in the comparison because cybersecurity is a constantly evolving aspect that cannot be compared over a large timeframe because of the many developments in the meantime. (Phillips, K., Davidson, C.K., Farr, R.R., Burkhardt, C., Caneppele, S., & Aiken, P.K. 2022).

1.1 Research questions and sub-questions

In order to investigate cybersecurity and the national cybersecurity strategies in the UK and the Netherlands, this study addresses the following research question*: ''How do the national cybersecurity strategies aim to influence the cybersecurity in the Netherlands and the United Kingdom? ''*

To tackle this question, there are four sub-questions that will be explained in order to add clarification on certain aspects of the research question. These sub-questions are listed and briefly explained below.

1. *Which governmental institutions and policies are involved in the cybersecurity system in the United Kingdom and the Netherlands?*

This sub-question provides insights into the national system of cybersecurity in the UK and the Netherlands. It explains what the main institutions and organizations involving cybersecurity are and their functions. It also elaborates on what policies and regulations are involved in the cybersecurity in the UK and the Netherlands.

2. *What are the main focuses and goals of the National Cyber Security Strategies of the United Kingdom and the Netherlands?*

This sub-question gives a deeper understanding of the national cybersecurity strategies in terms of their goals and focuses and what they want to achieve with the strategy. This is done by examining the strategies themselves and performing a textual coding analysis.

3. *What are the main differences between the National Cyber Security Strategies of the United Kingdom and the Netherlands?*

This sub-question explains what differences there are between the NCSS of the UK and the NCSS of the Netherlands using the information from sub-question 2 and the textual coding analysis to identify possible differences between the strategies.

4. *Why do the National Cyber Security Strategies of the United Kingdom and the Netherlands show differences and similarities?*

The last sub-question tries to provide a clear answer to why the differences as stated in sub-question 3 and the similarities between the strategies occur. This will use information about influences on cybersecurity as described in the theory and data from interviews with experts in cybersecurity.

This thesis contains information about the governmental institutions and policies that are involved in cybersecurity in the UK and the Netherlands. The theory of this study gives further details about what factors influence the cybersecurity in the UK and the Netherlands. In the methods chapter is explained how the comparative cross-national research design is used in combination with the textual coding analysis and interviews with cybersecurity experts. Furthermore, the analysis chapter gives an answer to the sub-questions by using the data and the conclusion provides an answer to the main research question.

2. Background Information

This chapter provides information on governmental institutions and policies in the UK and the Netherlands which is derived from relevant literature.

2.1. Governmental institutions and policies in the United Kingdom

Institutions:

In order to protect its citizens from digital threats, the government of the UK organizes the cybersecurity through a couple of governmental institutions. The National Cyber Security Centre (NCSC) is a central organization in cybersecurity in the UK and is part of the governments communication headquarters (GCHQ). (National Cyber Security Centre UK, 2023). The NCSC of the UK supports the main critical governmental organizations, the industry sector, and the general public in the UK in the form of cybercrime protection. (National Cyber Security Centre UK, 2023). When an incident of cybercrime occurs, the NCSC can help with the recovery and the minimization of the effects of this incident. The NCSC can also show organizations how to learn from cyber incidents to support their cybersecurity in the future. The national cybersecurity strategy from the UK shows the intentions of the government with founding the NCSC. (Crick, T., Davenport, J.H., Irons, A. & Prickett, T. 2019).

A partner from the NCSC that is also very important for the cybersecurity in the UK is the National Crime Agency (NCA). (National Crime Agency, 2023). This Agency focuses on multiple forms of organized and serious crime in the UK, including cybercrime. The National Crime Agency focuses in the field of cybercrime on creating a better law enforcement and resilience to cybercrimes. The NCA closely works together with the FBI, the police, and other units in the United Kingdom to combine knowledge about cybersecurity. (National Crime Agency, 2023). Another close partner of the NCSC is the National Proactive Security Authority (NPSA). This organization has the responsibility to provide national security and to increase the knowledge on how to counter state threats and terrorism. The NPSA works with different partners like businesses, security experts, and the government, in order to identify weaknesses and risks in the national cyberinfrastructure and provides advice on how to reduce those risks. (National Protective Security Authority, 2023).

Policies and regulations:

In the UK, there is not one coherent legislation or law for dealing with cybercrime. Instead, there are multiple laws that create the framework for the cybersecurity and the action against cybercrime. (Porcedda, M.G. 2023). There are a couple of laws and legislations that are normally used when an incident of cybercrime occurs, which are explained below. However, it is helpful to know that in a lot of cases where cybercrime is involved, there are also laws applicable that aren’t directly digitally focused. For example, a cybercrime that uses hacking for financial benefit can also be regulated under the Theft Act from 1968. (Lukings, M., Lashkari, A.H. 2022).

- The Computer Misuse Act (CMA)

The main legislation for malicious actors and individuals is the CMA. (The Crown Prosecution Service, 2020). The CMA prohibits unauthorized access to data and computer systems as well as their destruction or damage. Its purpose is to safeguard the security and integrity of data and computer systems by criminalizing any unauthorized access that has not been sanctioned by the owner of this data or computer system. (GOV.UK, 2023).

- The Data Protection Act (DPA)

Another legislation in the field of cybersecurity is the DPA from 2018. The DPA controls how and if data is used by the government, businesses, and organizations of the UK. The DPA is derived from the General Data Protection Regulation which was established by the European Union. The DPA also secures the rights of people regarding the kind of information the government or other organizations possess about them. (GOV.UK, 2018a).

- The Security of Network and Information Systems Regulations (NIS Regulations)

The NIS Regulations are also an important legislation in the prevention of cybercrime. This policy offers legal mechanisms aimed at increasing the security level, including cyber flexibility of the information systems in the UK that take care of online and essential services. (GOV.UK, 2018b).

2.2. Governmental institutions and policies in the NL

Institutions

The government of the Netherlands also undertakes action to prevent cybercrime within the country, in which the National Cybersecurity Center (NCSC) of the Netherlands plays a big role. The National cybersecurity centers of the UK and the Netherlands do not only share its name but are also similar in their functions. The NCSC of the Netherlands is an individual organization that has the responsibility to oversee the cybersecurity in the Netherlands. The goal of the NCSC is to increase the resilience of the Dutch society in the digital domain and to create a safe and stable information society. (Nationaal Cyber Security Centrum, 2023). The NCSC of the Netherlands used to be part of the National coordinator for terrorism and security (NCTV), but a few years ago the Dutch government separated them. However, these two organizations remain close partners since a good cooperation between the NCSC and the NCTV is vital to the cybersecurity of the Netherlands. (Kamara, I., Leenes, R., Stuurman, K., Boom, v.d. J, 2020). Another big institution that is involved in the cybersecurity in the Netherlands is the AIVD (Algemene Inlichtingen- en Veiligheidsdienst). This is the general intelligence and national security organization that addresses different forms of threats in the Netherlands. The cyber threats that are relevant for the AIVD are the national security threats posed by state actors. (General Intelligence and security service, 2023). The AIVD focuses on informing the government and other stakeholders about possible cyber risks and threats in order for them to take relevant measures in time. (General Intelligence and security service, 2023). The MIVD is the 'sister' organization of the AIVD, which delivers services and security information on different kinds of threats, including cyber threats, to the ministry of Defense and the army forces. (Militaire Inlichtingen- en Veiligheidsdienst, MIVD, 2023). The NCSC, the AIVD, the MIVD, the NCTV, the Dutch police, and other smaller organizations shape the framework for the national cybersecurity of the Netherlands.

Policies and regulations

The Netherlands has multiple policies and regulations around the topic of cybercrime. Some of the most influential policies in cybersecurity are explained below. However, just like in the UK, cases of cybercrime are also often assessed under another, more regular law. (Kamara, I., Leenes, R., Stuurman, K., Boom, v.d. J, 2020).

- The Network and Information Systems Security Act (WBNI), and the Network and Information Systems Security Decree. (BBNI)

Alongside the Dutch policies, the Netherlands must also comply with the European cyber policies agreements. The WBNI from 2018 implemented the European influences in the law of the Netherlands. This law states that organizations that provide digital or essential services must protect themselves against possible cyber threats and must report cyber incidents when they occur. (Ministerie van economische zaken en klimaat, n.d). With the implementation of the WBNI, the government decided to also implement the BBNI. The BBNI provides a clarification of some aspects of the WBNI, like which organizations are essential in the Netherlands and how the reporting of cyber incidents should be handled. (Kamara, I., Leenes, R., Stuurman, K., Boom, v.d. J, 2020).

- Article of law on computer intrusion (Wetsartikel computervredebreuk)

Another law of the Netherlands concerning cybercrime is the "Wetsartikel computervredebreuk". This law prohibits hacking in the Netherlands. (Openbaar ministerie, 1993).

- The Dutch Telecommunications Act

The Dutch Telecommunications Act also impacts the cybercrime. This law sets certain obligations towards companies that provide digital internet and phone services involving the commercialization, protection of privacy, and other operational obligations. (Wettenbank, 2023).

Overall, the UK and the Netherlands count a lot different institutions and laws that influence the cybersecurity in the nations.

3. Theoretical Framework

This chapter contains relevant theory for answering the sub-questions and the research question derived from academic literature.

3.1. Factors that are of influence on cybersecurity

Cybercrime threats

How the cybersecurity in the Netherlands and the United Kingdom is structured is based on what kind of cyber threats these countries face. Therefore it is important to understand which threats the United Kingdom and the Netherlands face. The more cybercrime, the better the motivation for good cybersecurity. And the better the cybersecurity, the harder it is for cyber criminals to commit a cybercrime. (Lukings, M., Lashkari, A.H. 2022). Because of this intermingled relationship between cybersecurity and cybercrime in a country, it is important to provide an understanding of which cybercrimes often occur in the UK and the Netherlands.

United Kingdom

In the United Kingdom, the biggest threats for citizens and businesses, are phishing and hacking, according to the annual review on cybercrime of the National Cyber Security Centre from 2022. (National Cyber Security Centre, 2022). Hacking can be done in many different ways and is about intentionally or unlawfully entering an automated work. (Oerlemans, J.J., & Wagen, v.d.W, 2020). Phishing on the other hand can be described as a type of cybercrime in which the victim is approached via the computer, phone, or other digital devices by someone pretending to be part of a certain institution or company with the purpose to lure the victims into giving up personal data, often for financial benefit. (Lukings, M., Lashkari, A.H. 2022). In the 12 months before March 2022, only the phishing and hacking related cybercrime, already occurred in 2.7 million incidents. (NCSC Annual Review 2022). For the national security of the United Kingdom, the main threats are evolving state threats from other countries, especially threats from Russia and China. (NCSC Annual Review 2022).

Netherlands

One of main threats to the national security of the Netherlands are also cyberattacks by other state actors, including Russia and China. (Akkermans, M., Kloosterman, R., Moons, E., Reep, C., Tummers-van der, M., 2022). For the citizen, businesses, and small organizations in the Netherlands, the main cyber threats are phishing and hacking, just like in the United Kingdom. (Nationaal Coordinator terrorismebestrijding en veiligheid, 2022). Aside from the threats to the national security by state actors, threats from cybercriminals are also dangerous for the national security. However, they are hard to distinguish due to mutual relationships.

Cyber threats by state actors have increased over the years and can, according to the Cybersecuritybeeld, be seen as the ‘new normal’. (Nationaal Coordinator terrorismebestrijding en veiligheid, 2022).

