Master Thesis

"FIGHTING IN THE FIFTH DIMENSION"

A comparative analysis between the German and Dutch Military Cyber capabilities

John van Veenhuizen – S1994964

Thesis Supervisors:
Mr. S. Boeke, Leiden University
Prof. Dr. P.H.A.M. Abels, Leiden University

This thesis was written in fulfilment of the requirements of the Executive Master in Cybersecurity from the Cyber Security Academy, The Hague.

A comparative analysis between the German and Dutch Military Cyber capabilities

By John van Veenhuizen
Student number S1994964

Executive Master Cyber Security

Cyber Security Academy, The Hague

"LIFE IS REALLY SIMPLE, BUT WE INSIST ON MAKING IT COMPLICATED."

CONFUCIUS

1. Abstract

From a military perspective, Germany and the Netherlands cooperate in many areas. This can be seen in various collaborations, such as the establishment of a German / Dutch Army Corps in 1995, the integration of various Army- and Air Force units and the joint use of the Dutch joint support ship, Zr. Ms. Karel Doorman [1]. In regard to the latter, in September 2018, a successful deployment of this ship in combination with the German 'Seebataillon', the German equivalent of the Marine Corps, took place. In the field of Cyber Operations and its governance, the Dutch Cyber framework as described by Ducheine [2], has served as one of the examples for the German Cyber framework [3] [4] [5] [6]. In this respect, Cyber Operations should be regarded as the whole range of military activities within Cyberspace, consisting of defensive, offensive, law enforcement and intelligence activities.

This thesis examines and analyzes the similarities and differences between the German and the Dutch organization of the Cyber domain. Despite the same starting points, the structure and governance differs considerably. Where the cooperation within Netherlands Cyber domain is based on a decentralized networked structure, Germany has centralized its capacities in a new part of the armed forces. Based on literature research and case studies in practice, this thesis compares the governance model, the procedures and the legal frameworks of the German military Cyber Operations with the Dutch situation.

2. Preface and acknowledgement

This thesis is the final assignment of a two-year Master's program at the Cyber Security Academy (CSA), in The Hague. The CSA is a collaboration between Leiden University, Delft University of Technology and The Hague University of Applied Sciences.

The subject that I have chosen for my thesis is an analysis of German and Dutch governance on military Cyber operations. In my previous position, working as a Cyber policy advisor at the Central Staff of the Dutch Ministry of Defense (MoD), I was confronted with starting points, policies and decisions within the Cyber domain that surprised me. These were different, compared to what I learned during this Master study. Different opinions and objectives of colleagues responsible for the Cyber domain amazed me and made me curious about origin and motive.

Because of the fact that I am very familiar with the German way of working, due to earlier placements in Seedorf, Germany, a mission in Mali and because of international contacts, comparing the German approach and governance to the Dutch starting points seemed very challenging to me. Especially during my mission to Mali, I worked closely with the German contingent. This was also the case for their Intelligence, Surveillance and Reconnaissance Company (ISR-Coy). Because reconnaissance is part of the newly established Cyber and Information Domain Service (CIDS) [1], I was very curious about how a scientifically founded comparison would work out. In addition, when I returned to the Netherlands, Cyber became my main portfolio during my placement at the Central Staff. In this position I was responsible for the departmental coordination of Cyber policy. In that respect, I was amazed of choices and approaches to possible resolutions. I hope my holistic approach will grant me a better understanding of Cyber as a general concept, as well as in relation to my personal work environment.

Apart from forming an interesting subject for my thesis, this idea also filled a gap in 'the body of knowledge', because in Germany it is not yet a standard practice to do academic studies or research in the English language. Relevant academic articles on Cyber, Defense and the relationship between them can therefore be found sparsely in the German university libraries.