It is difficult to exactly assess the impact of certain threats of cybercrime on the cybersecurity in the United Kingdom and the Netherlands. This is because of the many other factors that also influence cybersecurity and the fact that cyber threats and cybersecurity over the past decade constantly evolved and adapted which makes it difficult to measure the effectiveness over a longer period of time. (Asghar, M. Z., & Chen, D. 2019).

Interconnected elements of cybersecurity

In order for a society to function smoothly in these technological times, a good cybersecurity system is crucial. It is an impossible quest to make a society one hundred percent digitally safe, there is always a possibility of failure due to human or technological errors. (Nationaal Coordinator terrorismebestrijding en veiligheid, 2022). But both the UK and the Netherlands are currently in the process of trying to make their country as digitally safe as possible. As described in the previous section, the types of cyber threats that a country faces are important influences in the cybersecurity in a country. However, there are a lot more factors that can influence the cybersecurity, some with a small contribution and some with a large contribution to cybersecurity. The following elements that will be explained influence the system of cybersecurity.

- Governmental organizations and policies

Cybercrime and cybersecurity share a complex relationship and both influence each other. Since the government tries to regulate cybercrime with institutions, legislations, and policies, the cybersecurity in a country is also affected by which policies, laws, and implementation and interpretation of these policies and laws are maintained by the government. (Mishraa, A., Alzoubi, I.Y., Anwar, M.J., Gill, A.Q., 2022). Cyber institutions and policies are essential for organizations in order to ensure their cybersecurity. This is for example because a legislation for cybersecurity protects the data of these organizations. (Lukings, M., Lashkari, A.H. 2022).

- Education in cybersecurity

Cybersecurity is a crucial part of a safe society. However, not everyone understands the importance of it. The awareness of cybersecurity has substantial impact on the national cybersecurity in a country. A study by Emilia N. Mwim and Jabu Mtsweni defined the education and training of cybersecurity as a dominant factor in shaping the cybersecurity culture. The study states that it is important for organizations, businesses, and the governance of a society to be provided with the appropriate education and training to increase the knowledge about cybersecurity and the cybersecurity itself. (Mwim, E.M., Mtsweni, J., 2020). By creating more cybersecurity awareness through education, the number of cybersecurity incidents, or cyber accidents that are caused by people, can be reduced. (Casanove, de, O., Leleu, N., Sèdes, F, 2022).

- Technological infrastructure

Technological development is an important concept in today’s society. Because of the evolving digital technology, cybercrime in the world has increased a lot. However, a country can also benefit from its technological developments since it can provide methods to improve the national security. A technological advantage for a country in comparison to its attackers is very helpful because it can lead to a safer cybersecurity. (Johnson, R. 2022). As cyberspace is an entirely technological environment in a country, the matter of cybersecurity is closely connected to its advancement and utilization. Therefore, a country’s technological infrastructure and technological resources influence the cybersecurity. (Cavelty,M, D., Wenger, A. 2020).

- Financial factors

The economic status of a country also defines aspects of the cybersecurity. More developed, stronger economies usually also have a strong cybersecurity. (Merlevede, J., Johnson, B., Grossklags, J., Holvoet, T, 2020). These countries can invest more in technological resources, cyber experts, and in more comprehensive cyber measures than weaker economies. Weaker economies are more likely to struggle with these aspects, which can make them more vulnerable to digital threats. (Global Cybersecurity Index, 2020). Another element that is influenced by economic factors, is the motivation of actors for cyber-attacks. In states that are economically more developed is usually also more to gain for cybercriminals. Overall, the economy can have a significant impact on the state of the cybersecurity in a country. (Global Cybersecurity Index, 2020).

- The human factor

In the field of cybersecurity, humans are regularly considered the weakest aspect. A lot of the big cyber incidents are a result of human errors, often without the intention to do harm. But the human aspect is still often ignored or not given enough attention. (Rahman, T., Rohan, R., Pal, D., Kanthamanon, P, 2021). To fully understand how human factors influence the cybersecurity, innovative strategies on the complexity of human factors are required. However, the research on factors in the cybersecurity right now is still dominated by technology. To prevent this from happening, a study by Jeong, J, J., Mihelcic, J., Oliver, G. and Rudolph, C suggested that if future research focuses on studying cybersecurity with an interdisciplinary view and focus on the consolidation of human factors, that human factors are better understood and human errors are more likely to be prevented. (Jeong, J, J., Mihelcic, J., Oliver, G. and Rudolph, 2019).

- European Union

In the case of the Netherlands, there is another factor that influences the cybersecurity, which is the European Union. In the EU are several policies, laws, and organizations that are set up to improve the cybersecurity in the member states. An example of such a law is de General Data Protection Regulation, which sets rules about data protection. The GDPR had a big impact in the Netherlands because all the Dutch organizations needed to comply with this law when it was implemented. (European Commission, 2018). The EU also established multiple organizations to help the cybersecurity which the Netherlands can profit from. An example is ENISA, which provides technical support on the cybersecurity to the member states when necessary. (The European Union Agency for Cybersecurity, 2019). Overall, the European Union has a big international influence on cybersecurity and the politics of cybersecurity. (Walden, I., Michels, J, D, 2021).

To sum up what has been stated so far, in regard to influences on cybersecurity, there are three main sources of influences that are identified in this chapter which are visible in Table 1. The first one is threats of cybercrime and the second one are elements that are of influence on cybersecurity. The third influence source is the institutions and policies that are involved in cybersecurity which is also shortly mentioned as an element and can play a big role in the cybersecurity. However, which institutions and policies are involved are not specifically mentioned in Table 1, but are described in more detail in Chapter 2.

Table 1: Influences on cybersecurity derived from literature

Influences		Source
Cyber threats		
	Phishing & Hacking	(Oerlemans, J.J., & Wagen, v.d.W, 2020), (Lukings, M., Lashkari, A.H. 2022), (NCSC Annual Review 2022), (Akkermans, M., Kloosterman, R., Moons, E., Reep, C., Tummers-van der, M., 2022), (Nationaal Coordinator terrorismebestrijding en veiligheid, 2022).
	Threats from state actors	(NCSC Annual Review 2022), (Nationaal Coordinator terrorismebestrijding en veiligheid, 2022).

Elements		
	Governmental policies and procedures	(Mishraa, A., Alzoubi, I.Y., Anwar, M.J., Gill, A.Q., 2022), (Lukings, M., Lashkari, A.H. 2022).
	Education in cybersecurity	(Mwim, E.M., Mtsweni, J., (2020), (Casanove, de, O., Leleu, N., Sèdes, F, 2022).
	Technological infrastructure	(Johnson, R. 2022), (Cavelty,M, D., Wenger, A. 2020).
	Financial factors	(Merlevede, J., Johnson, B., Grossklags, J., Holvoet, T, 2020), (Global Cybersecurity Index, 2020).
	The human factor	(Rahman, T., Rohan, R., Pal, D., Kanthamanon, P, 2021), (Jeong, J, J., Mihelcic, J., Oliver, G. and Rudolph, 2019).
	European Union	(European Commission, 2018), (The European Union Agency for Cybersecurity, 2019), (Walden, I., Michels, J, D, 2021).

4. Methods

This chapter explains how this study is conducted with the purpose that it can be reproduced. It described the research approach, the method of data collection, and the method of data analysis.

4.1 Description of the research approach

In order to be able to provide an answer to the research question of this study, the research design that is used is a comparative cross-national design. The reason for the choice of this research design is because it can provide a clear overview of the focuses of both the national cybersecurity strategies and this design can show the differences and similarities between the two strategies which is helpful in answering the sub-questions.

In order to work with the two national cybersecurity strategies, this thesis uses a textual analysis. A coding scheme from the textual analysis of the two national cybersecurity strategies is made to gain better insights in the strategies and their main focuses and aims. There will be a separate coding scheme for both the strategy of the United Kingdom and the Netherlands which will be used in the data analysis. Because of the comparative cross-national research design in combination with a textual analysis, this thesis is able to provide an in-depth research on the national cybersecurity strategies.

4.2 Method of data collection

The thesis is a qualitative study and the data collection consists of three main types of resources. The first is the data from the two national cybersecurity strategies of the UK and the Netherlands directly, which are open-source policy documents that are freely available. The content of these documents is used as an information source and is analyzed with a textual analysis in Atlas.ti. The NCSS from the UK is called: "National Cyber Strategy 2022, Pioneering a cyber future with the whole of the UK", and is published in 2022. (National Cyber Strategy UK, 2022). The NCSS of the Netherlands is called: "Nederlandse Cybersecuritystrategie 2022-2028, Ambities en acties voor een digitaal veilige samenleving", and is also published in 2022. (Nederlandse Cybersecuritystrategie, 2022). These strategies are reliable sources set up by a combination of governmental organizations that show the vision of the UK and the Netherlands on the approach of cybersecurity in the upcoming years. (National Cyber Strategy UK, 2022), (Nederlandse Cybersecuritystrategie, 2022).

The second main type of data is relevant literature, which includes academic and scientific articles and policy documents which are all found on the internet and are open-source articles or documents. The third source of data is gathered through interviews. There are three interviews conducted with cybersecurity experts who have knowledge about the national cybersecurity strategy and the overall cybersecurity in the UK or the Netherlands.

Interviewee number 1 is an expert on cybersecurity in the UK, the second interviewee is an expert on cybersecurity in the EU and the Netherlands and the last interviewee is an expert on cybersecurity in the Netherlands. The data from these interviews is used in the analysis to confirm or check the findings and to know what the experiences of these experts are regarding the cybersecurity to gather relevant information.

4.3 Method of data analysis

The method of data analysis that is used in this thesis is a content document analysis. This method focuses on the content of the written text in documents, which in this case are the national strategies and the interview transcripts. The purpose of a content analysis is to categorize the written words into clusters with the same aim or conceptual category in order to discover relationships, differences, and similarities between themes or variables in the national strategies and the interviews. In order to do the content analysis, coding schemes will be provided for the analysis of the strategies and the interviews. There are two separate coding schemes for the NCSS of the UK and the NCSS of the Netherlands which give an overview of the main aims and focuses in the strategies. The tool that is used to perform the content analysis is Atlas.ti. This is a qualitative research tool that can be used to divide large qualitative data sets into codes, categories, and folders, which can create measurable or observable data from the national strategy documents.

The codes in these coding schemes are a description of what a certain part of textual data is about and the codes themselves are not specifically used in the analysis. Each code is placed in one aim category and one focus category. The aim and focus categories are formed with the goal to provide an answer to the research question and the aim categories are chosen by combining the main goals of the NCSS of the UK and the NCSS of the Netherlands.

The aim categories describe the different goals that a code attributes to that want to be achieved in the strategy. The aim categories also have a category named ‘independent codes’ which includes all the codes that do not specifically state an aim or goal. In the figures of the analysis of this study, the aim categories will be referred to by the keywords as stated in the brackets behind the aims in Table 2 to provide a more comprehensive overview. The focus categories are formed by looking at how the strategies state to implement and handle these goals. The focus categories also include some regular aspects, like vision, threats, and independent codes.

Table 2 shows what aim and focus categories the coding schemes of the strategies used to qualify the codes in. In this process of determining the aim and focus category is looked into detail at how the code is described and which aim and focus is most applicable to the code. The analysis uses the aim categories and the focus categories that the codes are in by analyzing the number of times a certain goal or topic is mentioned (so the number of codes), which can provide information on how important the strategy deems that topic to be.