For me this research was a beautiful journey, both literally and figuratively. Much of the information used in this thesis was personally obtained by interviews held in German Defense locations. This is because colleagues at the German Ministry of Defense are (understandably) reluctant when it comes to providing information and documents without a face-to-face meeting. Nevertheless, in all cases I have found nothing but the willingness to help me, and was provided with all requested information, as far as legally possible of course. This also applies to Dutch colleagues at various positions within the Dutch MoD.

My thanks go to the following people:

- A Dutch colleague who tipped me for this Master study and with whom the adventure started;
- The various colleagues who helped me with the many assignments and also provided me with the right information;
- The colleagues who introduced me to Dutch and German colleagues so that I could find the right contact partners for this thesis;

[1] In Germany CIDS is known as Kdo CIR – Kommando Cyber- und Informationsraum

- The Dutch and German colleagues who helped me with the conclusion of the thesis. Especially the openness during the discussions, the provision of material and the bringing of new sources have helped me a lot.

I would also like to thank my wife Elleke, for her patience and her help as a contributor and dictionary for the assignments and thesis. She is so happy for me concluding this thesis that she has even promised to get me my very own house, if I ever dare pick up another study after this one.

Finally, I want to thank Mr. Sergei Boeke and Prof. Dr. Paul Abels, respectively as first and second supervisor. Without their patience, help and critical notes, I still would have been sweating in the attic.

John van Veenhuizen
Zoetermeer, January 24, 2019

3. Table of Contents

4 Introduction

4.1 Motivation

Importance of Institutions

Cyberspace has become a fundamental feature of the world in which we live. Phenomena such as 'Digitization' or 'Digital Transformation' are changing society and thus have a direct or indirect impact on both our business and private life. There are undeniably positive sides to new technological and / or social developments (the benefits can be enormous), however the negative downsides in the form of abuse, crime and terrorism are also lurking. In order to continue to use Cyberspace in an unhindered and safe fashion, 'Governance' and 'Regulation' are necessary.

'Governance' and 'Regulation' are known as institutions. Institutions are people-designed limitations and mechanisms that structure and determine the behavior of a group of individuals within a certain community. They are identified with a social or organization objective that transcend individual interests. These objectives are achieved by mediating in the rules that determine living behavior. Organizations and the associated structures are also seen as institutions [7]. In order for an institution to function as agreed, a degree of control is necessary. There are a lot of mechanisms how control can take place.

Institutions can occur in many forms, both formal and informal in nature. The goal of an institution is to structure behavior and to bring order into chaos. The most important formal control mechanisms come from the government and public services. Informal mechanisms are self-designed limitations that structure behavior and affect culture, such as religion and marriage. Military events, such as the Second World War, have an effect on the further development and / or implementation of institutions. It can be argued if the rise of Cyberspace and its impact on society can be seen as a new effect on institutions.

The importance of the role and use of Cyberspace and its effect on institutions is internationally more and more recognized within the military spectrum. Some countries such as the United States (US) and the Netherlands have characterized Cyberspace as the fifth operational domain, alongside land, sea, air and space. In the Warsaw Summit of 2016, NATO recognizes Cyberspace as the fourth domain [8]. The NATO-alliance has been reluctant to agree on the task set within this domain. The alliance recognizes Cyberspace as a 'domain of operations', but sets the defensive deployment as a priority. This despite different recommendations from the NATO Center of Excellence [9]. This is in line with statements of Rid and Libicki, who argue that a Cyber War will never occur in the full extent of a traditional war with all its features. Rid, Libicki and the NATO alliance state that caution is required in defining the use of offensive cyber activities.

There is a lot of contradictory literature if cyberwar does or doesn't take place [10] [11] [12]. Rid argues that the so-called offensive (cyber) events fall under the category sabotage or subversion and identifies espionage as the third category [10]. He uses a narrow Clausewitz definition to explain this. Libicki states that Cyberspace is not a war domain. He even states that by using concepts from the traditional Defense domains within the Cyber domain, you create wrong associations and even false expectations [13]. Even if cyberwar is not existing and categorized under existing protocols and modus operandi, the elements have effect on the development and implementation of institutions.