Table 2: Aim categories and focus categories in the coding schemes of the national cybersecurity strategies of the UK and the Netherlands

Aim category	***Focus category***
Expanding the nation's cyber skills and meeting the demand in CS experts (1. Cyber,- skills and experts)	Continuing with good measures/aspects of CS
Improvement in education in CS. (2. Education)	Creating new measures/aspects/regulations in CS
Improving to detect and disrupt state, criminal and other malicious cyber actors. (3. Detect and disrupt)	Cyber threats
Increasing the cyber resilience. (4. Cyber resilience)	Improving measures/aspects of CS
Increasing the safety of digital products and services. (5. Products and services)	Independent codes
Organizations and businesses can deal with and understand cyber threats and risks. (6. Organizations and businesses)	Institutions and organizations
Shaping global governance and securing the international advantage in CS technologies. (7. Global governance and technology)	Investing in a measure/ aspect of CS
Strengthening the structures, partnerships and networks in CS. (8. Structures and networks)	Recommendations for the future
The government and its institutions understand and can handle cyber threats. (9. Government and institutions)	Vision
The public is well protected against cyber risks. (10. Public)	
Independant codes. (11. Independent)	

The full content of both the national cybersecurity strategies is coded except for the foreword, the table of contents, and the appendixes. In the coding schemes are the words cybersecurity and cybercrime visible as; 'CS' and 'CC', to provide a more comprehensive coding scheme. The coding schemes are available in the data appendix at the end of this thesis.

The interviews will also be used in the data analysis and are semi-structured which means that there was a list of questions for the interview set up beforehand, however, the questions are sometimes a little adapted depending on the answers of the interviewees. The transcripts from the interviews are also coded in Atlas.ti. Most of the codes are content-based and provide the function of summarizing the answers of the interviewees. However, some of the data from the interviewees is coded in ViVo in the form of a quotation. The codes from the interviews are divided into categories which are formulated based on providing answers to the sub-questions. The codes are further categorized in terms of which interviewee said what code. The coding scheme with the categories and the codes from the interview is available in the data appendix at the end of this thesis.

Based on the coding of the strategies, the coding of the interviews, and the information from the gathered scientific articles and policy documents, the data analysis is formed to answer the sub-questions and the research question.

5. Data Analysis

This chapter analyses the theory, the strategies, and the interviews in order to answer the sub-questions.

5.1 Which governmental institutions and policies are involved in the cybersecurity system in the UK and the Netherlands?

To form an answer to this descriptive question, the theory from the chapter: 'Background information' of this study is analyzed. In combination with the theory and the data from the interviews about institutions and policies, an answer to this question is formed.

For the institutions in the UK, the National Cyber Security Centre, the National Crime Agency and the National Protective Security Authority are, as described in Chapter 2, the main institutions in the cybersecurity in the UK. The NCSC is part of the Government Communications Headquarters and collaborates with the NCA and the NPSA, which partner with the police, businesses, the government, and other actors. The NCSS of the UK points out the importance of the National Cyber Force, which is responsible for countering, disrupting, and degrading possible dangerous actors for the national security. (National Cyber Strategy UK, 2022). The cybersecurity system is complex and is defined by a lot of big and small institutions, government departments, police teams, legislations systems, and more. However, the mentioned institutions can be considered as the main institutions and organizations involved in the cybersecurity of the UK.

In the Netherlands, just like in the UK, a crucial institution in cybersecurity is the National Cyber Security Centre, which falls under the supervision of the Nationaal Coordinator Terrorisme en Veiligheid (NCTV) in the Netherlands. The NCSC in the Netherlands has a lot in common with the NCSC of the UK in terms of functions and responsibilities. As stated in Chapter 2, the NCSC works together with the AIVD and the MIVD. The NCTV, the NCSC, the AIVD, and the MIVD together with the Dutch police forces and other smaller cyber organizations and government departments form the cybersecurity framework of the Netherlands. However, the cyber ecosystem is, just like in the UK, very complex and is defined by more factors than only these main institutions.

So, it is clear that the mentioned institutions are involved in the cybersecurity in the UK and the Netherlands. However, it is difficult to assess exactly what kind of role they play within the cybersecurity. One of the reasons for this was mentioned by interviewee number 1. The code from this part of the interview is named: "Difficult to specifically assess the role of the NCSC because they keep a lot of their information private". (Interview 1, lines 120-126). With this code, the interviewee tried to explain that a lot of the actions, plans, and other information of the NCSC from the UK and other organizations in cybersecurity is not publicly available.

Therefore, it is difficult to know what these institutions are all doing because it can be assumed that not all the information that should be considered is provided.

In order to know which policies are involved in cybersecurity, again is referred to Chapter 2 where the major policies concerning cybercrime in the UK and the Netherlands are listed. In the UK are different policies applicable to different types of cybercrime. The main legislations to fight cybercrime are the Computer Misuse Act, the Data Protection Act, and The Security of Network and Information Systems Regulations. The Netherlands also has multiple policies around cybersecurity. But unlike the UK, the Netherlands must also comply with the European Union cyber policies, alongside the Dutch policies. Important laws of the Netherlands concerning cybercrime are the “Wetsartikel computervredebreuk” , the Dutch Telecommunications Act, the WBNI, and the BBNI.

These policies of the UK and the Netherlands are specifically considering cybercrime, but as stated in Chapter two and three, in reality a lot of cases of cybercrime are often judged under another, more general law. This is because a lot of crimes include a digital aspect, but are considered for example as fraud or theft and therefore not specifically addresses as cybercrime in the justice system. Therefore, it is difficult to know which policies are all involved in cybersecurity, because next to the obvious policies in cybersecurity, there are also a lot of other general policies used in cases of cybercrime.

Another difficulty concerning policies about cybercrime is mentioned by interviewee 3. This quotation shows how the interviewee stated this difficulty as a question.

> “How we can best deal with hackers in countries where Dutch law has no reach?” - Interviewee Number 3, lines 331-332.

With this, the interviewee meant that cybercrime often crosses national borders. This makes it difficult for Dutch (and Englisch) policies to reach criminals that operate from other states. Therefore, other international regulations, policies, or agreements about cybersecurity are also involved in the cybersecurity of the UK and the Netherlands.

5.2 What are the main focuses and goals of the National Cyber Security Strategies of the United Kingdom and the Netherlands?

In order to answer this question, the qualitative data from the NCSS of the UK and the NCSS of the Netherlands is used, as well as the data from the coding schemes in the aim categories. This sub-question has been considered in multiple ways. Primarily, the strategies of the UK and the Netherlands themselves describe what kind of goals they want to achieve and how they plan to reach these goals. Furthermore, this section also analyses what kind of goals and focuses are derived from the coding schemes to see if there are underlying focuses or relationships.

Data from Strategies

First of all, the strategy of the United Kingdom has five pillars which contain the main aims and focuses of the strategy. The first pillar is named: “Strengthening the UK cyber ecosystem”. This pillar consists of three objectives in which is described that the UK should ensure that the networks, partnerships, and people in the UK are diverse enough in terms of cybersecurity knowledge. This pillar also explains how to ensure the growth of the IT/cyber, including the expansion of education in cyber skills in order to improve the expertise in cybersecurity in the future. (National Cyber Strategy UK, 2022). The second pillar is named: “Building a resilient and prosperous digital UK”. This pillar also has three objectives which describe that the understanding of cyber threats and the effects of cybercrime should be improved in order to ensure a more effective approach regarding cybersecurity. Overall, it describes how the cyber resilience should be optimized in terms of preparations, response, and recovery in the case of cybercrime. (National Cyber Strategy UK, 2022).

“Taking the lead in the technologies vital to cyber power”, is the third pillar of the NCSS of the UK. This pillar has four objectives that are all focused on creating a technological advantage towards attacking actors. It describes how to improve the use of new technological developments and how to secure a well-functioning technology sector in the upcoming years. (National Cyber Strategy UK, 2022). The fourth pillar is named: “Advancing UK global leadership and influence for a more secure, prosperous and open international order.” This pillar has three different objectives which focus on shaping and improving global governance to promote a safe and peaceful international cyberspace. This pillar describes how the UK should improve its strategic advantage regarding cybersecurity and promote the national interest of the UK. (National Cyber Strategy UK, 2022). The fifth and last pillar of the NCSS from the UK is named: “Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace”. This pillar states that the UK should focus on the detection and investigation of cybercrime and should share information between organizations to protect the UK and its citizens. (National Cyber Strategy UK, 2022).

The NCSS of the Netherlands has four different pillars that describe the main aims. The first pillar in the NCSS of the Netherlands is called: “Digital resilience of government, businesses and civil society organizations”. This pillar focuses on using multiple measures of preventing cybercrime to improve the ability of the Netherlands to minimize cyber risks and create better resilience. (Nederlandse Cybersecuritystrategie, 2022). The second pillar is named: “Safe and innovative digital products and services”. This second pillar of the NCSS outlines that the Netherlands should focus on improving cybersecurity expertise, innovation, and development. Doing this with a focus on consumers and suppliers of technological and digital products will improve the cybersecurity in the Netherlands. (Nederlandse Cybersecuritystrategie, 2022).

The third pillar is: “Countering cyber threats posed by states and criminals”. This pillar focuses on the strategies employed at both the domestic and global level to counter potential harmful actors and obtain a better understanding of the overall cybersecurity situation, which serves as a foundation for taking necessary measures. The government holds a distinct obligation in this area and has access to various tools to confront cyber threats. (Nederlandse Cybersecuritystrategie, 2022). The fourth pillar is named: “Cybersecurity labor market, education and the public cyber resilience”. The primary focus of this pillar is on the people who utilize technology and the ability of the public to withstand cyber threats. It states that Dutch society has a significant part to contribute in terms of enhancing digital literacy, ranging from fundamental comprehension and abilities to advanced expertise and specialized skills in cybersecurity. (Nederlandse Cybersecuritystrategie, 2022).

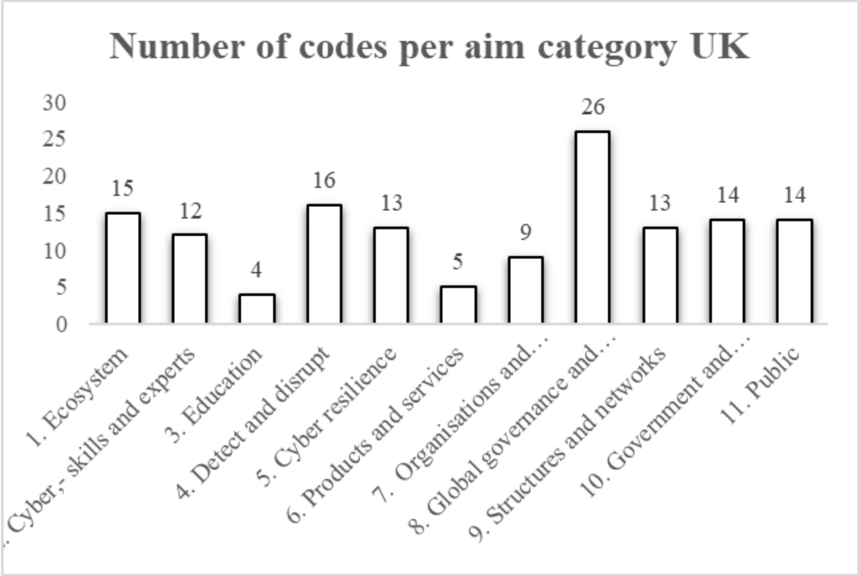
Data from the Coding scheme

The coding scheme analysis provides additional information about the goals and focuses of the strategies. The strategies of the Netherlands and the UK are coded with the same aim categories and this resulted in a certain number of codes per aim. The number of codes indicates how many details, actions, or other aspects of that aim are described in the text of the strategy, so the more codes, the more focus is given to a certain aim. The aims are listed in Table 2 in the previous Chapter, and will be referred to in the keywords and numbers in the figures of this chapter.