The MoD is dealing with the effects of the relatively new phenomenon of Cyberwar. Consequently, this makes Cyberspace a domain in which the Armed Forces play or will play a role. Defense institutions, like Central Staff and involved Operational Units and Commands like e.g. the Defense Cyber Command, are required to manage the use of this new spectrum in the right direction. These institutions can make use of existing modus operandi combined with new aspects from this cyber realm. In this thesis, there is assumed that cyberwar as such does not take place, but that MoD has to deal with offensive operations in this new operational domain.

Every Country its own way

In addition to matters such as history and politics, culture, religion and geography largely determine institutions. These matters have effect on the formation of a region, a country, their people, their legislation, culture and religion. The change of institutions is a fluid process and can be influenced by a lot of different aspects. Because every country is unique, the use and form of institutions is also unique. However, aspects of institutions can also be similar. One of the most well-known institutions is the social contract. In exchange for protection (Defense) people renounced their individual rights to a greater or lesser extent [14]. This is formalized in legislation.

According to literature, in the years after the initial formation of a state, the original form and principles are subject to change. This is clearly visible in Germany, one of the two countries that is the subject of study in this thesis. As stated before, military events can have a big impact on institutions. The impact of the Second World War, and the demands made by the Allies on Germany's 'post' Second World War state form, limit the political decision-making process. Since that time, Germany as a federation, initially had eleven and later sixteen so-called federal states that all have their own government, a parliament and a constitution. These federal states influence federal legislation and decision-making through a federal council. This sometimes hinders national decision making when federal states and national governments disagree. An example of this problem is the discussion about inheritance and wealth tax in 2002 [15].

The reunification of former East- and West-Germany in 1990 also had a great impact on legislation and regulations. The fear of the former German Democratic Republic (GDR) for intelligence services and their resources, still reflects on political and MoD decision-making. This can be seen in the implementations and acceptance of areas such as biometrics and intelligence in the Cyber domain. German political decision-making is very cautious, which was also observed in an American report that examined the implications for a partnership between the US and Germany. The conclusion of this report was that both in a civilian and military context, Germany had to take more bureaucratic hurdles than other countries [16].

Why compare Germany and the Netherlands?

The choice to take Germany and the Netherlands as a subject for this analysis is a multiple-sided one. Firstly, Germany and the Netherlands show great similarities in economic and social terms. This also applies to 'Cyber and Information Services'. Documents such as the 'Cyber Security Scan' [17], show that the Netherlands wants to become a digital leader, that it wants to play a major role in Europe and that it considers the protection of its own ICT infrastructure and resources to be important. Germany has similar aspirations and goals, and in the German Cybersecurity strategy these ambitions have been translated into so-called 'Handlungsfelder' or 'Action Areas' [18].

Secondly, these ambitions in the Cyber domain also apply in the military field. This is apparent, among other things, from the fact that the Dutch governance framework was one of the examples to come to a German framework. The structure of the framework, with the same parties, also serves here to position and mirror players, roles and legal frameworks in order to arrive at a congruent story, and to deal with cyber threat.

Besides the mutual goals, similarities and frameworks, the Netherlands and Germany have a mutual Army Corps, the 1 (German/Netherlands) Corps. Although participation is from two countries with two different institutions, this cooperation in Defense shows the near distance of these two countries, not only geographically, but also institutionally.

And finally, little is known about academic research on the Cyber Security approach within the German Ministry of Defense. The little academic literature which is available is mostly written in German. Even though there is a mutual Army Corps which shows the near distance and great similarities in institutions, the only availability of literature in German immediately shows the contrary. It is therefore a challenge to provide more clarity on this matter, through this research.