The number of codes per aim category, except for the category ‘independent codes’, is visible in Figure 1 for the NCSS of the UK and in Figure 2 for the NCSS of the Netherlands. As visible in the figures, each aim category has multiple codes, meaning that each aim is discussed in the strategies of both countries. All the goals that are discussed in the strategies are combined into the aim categories, and because all the aim categories contain multiple codes, these aims can be seen as the main goals that the NCSS from the UK and the NCSS from the Netherlands address.

However, the aim categories did not receive the same amount of codes. In the coding of the strategy from the UK, one aim has distinctively more codes than the other aims, which is number 8; ‘Shaping global governance and securing the international advantage in cybersecurity technologies’. A lot of details, visions, and implementation plans etc. are discussed about this aim, which resulted in a large number of codes. On the other hand, the aim categories 3 and 5; ‘Improvement in education in cybersecurity’, and ‘Increasing the cyber resilience’ contain less codes than most of the other aims, so the NCSS from the UK places less focus on these aims than on the other main aims. Overall, under the eleven goals that are already defined as ‘main’ goals, the goal that the strategy of the UK places the most focus on is “Shaping global governance and securing the international advantage in cybersecurity technologies”.

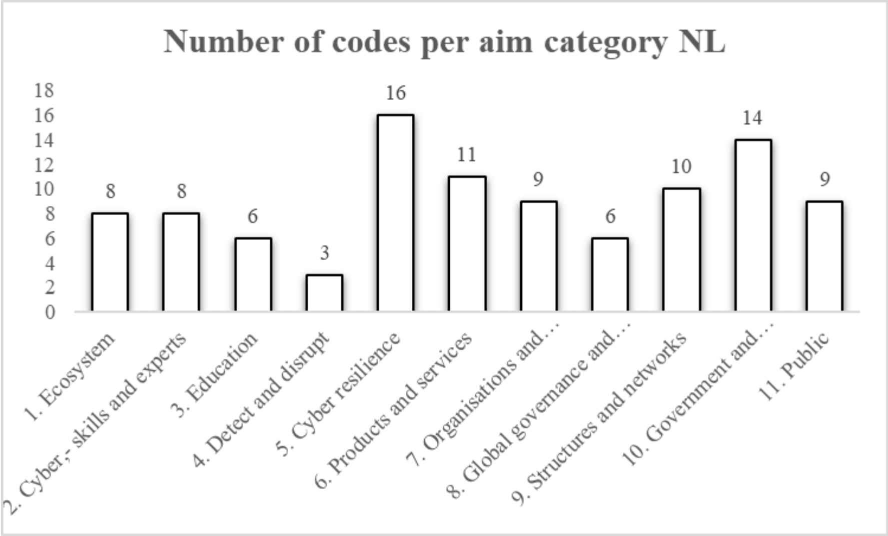
Figure 1: Number of codes per aim category in the NCSS of the UK



The codes in the strategy from the Netherlands are also not equally divided between the aim categories. The aim category that got the most codes is number 5; ‘Increasing the cyber resilience’, followed by number 10; ‘The government and its institutions understand and can handle cyberthreats’. The aim category with the least codes is number 6; ‘Improving to detect and disrupt state, criminal and other malicious cyber actors’ with only three codes. This is followed by numbers 3 and 8; ‘Improvement in education in CS and Shaping global governance’ and ‘Securing the international advantage in CS technologies’, which both contain six codes.

This means that under the eleven goals that are already defined as main goals, the goals that the strategy of the Netherlands places the most focus on are; “Increasing the cyber resilience & The government and its institutions understand and can handle cyber threats”.

Figure 2: Number of codes per aim category NL



5.3 What are the main differences between the National Cyber Security Strategies of the Netherlands and the UK?

This descriptive question is answered by using the data from the previous section, the data from the coding scheme in the focus category, and some relevant data from the interviews.

The National cybersecurity strategies from the UK and the Netherlands state what the general goals and focuses are since they are defined in the pillars and objectives of the strategies. As explained in section 5.2, the strategy of the UK has five pillars and the strategy of the Netherlands has four pillars. When reading the strategies, it can be noticed that these pillars show a lot of similarities in terms of general goals and focuses. However, it is a lot more difficult to determine what the differences between the strategies are when reading them because of differences in formulation and structure. Therefore, the coding schemes of the strategies and the interview data are applied in order to identify possible differences between the strategies of the UK and the Netherlands.

In the previous section of this analysis, two graphs were provided with the data from the aim categories of the coding scheme, referred to as Figure 1 and 2. The data from these figures will be used in this section. As visible when comparing the figures, the number of codes in a lot of the aims differ between the two strategies, which could mean that there is a difference in focus points between the strategies. However, it is important to incorporate the fact that the NCSS of the UK has more textual data in the form of words and pages and because of that also has more codes than the strategy of the Netherlands. Therefore, it is not correct to compare the exact number of codes in the aim categories of the two strategies. However, there are some differences that can be identified within this data based on comparing the distribution of codes in all the aim categories within one strategy, and comparing that to the distribution of codes in the other strategy.

One of the differences is found in the aim category “Shaping global governance and securing the international advantage in CS technologies”. This is the aim with by far the most codes in the strategy of the UK, so there is a lot of focus on that aim in comparison to the other aim categories. On the other hand, in the NCSS of the Netherlands, this aim is one of the aims with the least codes. The same applies to the aim category “improving to detect and disrupt state, criminal and other malicious cyber actors”. This aim is in the coding scheme from the NCSS of the UK one of the aims with the most codes of all the categories. However, this aim has the least amount of codes in the NCSS of the Netherlands. Therefore it can be concluded that in comparison to the other aim categories, the aims “global governance and technology” and “improving to detect and disrupt state, criminal and other malicious cyber actors” are more focused on in the strategy of the UK than in the strategy of the Netherlands. On the other hand, the aim category “increasing the safety of digital products and services”, is one of the categories with the most codes in the strategy of the Netherlands, but in the strategy of the UK, it is one of the categories with the least codes. Therefore, this aim is given more attention in the NCSS of the Netherlands than in the NCSS of the UK.

Another reason that the coding scheme was made, was to see if there would be differences in the way the strategies would imply to handle or implement certain problems and aspects of the national cybersecurity. Figures 3 and 4 represent the number of codes per focus category. In these figures are only a couple of focus categories displayed, which are the ones that describe the way an aspect or problem is handled or implemented. These categories are: "Continuing with good measure/aspect of CS, Creating new measures/aspects/regulations in CS, Improving measures/aspects of CS, Investing in a measure/aspect of CS and Recommendations for the future." Here the same applies as for the aim categories, it is not correct to compare the number of codes since the strategies do not have the same amount of textual data. However, when looking at the figures one can see that the distribution of codes in the strategy of the UK and the Netherlands are largely the same. It is clear that the focus category; 'Improving measures/aspect of CS' is the biggest in both strategies. Overall, there are no clear differences in this area of the coding scheme that can be identified.

Figure 3: Number of codes per focus category in the strategy of the UK

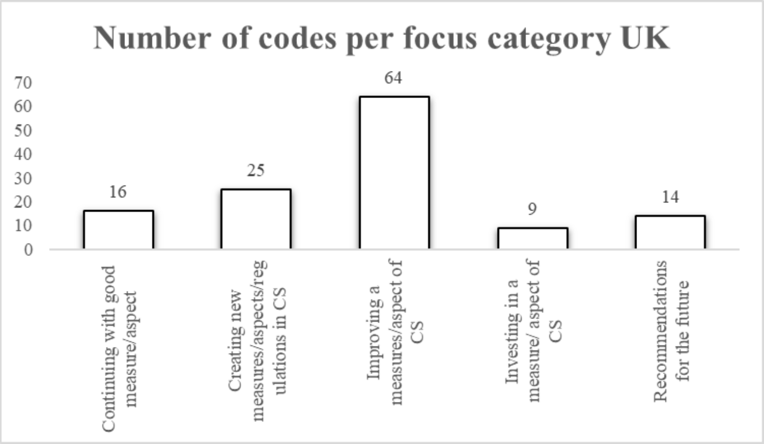
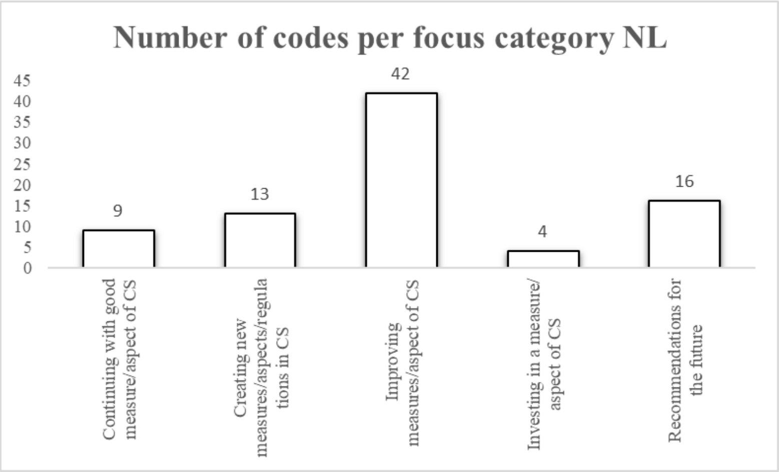


Figure 4: Number of codes per focus category in the strategy of the Netherlands



When conducting the interviews, there are also some differences that can be observed and identified. One of these differences is stated in the code: “NCSC in the UK is part of the GCHQ and in the Netherlands they are separate organizations” (Interview 3, lines 105-109). What is meant by this code is that the NCSC in the UK falls under the authority of the government, and the NCSC in the Netherlands is an independent organization. This difference can also be derived from the information about the NCSC in the UK and the Netherlands in Chapter 2. Another aspect that was noticeable during the coding of the interview was among other things found in the code: “NL not as far as the UK in programs like Active Cyber defense and endpoint detection, mostly because of legal restrictions.” (Interview 3, line 213-225). This code points out the difference in the fact that the offensive side of the cybersecurity in the Netherlands is not as advanced as the offensive side of the cybersecurity in the UK. This is also visible in a quotation from interviewee 3:

> “In the Netherlands we definitely are not that far yet.” - Interview Number 3, line 213

This quotation refers to the text that was mentioned before about the status of the British offensive cybersecurity. And this can also be seen in the code: “The Netherlands is not well known for counterattacks”. (Interview 2, lines 84-86). This code refers to a certain aspect of offensive cybersecurity, the counterattacks, as a weak point of the cybersecurity in the Netherlands. Overall, in the strategy of the UK is more attention for offensive cybersecurity than in the strategy of the Netherlands.

5.4 Why do the National Cyber Security Strategies of the United Kingdom and the Netherlands show differences and similarities?

This explanatory question is answered through the theory in Chapters 2 and 3 in combination with relevant interview data.

As stated in Chapter 3, there are many factors that could be of influence on cybersecurity, so it is difficult to know what impact one specific factor has. And, as also discussed in Chapter 3, cybersecurity has constantly evolved and adapted to new developments over the past decade which makes it difficult to measure the influence of an effect on cybersecurity over a longer period of time. However, this section will make assumptions providing relevant arguments about what factors impact the cybersecurity and the National Cyber Security Strategies of the UK and the Netherlands in order to explain the differences and similarities.

First of all, differences in the structure of governmental organizations, policies, and public companies in the cybersecurity in the UK and the Netherlands can lead to differences in their national cybersecurity strategies.

When the information from Chapter 2 about the institutions and policies in the UK and the Netherlands is compared, a lot of similarities can be found, for example in organizations like the NCSC and their functions. However, there are also differences in the cybersecurity systems in the UK and the Netherlands, which can lead to differences in the approach to cybersecurity. This is also stated by an interviewee when talking about differences between the NCSS of the UK and the Netherlands, which is visible in this quotation:

> “Of course, you will have differences because we all have different governments with different structures and responsibilities “ – Interview Number 3, lines 175-177

Next to the institutions and policies, the differences and similarities in cyber threats that the UK and the Netherlands face, as explained in Chapter 3, can also influence the cybersecurity. The main types of threats to the Netherlands and the UK are the same, which are threats from state actors and hacking and phishing. Because they share a lot of the same types of threats, a similar approach to these threats can be expected which will result in similarities in the cybersecurity strategies. However, not a lot of information about specific threats to the national security is publicly available, so it is difficult to compare the threats and to conclude how they exactly cause similarities. As also described in Chapter 3, there are a lot of other factors that can also influence the cybersecurity in the UK and the Netherlands. The elements that can have a big impact on cybersecurity according to Chapter 3 are; governmental policies and procedures, education in cybersecurity, technological infrastructure and development, financial factors, human factors, and the European Union. All these factors are in some ways differently organized in the UK and the Netherlands and can therefore also take responsibility for differences in the national cybersecurity strategies.

An example of the influence of the element; governmental policies and procedures, can be found in the difference in the offensive side of the cybersecurity, which is more advanced in the UK than in the Netherlands. This can be partly explained by the fact that the Netherlands has stricter policies around offensive cybersecurity which make the development of it difficult. This is also mentioned in the code: “NL not as far as the UK in programs like Active Cyber defense and endpoint detection, mostly because of legal restrictions.” (Interview 3, line 213-225). This code was already mentioned in 5.3 to point out this difference, but it also explains why the difference occurs, because of legal restrictions. In this code is referred to legal restrictions in the Netherlands. So this element explains the difference that the NCSS of the UK focuses more on offensive cybersecurity than the NCSS of the Netherlands.

Another element that explains differences between the NCSS from the UK and the NCSS from the Netherlands is the fact that the Netherlands is part of the European Union and the UK is not. This is also stated by an interviewee who talked about the differences in the cybersecurity in the UK and the

Netherlands which are largely impacted by the EU. This is visible in the code: “Differences between the UK and the Netherlands because of EU, but overall they are largely similar” (Interview 3, lines 181-185). As discussed in Chapter 3, the EU has its own regulations and organizations that concern cybersecurity in order to improve the cybersecurity in its member states. The Netherlands needs to abide by these regulations which affects the cybersecurity in the Netherlands, but they also benefit from the organizations and resources from the EU. This creates differences because the UK does not has to follow the regulations from the EU but can also not benefit from the EU in the field of cybersecurity like the Netherlands can. For example, the difference explained in the previous sub-section about the aim “Shaping global governance and securing the international advantage in CS technologies” which the strategy of the UK places more focus on than the strategy of the Netherlands, can be explained by the influence of the EU. The European Union has a big international influence on cybersecurity which the Netherlands can profit from. Therefore the Netherlands might focus less on the global governance and technology aim, since they already have global influence in cybersecurity through the EU. However, the UK is not part of the EU which could be a reason why they focus more on creating global and international power in cyberspace than the Netherlands.

But there are not only differences between the strategies, there are even more similarities that the two strategies share. As stated in the introduction, the Netherlands and the United Kingdom are both developed countries with a very high Human Development Index and a very high score on the Global Cyber Security Index from 2020. Therefore, the two countries are considerably similar in terms of development in cybersecurity and technical and economic resources which cause similarities in the national cybersecurity strategies. There is also an interesting code from interview 3 which is the following: “During the forming of the strategy is looked at other countries” (Interview 3, line 174-175). In this code, there was asked if during the creation of the NCSS from the Netherlands, the strategy of the UK or other countries were taken into regard. The interviewee said that this was indeed the case and that during the formation of the NCSS of the Netherlands, multiple national cybersecurity strategies were looked at as a reference, including the NCSS from the UK. This can also be an explanation of why the strategies from the UK and the Netherlands show a lot of similarities.

6. Conclusion and Discussion

This thesis started with an introduction that announced the following research question: *''How do the national cybersecurity strategies aim to influence the cybersecurity in the Netherlands and the United Kingdom? ''* This thesis provided information and an analysis in order to answer this research question.

The aim of this study was to compare the national cybersecurity strategies of the Netherlands and the United Kingdom, with the hope to identifying potential areas for improvement and learning points of each other's cybersecurity approaches. However, conducting a comparison on these two strategies proved challenging due to several factors. First of all, a noticeable limitation of this study was that in order to make recommendations about weaknesses and learning points, the strategies need to be evaluated on their effectiveness. However, evaluating the effectiveness of the national strategies is significantly challenging since the strategies are recently published, in 2022, and there is not yet substantial evidence or performance indicators to assess the impact of the strategies. Therefore, determining the true strengths and weaknesses of the influence of the strategies was not really feasible within the scope of this study.

It was also difficult to identify and compare the weaknesses of the overall cybersecurity that the national cybersecurity strategies wanted to address since the strategies only really mention points of improvement but not specifically their weaknesses and vulnerabilities. This is logical because attackers could use this information in the preparation of a cyber-attack. However, this makes it more complicated to compare and identify weaknesses that the strategies of the UK and the Netherlands want to address and overcome. Overall, there is a need for further research that addresses these limitations in order to obtain a more comprehensive understanding of the strengths and weaknesses of the national cybersecurity strategies in both the UK and the Netherlands in order to provide recommendations for future national cybersecurity strategies.

In order to answer the research question, this study provided a lot of information on cybersecurity in the UK and the Netherlands and their national cybersecurity strategies. The sub-questions were formulated with the goal to provide insights into the possible answer to the research question. The first sub-question was answered by summarizing the main organizations and policies involved in cybersecurity in Chapter 5.1. In the analysis of the second sub-question, the main aims and goals are investigated. Next to the goals that are defined in the strategies themselves, this thesis formulated eleven main goals to use in the coding analysis of the strategies. All of these goals were present in the strategies, however, there were a few aims that were obviously more discussed than most other aims. In the case of the UK is this the aim; 'Shaping global governance and securing the international advantage in cybersecurity technologies".

In the coding strategy from the Netherlands are the aims; “Increasing the cyber resilience”, and; “The government and its institutions understand and can handle cyber threats” the aims that were most discussed and explained in the strategy.

Chapter 5.3 provides insights into the differences between the national cybersecurity strategies from the UK and the Netherlands. This section concluded that in comparison to the other aim categories, the aims “Shaping global governance and securing the international advantage in cybersecurity technologies” and “improving to detect and disrupt state, criminal and other malicious cyber actors” are more focused on in the NCSS of the UK than in the NCSS of the Netherlands. On the other hand, the aim category “increasing the safety of digital products and services” is given more attention in the NCSS of the Netherlands than in the NCSS of the UK. Another interesting difference is that the offensive side of the overall cybersecurity in the Netherlands is not as advanced as the offensive side of the cybersecurity in the UK. Therefore, the NCSS of the UK gives more attention to offensive cybersecurity than the NCSS of the Netherlands.

The last sub-question explains the differences and similarities between the strategies. The factors that are identified as elements of influence are governmental organizations and policies, cyber threat and other elements like; Governmental policies and procedures, Education in cybersecurity, Technological infrastructure and development, Financial factors, Human factors, and the European Union. All these elements have an influence on the cybersecurity in the UK and the Netherlands and can therefore also explain some differences in the national cybersecurity strategies. One interesting example of this is the difference between the offensive side of the cybersecurity in the UK and the Netherlands, which can be explained by the fact that the Netherlands has more strict policies around offensive cybersecurity than the UK which restricts the development of offensive technologies in the Netherlands.

So to shortly answer the research question, the national cybersecurity strategies aim to influence the cybersecurity in the Netherlands and the United Kingdom by addressing all of the main aims as identified in the coding scheme. The strategies set goals, objectives, and expectations that the nations should follow and achieve before a certain time frame in order to improve the cybersecurity. For the strategy of the UK, the main aim to influence the cybersecurity according to the coding scheme is to shape global governance and to secure the international advantage in cybersecurity technologies. For the strategy of the Netherlands on the other hand, the main goal to influence the cybersecurity is to increase the cyber resilience and to make the government and its institutions understand and ready to handle cyber threats. The strategies also state how they want to achieve and implement the goals and objectives that are set out, and in both the strategies, improving the current measures of aspects of cybersecurity is the most common way to address the objectives and goals in order to improve the cybersecurity. However, creating new measures or aspects in cybersecurity is also often mentioned as a way to address the aims in both strategies.

Overall, the NCSS of the UK and the NCSS of the Netherlands set different guidelines and expectations to improve the security in cyberspace of the businesses, government institutions, and the citizens of their country.

As said before, it is still unclear how national cybersecurity strategies actually effect cybercrime and which national strategies perform better than others. Even though this study did not specifically focus on the effect of the national cybersecurity strategies, it did compare two of these strategies of highly developed countries and explains the differences. There are a few previous comparison studies of national cybersecurity strategies of countries, however, this study still distinguishes itself because it is a very in-depth investigation on the cybersecurity strategies of these specific two countries, as well as the newest versions of these strategies which have not been studied in this way before. The combination of a comparative cross-national research design with a textual coding analysis which is used to analyze the national cybersecurity strategies is a new way to draw conclusions about this certain topic. Therefore, this thesis was able to combine different insights about the strategies from the coding scheme, the qualitative data from the strategies, and other relevant literature and policy documents.

One of the main relevant insights this study has added to the state of the art are what the main focuses and aims are, how much attention each focus point was given, and how the NCSS aims to handle and implement the actions. However, there is still a lot more research that can be done in the area of comparing the national cybersecurity strategies of the Netherlands and the UK. For example, more research on how to evaluate an NCSS in order to compare the effectiveness of the strategies rather than comparing the strategies itself, which is in this study the case, because that can be really helpful for the formation of a future NCSS. The effects of certain fields on the NCSS can also be very interesting to investigate further in more detail, for example investigating the effect of institutions and policies in order to get a clearer understanding of how these fields influence the strategies. But, as mentioned in this study, cybersecurity is a constantly evolving aspect and in order to keep up with its developments, a lot more research needs to be conducted in the future.

8. References

Akkermans, M., Kloosterman, R., Moons, E., Reep, C., Tummers-van der, M., (2022). Veiligheidsmonitor 2021. Centraal Bureau voor de statistiek. Retrieved at 19-06-2023 from: https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021

Asghar, M. Z., & Chen, D. (2019). Cybersecurity and data protection: An analysis of the European Union’s General Data Protection Regulation. Computers & Security, Volume 83, 237-250. Retrieved at 08-05-2023 from: https://www.sciencedirect.com/journal/computers-and-security/vol/83/suppl/C

Autumn budget and spending review. (2021). A stronger economy for the British people. Crown copyright. Retrieved at 01-05-23 from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043688/Budget_AB2021_Print.pdf

Casanove, de, O., Leleu, N., Sèdes, F. (2022). Applying PDCA to Security, Education, Training and Awareness Programs. Institut de Recherche en Informatique de Toulouse. Human Aspects of Information Security and Assurance. Springer. p.39-48.