Gap in the body of knowledge

There is little English academic literature available with regard to German insights and the German approach to the military Cyber spectrum. Much of the available literature on this subject in general is in English and comes from the Anglo-Saxon bibliography and concerns American insights, insights from the United Kingdom (UK) or insights from countries that have a strong bond with the aforementioned countries. The main reason for the primary use of the English language in available literature regarding cyber is the US and the UK have been investigating the possible influence of digitization or cyber within the military spectrum for a longer time and as a result are also predominant in the academic world.

Much of the background information that provides insight into the starting points, objectives and formation of the German military Cyber component comes from classified or unclassified military literature, the so-called ‘grey-literature’. Public sources, whether or not fed by 'illegally' obtained information [19] also provide insight into what the military Cyber objective of Germany is.

The reason for the lack in literature of German military cyber is threefold. On the one hand Cyber is still a rather young phenomenon within the German Defense. The build-up of Cyber capacities within the German armed forces has been officially taking place since 2015. As a result, academic research did not or could hardly take place. The University of the German Armed Forces in Munich welcomed its first cyber students in ‘Cyber Security and Information Technology’ in 2018. This means that graduation assignments from this faculty have not yet taken place [20]. In contrast, the Netherlands already implemented the course ‘Cyber Operations in the Netherlands Defense Academy’ in 2012 and ‘Cyber Warfare’ in 2015 as minor courses in their military officers training [21]. Although the Netherlands has more years’ experience with cyber in their military studies, the start of the full cyber military university course in Germany immediately has overtaken the Netherlands in maturity of military cyber training. The third reason is that in Germany, traditionally a lot of academic work takes place in the German language.

4.2 Research Question

Germany has included the Dutch Cyber framework as defined by Ducheine [2] in its efforts to compose a model for its own Cyber approach within the German Ministry of Defense. In order to make a good comparison between the governance of both countries, this fact serves as the starting point for this research and the formulation of main and sub questions. The main question for this study is therefore as follows:

> *"What is the governance model for German Military Cyber operations, and how do the German procedures and frameworks relate to the Dutch situation?"*

In order to support this main question, the following supportive questions/statements have been formulated:

- How are the German- and Dutch military Cyber capacities built and organized?
- How does the Dutch Cyber Governance Framework apply for the German Armed Forces?
- How is the decision-making process organized in Germany and the Netherlands with regards to Cyber operations?
- What are the main characteristics of the Dutch and German legal frameworks with regards to Cyber operations?
- What are the main advantages and disadvantages of the current governance structures and modus operandi per country?

4.3 Research Methodology

Methodology

In this holistic research, a comparative analysis with respect to the governance of the military Cyber capabilities of Germany and the Netherlands is conducted. To this end, relevant research questions have been formulated. In order to answer these questions as well and completely as possible, desk research was conducted and interviews were held in both Defense organizations on the basis of pre-established questionnaires.

The method of this research is largely done on the basis of empirical research as applied in 'Natural Science'. Within the approach of this research aspects of 'design science' as defined by Hevner are also identified. This involves defining the artefact and testing for its usefulness by means of a 'rigor' and 'relevance' feedback loop in the IS research framework [22]. In this case the Cyber Governance framework as defined by Ducheine [2]. In this thesis, aspects of both methods will be used to be sure to perform a thorough investigation with relevant conclusions.

The sources for desk research are twofold. Scientific documents and literature were researched. With regard to the general part, 'Governance', sufficient material was available in the various academic libraries. For the study of the Cyber capabilities of both countries and the governance as arranged within the two Ministries of Defense, little academic literature was available, especially for Germany. That is why non-scientific literature such as governmental publications, reports and internal policies, strategies and doctrines have been used in relation to these aspects.

Interviews
Due to the partial lack of academic literature, interviews with subject matter experts were conducted. These interviews were also used to receive input and insights from the field. In addition, information from these interviews could also be used to verify the correctness of the information and could be correlated with the information found in the literature.

The choice for the Subject Matter experts (SME's) to be interviewed, has been made on the basis of their relevance for this research. Several officials have been interviewed, in all layers of the German and Dutch Defense organization. In Germany, because of the more hierarchical organization, the start was with the Central Staff. After the Central Staff, the SME's within the relevant organizational units were interviewed. In the Netherlands, the participants were chosen on the basis of their additional expertise, and for verification and correlation of literature or explanation of legislation.

In particular, the German colleagues, as well as Dutch colleagues working in the intelligence services or related units asked to anonymize the interviews and not to publish them as part of this thesis. Because these interviews were processed anonymously, the SME's were willing to be more open during the interviews, which resulted in a better perspective for this thesis.

Interviews reflect personal views. Although the interview questions were drafted and related to a subject, the answer is always subjective. Despite more, deeper and specifically targeted questions from the interviewer and the specific request for objectivity, the aforementioned must be considered. In the elaboration of the interviews, an attempt was made to guarantee objectivity as much as possible. By placing the answers in the right context, correlating it with existing literature and cross-referencing it with other interviewees, subjectivity and bias is prevented as much as possible.

4.4 Relevance

This research is relevant from both an academic perspective as from a Germany-Netherlands cooperative perspective. Firstly, due to the lack of existing literature, concerning this topic it is important to gain insight into the governance of Cyber capabilities within German Defense. Secondly, these insights are also relevant in the context of cooperation between the German- and Dutch Ministry of Defense. As mentioned before, cooperation is already taking place in many areas. Additional clarity of operational backgrounds, working methods, as well as in the governance within the Cyber domain of both countries will improve mutual insights. It therefore contributes to better cooperation and the possible deployment of new joint initiatives within the Cyber domain and other segments of Defense.

4.5 Limitation of Research

Like in all research, this research also has its limitations. This has several reasons. In the first place the factor time. The relative short timeframe to work out the complete thesis limited a number of things. For example, the number of interviews. These had to be limited to a small selection of German and Dutch officials, given travel time and elaboration. The literature search and the further draft could also be carried out to a limited extent for that reason. Ultimately, it reflects a limited representation of reality. It is therefore recommended to conduct further research on this topic.

A second limitation is the absence of sufficient academic literature in regard to the Dutch, and in particularly the German situation. As a result, the description and analysis is based on a narrow range of sources. The government documents in this case are formal representations of the prevailing Defense policy and are not objective and academically substantiated in this sense. However, because in both Germany as the Netherlands there is now more focus on Cyber within the MoD's, this thesis fills a part of the literature gap and can be used as starting point for further research.

In the Netherlands, more English academic literature on Defense in relation to Cyber is available than in Germany, but this cannot be labeled as objective in all cases. Much of the available literature, especially in the field of legal frameworks, legislation and offensive Cyber comes from a limited number of officers who have been involved from the beginning in the establishment of the Defense Cyber Command (DCC) [2]. These officers and researchers are not only observers, but also have personal interests.

The last restrictions concern the classification of the material that was necessary to bring this research to a successful conclusion. Because much of the material is classified or politically sensitive, not everyone was prepared to share all information or to offer it for processing. This creates a limited image that is not complete in all cases. Finally, because of the personal knowledge and experience in this field, and because the author can be seen as a SME, the author has also added and supplemented parts of the research with personal insights. The limitation here is the danger that this has happened with some subjectivity.

4.6 Structure of Thesis

The structure of this research is as follows. After the general explanation of the assignment and the presentation of the research question, as well as the indication of relevance and constraints in Chapter 4, Chapter 5 describes a theoretical consideration of aspects related to 'Governance' and presents a theoretical framework.

Chapters 6 and 7 describe and consider the Dutch and German Cyber structures respectively, and an analysis is performed on the basis of the Dutch problem areas identified. After this analysis, the findings are presented in Chapter 8 and the conclusions and future work are presented in Chapter 9.