Cavelty,M, D., Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contempory security Policy. Vol. 41, No. 1, 5–32. Retrieved at 08-05-2023 from: https://www.tandfonline.com/doi/epdf/10.1080/13523260.2019.1678855?needAccess=true&role=button

Crick, T., Davenport, J.H., Irons, A. & Prickett, T. (2019). A UK Case Study on Cybersecurity Education and Accreditation. Retrieved at 16-03-2023 from: https://arxiv.org/pdf/1906.09584.pdf

European Commission. (2018). EU. The General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and other rules concerning the protection of personal data. Retrieved at 08-05-2023 from: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

General Intelligence and security service.(2023). About us, An insight into the role of the AIVD. Ministry of interior and kingdom relations. Retrieved at 06-05-2023 from: https://english.aivd.nl/about-aivd

Global Cybersecurity Index (2020). Measuring commitment to cybersecurity. ITU Publications. Retrieved at 08-05-2023 from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

GOV.UK (2018a). The Data Protection Act. Retrieved at 24-04-2023 from: https://www.gov.uk/data-protection

GOV.UK (2023). Review of the Computer Misuse Act 1990: consultation and response to call for information (accessible). Retrieved at 24-04-2023 from: https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990/review-of-the-computer-misuse-act-1990-consultation-and-response-to-call-for-information-accessible

GOV.UK. (2018b). The NIS Regulations 2018. Retrieved at 24-04-2023 from: https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

Human Development Index. (2022). United Nations Development Program. Human Development Reports. Retrieved in 23-05-2023 from: https://hdr.undp.org/data-center/human-development-index#/indicies/HDI

Jeong, J, J., Mihelcic, J., Oliver, G. and Rudolph. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. IEEE. 5th International Conference on Collaboration and Internet Computing (CIC). Retrieved at 10-05-2023 from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8998491

Johnson, R. (2022). Evolving Technology and The Impact on Cybersecurity. TechReport. Retrieved at 08-05-2023 from: https://techreport.com/blog/3476302/evolving-technology-cybersecurity/

Kamara, I., Leenes, R., Stuurman, K., Boom, v.d. J. (2020). The cybersecurity certification landscape in the Netherlands after the Union Cybersecurity Act. Tilburg Institute for Law, Technology, and Society. Retrieved at 06-05-2023 from: https://www.researchgate.net/publication/346446107_The_Cybersecurity_Certification_Landscape_in_the_Netherlands_after_the_Union_Cybersecurity_Act_Final_Report

Luiijf, H.A.M., Besseling, K., Spoelstra, M., Graaf.d.P. (2011). Ten National Cyber Security Strategies: A Comparison. Critical Information Infrastructure Security. Springer. Retrieved at 24-04-2023 from: https://link.springer.com/content/pdf/10.1007/978-3-642-41476-3.pdf?pdf=button

Lukings, M., Lashkari, A.H. (2022). Understanding Cybersecurity Law and Digital Privacy A Common Law Perspective. Future of Business and Finance book. Springer.

Merlevede, J., Johnson, B., Grossklags, J., Holvoet, T. (2020). Exponential discounting in security games of timing. Journal of Cybersecurity, Volume 7, Issue 1. Retrieved at 08-05-2023 from: https://doi.org/10.1093/cybsec/tyaa008

Militaire Inlichtingen- en Veiligheidsdienst (MIVD). (2023). Rijksoverheid. Contactgegevens en andere onderdelen overheid. Retrieved at 29-05-2023 from: https://www.rijksoverheid.nl/contact/contactgids/militaire-inlichtingen-en-veiligheidsdienst-mivd

Ministerie van economische zaken en klimaat. (n.d.). Wet beveiliging netwerk- en informatiesystemen. Retrieved at 06-05-2023 from: https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen#:~:text=De%20Wet%20beveiliging%20netwerk%2D%20en%20informatiesystemen%20is%20de%20Nederlandse%20implementatie,gevolgen%20van%20cyberincidenten%20te%20verkleinen.

Ministry for justice and security. (2022). CSAN 2022. Cyber Security Assessment Netherlands. National coordinator for counterterrorism and security. Retrieved at 29-04-23 from: https://english.nctv.nl/topics/cyber-security-assessment-netherlands/documents/publications/2022/07/04/cyber-security-assessment-netherlands-2022

Mishraa, A., Alzoubi, I.Y., Anwar, M.J., Gill, A.Q., (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computer and Security. Elsevier. Retrieved at 02-05-2023 form: https://www.sciencedirect.com/science/article/pii/S0167404822002140

Mwim, E.M., Mtsweni, J., (2020). Systematic Review of Factors that Influence the Cybersecurity Culture. Human Aspects of Information Security and Assurance. Springer. p.147-172.

Nationaal Coordinator terrorismebestrijding en veiligheid. (2022). National Cybersecuritybeeld Nederland. Retrieved at 29-03-2023 from: https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022

National Crime Agency. (2023). National Crime Agency, Cyber Crim. The treat from cyber crime. Retrieved at 24-04-2023. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

National Cyber Security Centre UK. (2023). About the NCSC. History of the NCSC. Retrieved at 16-03-2023 from: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

National Cyber Security Centre. (2022). Annual Review 2022. Making the UK the safest place to live and work online. Retrieved at 05-05-2023 from: https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf

National Protective Security Authority. (2023). About the NPSA. National Protective Security Authority, Who are we. Retrieved at 29-05-2023 from: https://www.npsa.gov.uk/about-npsa

Oerlemans, J.J., & Wagen, v.d.W. (2020). Verschijningsvormen van cybercriminaliteit. Research gate. 3, 55-105 Retrieved at 29-04-2023 from: https://www.researchgate.net/profile/Jan-Jaap-Oerlemans/publication/356171366_Verschijningsvormen_van_cybercriminaliteit/links/618e756b07be5f31b771f33e/Verschijningsvormen-van-cybercriminaliteit.pdf

Openbaar ministerie. (1993). Wetsartikel computervredebreuk. Retrieved at 10-05-2023 from: https://www.om.nl/onderwerpen/cybercrime/hack_right/wetsartikel-computervredebreuk

Porcedda, M.G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. Elsevier. School of Law, Trinity College Dublin, Ireland. Retrieved at 24-04-2023 from: http://www.tara.tcd.ie/bitstream/handle/2262/98325/1-s2.0-S0267364923000043-main.pdf?sequence=3&isAllowed=y

Rahman, T., Rohan, R., Pal, D., Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. The 12th International Conference on Advances in Information Technology. Retrieved at 08-05-2023 from: https://doi.org/10.1145/3468784.3468789

Sabillon, R., Cavaller, V., Cano, J., (2016). National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering (IJCSSE). Volume 5, Issue 5. Retrieved at 04-05-2023 from: https://www.proquest.com/openview/d678b09e570d574b39f77cf26bb2e9d4/1?cbl=2044552&pq-origsite=gscholar&parentSessionId=Kl2wTNReb%2Bwci0y5U6g48RWQnTxoFzDmhSeFU39L2sw%3D

Shafqat, N., Masood, A., (2016). Comparative Analysis of Various National Cyber Security Strategies. International Journal of Computer Science and Information Security, Vol. 14, No. 1, January 2016. Retrieved 24-04-2023 from: https://www.academia.edu/21493919/Journal_of_Computer_Science_IJCSIS_January_2016

The Cambridge Business Dictionary. Meaning of cybercrime in English. The Cambridge Business English Dictionary. Cambridge University Press. Retrieved at 15-05-2023 from: https://dictionary.cambridge.org/dictionary/english/cybercrime

The Crown Prosecution Service. (2020). Computer Misuse Act. Retrieved at 24-04-2023 form: https://www.cps.gov.uk/legal-guidance/computer-misuse-act

Walden, I., Michels, J, D. (2021). Going it alone? UK cybersecurity regulation post-Brexit. Int. Cybersecur. Law Rev. (2021) 2:19–26. Retrieved at 08-05-2023 from: https://doi.org/10.1365/s43439-021-00020-z

Wettenbank. (2023). Telecommunicatiewet. Overheid.nl. Retrieved at 22-05-2023 from: https://wetten.overheid.nl/BWBR0009950/2023-06-01

9. Data Appendix

Appendix A: Analysed documents

National Cyber Strategy UK 2022. Pioneering a cyber future with the whole of the UK. HM Government. Retrieved at 01-03-2023 from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

Nederlandse Cybersecuritystrategie. (2022). Ambities en acties voor een digitaal veilige samenleving. Rijksoverheid. Retrieved at 01-03-2023 from https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022-2028

Appendix B: Interview transcripts and coding scheme

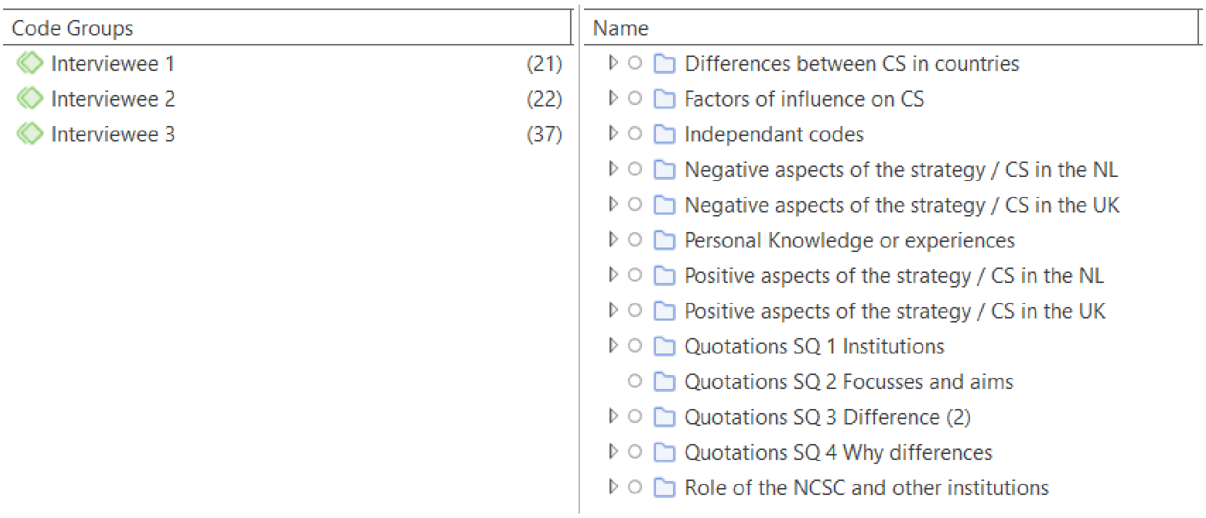
Interview transcript Participant 1 (conducted 09-05-2023): https://d.docs.live.net/336d5ca7ee3a1a43/Documents/Module%2012/Interview%20Number%201%20transcript%20.docx

Interview transcript Participant 2 (conducted 11-05-2023): https://d.docs.live.net/336d5ca7ee3a1a43/Documents/Module%2012/Interview%20Number%202%20Transcript.docx

Interview transcript Participant 3 (conducted 19-05-2023): https://d.docs.live.net/336d5ca7ee3a1a43/Documents/Module%2012/Interview%20Participant%203.docx

Coding scheme interviews: https://d.docs.live.net/336d5ca7ee3a1a43/Documents/Module%2012/Interview%20coding%20scheme.xlsx

Picture 1: Screenshot Coding categories interviews in coding scheme.



Code Groups	
Interviewee 1	(21)
Interviewee 2	(22)
Interviewee 3	(37)

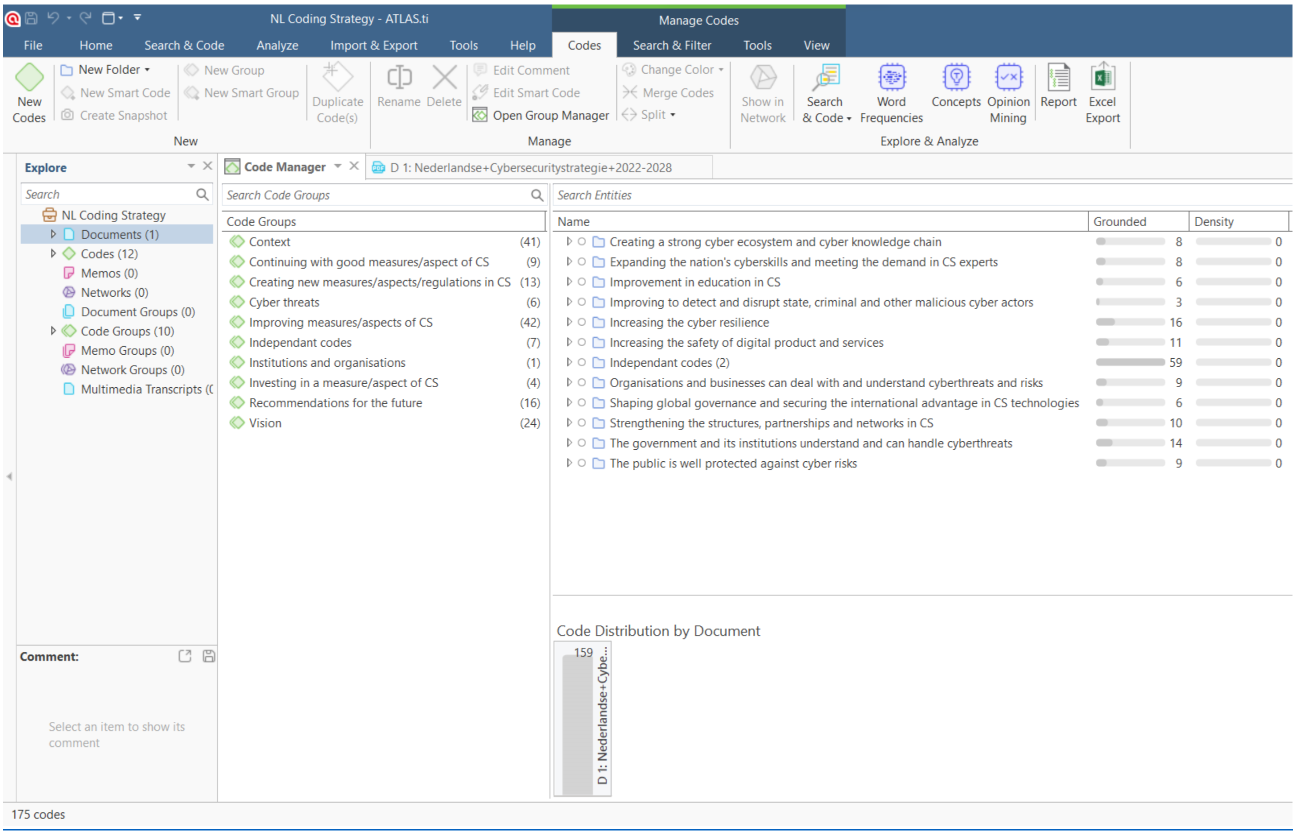
Name

- Differences between CS in countries
- Factors of influence on CS
- Independant codes
- Negative aspects of the strategy / CS in the NL
- Negative aspects of the strategy / CS in the UK
- Personal Knowledge or experiences
- Positive aspects of the strategy / CS in the NL
- Positive aspects of the strategy / CS in the UK
- Quotations SQ 1 Institutions
- Quotations SQ 2 Focusses and aims
- Quotations SQ 3 Difference (2)
- Quotations SQ 4 Why differences
- Role of the NCSC and other institutions

Appendix C: Coding schemes NCSS UK and Netherlands

Coding scheme NCSS from the Netherlands:
https://d.docs.live.net/336d5ca7ee3a1a43/Documents/Module%2012/NL%20Strategy%20Coded.xlsx

Picture 2: Screenshot Atlas.ti overview coding NCSS Netherlands:



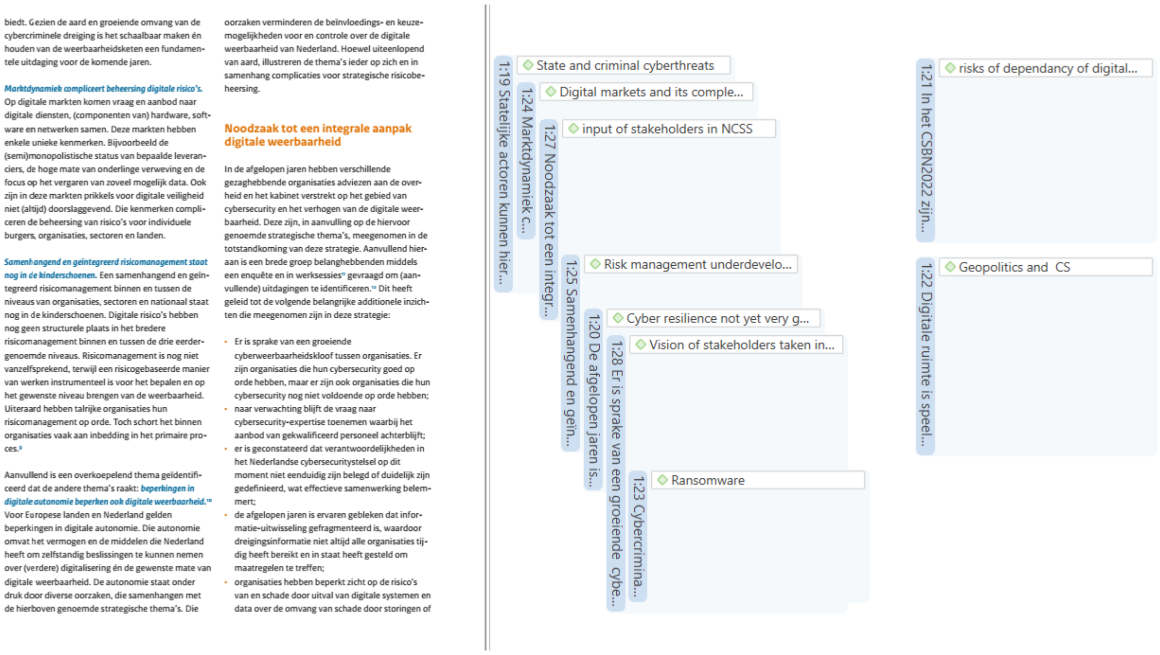
- NL Coding Strategy
  - Documents (1)
  - Codes (12)
  - Memos (0)
  - Networks (0)
  - Document Groups (0)
  - Code Groups (10)
  - Memo Groups (0)
  - Network Groups (0)
  - Multimedia Transcripts (

Code Groups	
Context	(41)
Continuing with good measures/aspect of CS	(9)
Creating new measures/aspects/regulations in CS	(13)
Cyber threats	(6)
Improving measures/aspects of CS	(42)
Independant codes	(7)
Institutions and organisations	(1)
Investing in a measure/aspect of CS	(4)
Recommendations for the future	(16)
Vision	(24)

Name	Grounded	Density
Creating a strong cyber ecosystem and cyber knowledge chain	8	0
Expanding the nation's cyberskills and meeting the demand in CS experts	8	0
Improvement in education in CS	6	0
Improving to detect and disrupt state, criminal and other malicious cyber actors	3	0
Increasing the cyber resilience	16	0
Increasing the safety of digital product and services	11	0
Independant codes (2)	59	0
Organisations and businesses can deal with and understand cyberthreats and risks	9	0
Shaping global governance and securing the international advantage in CS technologies	6	0
Strengthening the structures, partnerships and networks in CS	10	0
The government and its institutions understand and can handle cyberthreats	14	0
The public is well protected against cyber risks	9	0

175 codes

Picture 3: Screenshot coding example NCSS Netherlands:



biedt. Gezien de aard en groeiende omvang van de cybercriminele dreiging is het schaalbaar maken én houden van de weerbaarheidsketen een fundamentele uitdaging voor de komende jaren.

Marktdynamiek compliceert beheersing digitale risico's. Op digitale markten komen vraag en aanbod naar digitale diensten, (componenten van) hardware, software en netwerken samen. Deze markten hebben enkele unieke kenmerken. Bijvoorbeeld de (semi)monopolistische status van bepaalde leveranciers, de hoge mate van onderlinge verweving en de focus op het vergaren van zoveel mogelijk data. Ook zijn in deze markten prikkels voor digitale veiligheid niet (altijd) doorslaggevend. Die kenmerken compliceren de beheersing van risico's voor individuele burgers, organisaties, sectoren en landen.

Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen. Een samenhangend en geïntegreerd risicomanagement binnen en tussen de niveaus van organisaties, sectoren en nationaal staat nog in de kinderschoenen. Digitale risico's hebben nog geen structurele plaats in het bredere risicomanagement binnen en tussen de drie eerdergenoemde niveaus. Risicomanagement is nog niet vanzelfsprekend, terwijl een risicogebaseerde manier van werken instrumenteel is voor het bepalen en op het gewenste niveau brengen van de weerbaarheid. Uiteraard hebben talrijke organisaties hun risicomanagement op orde. Toch schort het binnen organisaties vaak aan inbedding in het primaire proces.[9]

Aanvullend is een overkoepelend thema geïdentificeerd dat de andere thema's raakt: ***beperkingen in digitale autonomie beperken ook digitale weerbaarheid.***[10] Voor Europese landen en Nederland gelden beperkingen in digitale autonomie. Die autonomie omvat het vermogen en de middelen die Nederland heeft om zelfstandig beslissingen te kunnen nemen over (verdere) digitalisering én de gewenste mate van digitale weerbaarheid. De autonomie staat onder druk door diverse oorzaken, die samenhangen met de hierboven genoemde strategische thema's. Die oorzaken verminderen de beïnvloedings- en keuzemogelijkheden voor en controle over de digitale weerbaarheid van Nederland. Hoewel uiteenlopend van aard, illustreren de thema's ieder op zich en in samenhang complicaties voor strategische risicobeheersing.

Noodzaak tot een integrale aanpak digitale weerbaarheid

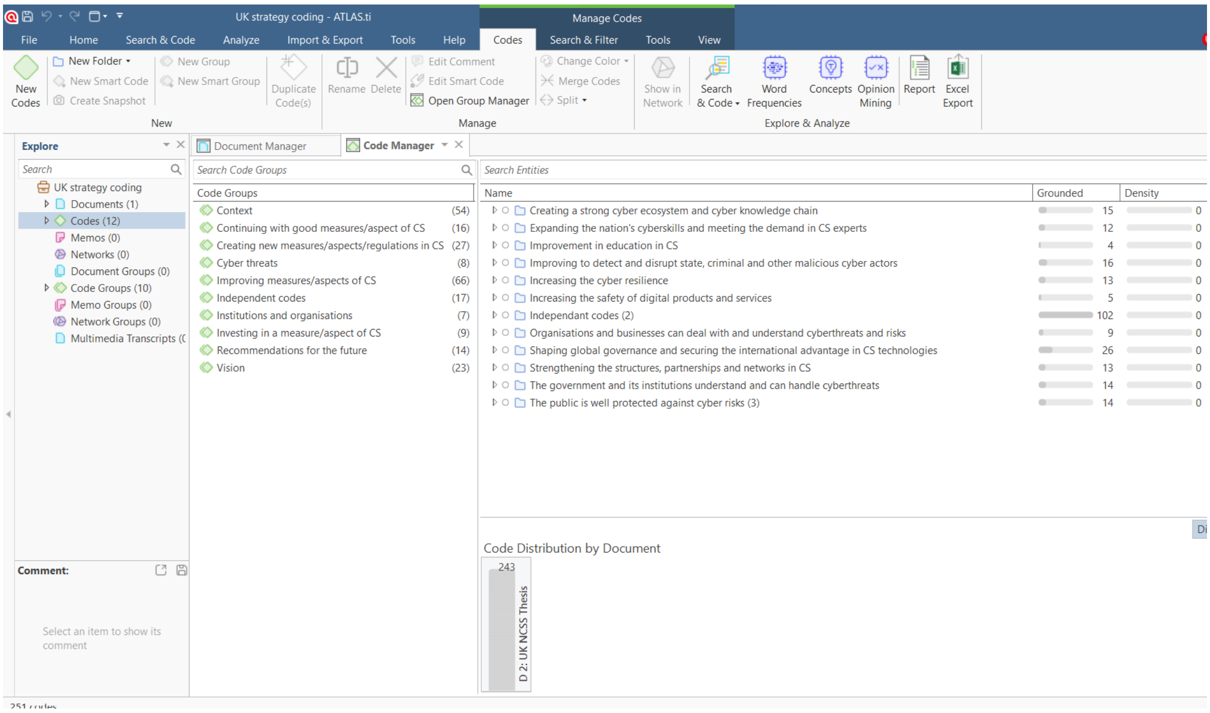
In de afgelopen jaren hebben verschillende gezaghebbende organisaties adviezen aan de overheid en het kabinet verstrekt op het gebied van cybersecurity en het verhogen van de digitale weerbaarheid. Deze zijn, in aanvulling op de hiervoor genoemde strategische thema's, meegenomen in de totstandkoming van deze strategie. Aanvullend hieraan is een brede groep belanghebbenden middels een enquête en in werksessies[11] gevraagd om (aanvullende) uitdagingen te identificeren.[12] Dit heeft geleid tot de volgende belangrijke additionele inzichten die meegenomen zijn in deze strategie:

- Er is sprake van een groeiende cyberweerbaarheidskloof tussen organisaties. Er zijn organisaties die hun cybersecurity goed op orde hebben, maar er zijn ook organisaties die hun cybersecurity nog niet voldoende op orde hebben;
- naar verwachting blijft de vraag naar cybersecurity-expertise toenemen waarbij het aanbod van gekwalificeerd personeel achterblijft;
- er is geconstateerd dat verantwoordelijkheden in het Nederlandse cybersecuritystelsel op dit moment niet eenduidig zijn belegd of duidelijk zijn gedefinieerd, wat effectieve samenwerking belemmert;
- de afgelopen jaren is ervaren gebleken dat informatie-uitwisseling gefragmenteerd is, waardoor dreigingsinformatie niet altijd alle organisaties tijdig heeft bereikt en in staat heeft gesteld om maatregelen te treffen;
- organisaties hebben beperkt zicht op de risico's van en schade door uitval van digitale systemen en data over de omvang van schade door storingen of

1:19 Statelijke actoren kunnen hier...
State and criminal cyberthreats
1:24 Marktdynamiek c...
Digital markets and its comple...
1:27 Noodzaak tot een integr...
input of stakeholders in NCSS
1:25 Samenhangend en geïn...
Risk management underdevelo...
1:20 De afgelopen jaren is...
Cyber resilience not yet very g...
1:28 Er is sprake van een groeiende cybe...
Vision of stakeholders taken in...
1:23 Cybercrimina...
Ransomware
1:21 In het CSBN2022 zijn...
risks of dependancy of digital...
1:22 Digitale ruimte is speel...
Geopolitics and CS

Coding scheme NCSS from the UK: https://d.docs.live.net/336d5ca7ee3a1a43/Documents/Module%2012/UK%20Strategy%20finished.xlsx

Picture 4: Screenshot Atlas.ti overview coding NCSS UK:

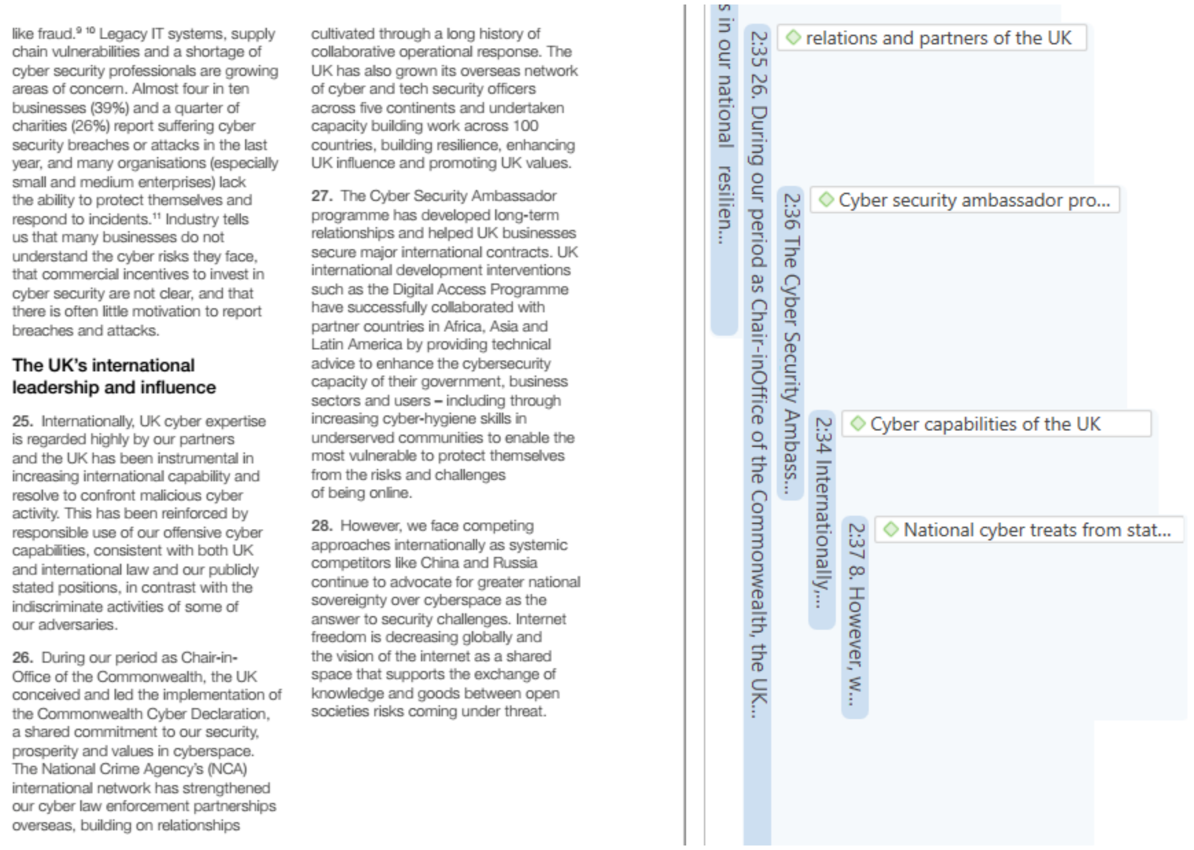


UK strategy coding
- Documents (1)
- Codes (12)
- Memos (0)
- Networks (0)
- Document Groups (0)
- Code Groups (10)
- Memo Groups (0)
- Network Groups (0)
- Multimedia Transcripts (

Code Groups	
Context	(54)
Continuing with good measures/aspect of CS	(16)
Creating new measures/aspects/regulations in CS	(27)
Cyber threats	(8)
Improving measures/aspects of CS	(66)
Independent codes	(17)
Institutions and organisations	(7)
Investing in a measure/aspect of CS	(9)
Recommendations for the future	(14)
Vision	(23)

Name	Grounded	Density
Creating a strong cyber ecosystem and cyber knowledge chain	15	0
Expanding the nation's cyberskills and meeting the demand in CS experts	12	0
Improvement in education in CS	4	0
Improving to detect and disrupt state, criminal and other malicious cyber actors	16	0
Increasing the cyber resilience	13	0
Increasing the safety of digital products and services	5	0
Independant codes (2)	102	0
Organisations and businesses can deal with and understand cyberthreats and risks	9	0
Shaping global governance and securing the international advantage in CS technologies	26	0
Strengthening the structures, partnerships and networks in CS	13	0
The government and its institutions understand and can handle cyberthreats	14	0
The public is well protected against cyber risks (3)	14	0

Picture 5: Screenshot coding example NCSS UK:


s in our national resilien...
2:35 26. During our period as Chair-inOffice of the Commonwealth, the UK...
relations and partners of the UK
2:36 The Cyber Security Ambass...
Cyber security ambassador pro...
2:34 Internationally,...
Cyber capabilities of the UK
2:37 8. However, W...
National cyber treats from stat...

like fraud.[9] [10] Legacy IT systems, supply chain vulnerabilities and a shortage of cyber security professionals are growing areas of concern. Almost four in ten businesses (39%) and a quarter of charities (26%) report suffering cyber security breaches or attacks in the last year, and many organisations (especially small and medium enterprises) lack the ability to protect themselves and respond to incidents.[11] Industry tells us that many businesses do not understand the cyber risks they face, that commercial incentives to invest in cyber security are not clear, and that there is often little motivation to report breaches and attacks.

The UK's international leadership and influence

25. Internationally, UK cyber expertise is regarded highly by our partners and the UK has been instrumental in increasing international capability and resolve to confront malicious cyber activity. This has been reinforced by responsible use of our offensive cyber capabilities, consistent with both UK and international law and our publicly stated positions, in contrast with the indiscriminate activities of some of our adversaries.

26. During our period as Chair-in-Office of the Commonwealth, the UK conceived and led the implementation of the Commonwealth Cyber Declaration, a shared commitment to our security, prosperity and values in cyberspace. The National Crime Agency's (NCA) international network has strengthened our cyber law enforcement partnerships overseas, building on relationships cultivated through a long history of collaborative operational response. The UK has also grown its overseas network of cyber and tech security officers across five continents and undertaken capacity building work across 100 countries, building resilience, enhancing UK influence and promoting UK values.

27. The Cyber Security Ambassador programme has developed long-term relationships and helped UK businesses secure major international contracts. UK international development interventions such as the Digital Access Programme have successfully collaborated with partner countries in Africa, Asia and Latin America by providing technical advice to enhance the cybersecurity capacity of their government, business sectors and users – including through increasing cyber-hygiene skills in underserved communities to enable the most vulnerable to protect themselves from the risks and challenges of being online.

28. However, we face competing approaches internationally as systemic competitors like China and Russia continue to advocate for greater national sovereignty over cyberspace as the answer to security challenges. Internet freedom is decreasing globally and the vision of the internet as a shared space that supports the exchange of knowledge and goods between open societies risks coming under threat.