[2] In the Netherlands DCC is known as DCC – Defensie Cyber Commando

Figure 1 shows schematically the research model including the intended results per chapter.

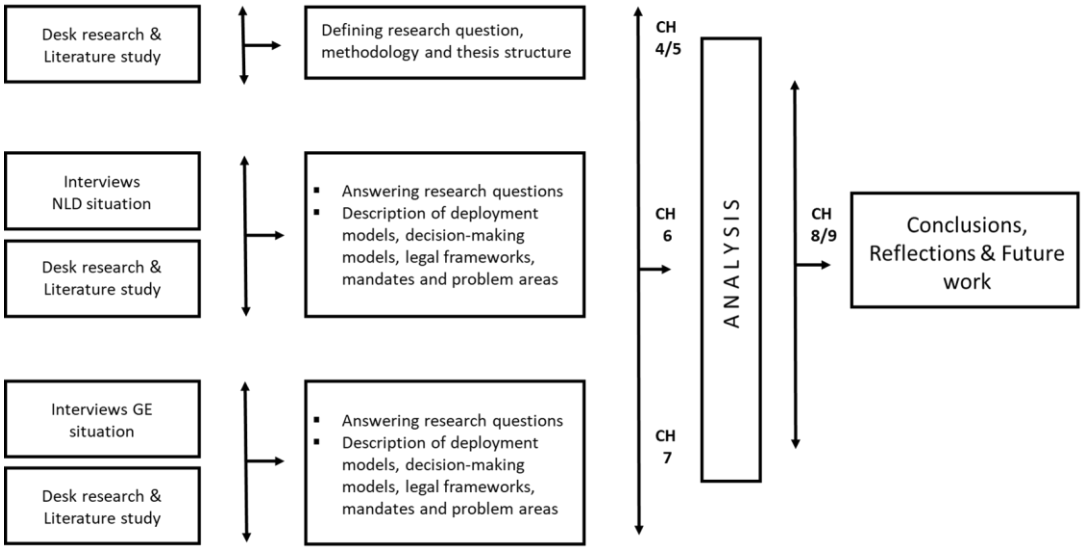


Figure 1: Research model

5 The governance framework explained

5.1 Introduction

This chapter first describes the basic governance framework, by giving insight of the origin of this framework. Next, a relation is made with the Three Layer Model of van den Berg, with specific focus on the Governance Layer. Next, a relation with the Dutch Defense Cyber Framework is made, by giving insight into the origin of this framework. A correlation is made between ‘national coordination and cooperation’ and ‘military coordination and cooperation’ which results in four paradigms. Finally, these paradigms are extrapolated in governance dynamics.

5.2 The governance framework

General

In order to answer the research question a proper framework regarding the governance of the military Cyber capabilities of Germany and the Netherlands has to be created. In order to create the framework, three important definitions of ‘Cyber’ or 'Cyberspace', 'Governance' and 'Military Operations' are needed.

Cyber or Cyberspace

Folsom defines Cyberspace as as an embodied switched network for moving information traffic, further characterized by degrees of access, navigation, information-activity augmentation (and trust) [23]. A study conducted at the University of Tilburg in 2015 by Adams et al [24], also investigated the term 'Cyber' or 'Cyberspace' as part of a broader definition of ‘Governance of Cyber Security’. At first this study seems to tend towards a statement based on the traditional information security 'CIA triangle' [25] [26]. However, in the further course of the study, the elaboration goes beyond this limited definition of technical concepts such as Confidentiality, Integrity and Availability.

Cyber, according to this study [24], is derived from the Greek word 'kyber' which means navigation. By reasoning further, the authors indicate that a quotation in a science fiction novel written by William Gibson has led to the first introduction of the term ‘Cyberspace’. Subsequently, according to this study, a usable and broadly accepted definition of Cyberspace, is defined by C. Hamelink. He outlines Cyberspace as a 'geographically unlimited, non-physical space, in which - independent of time, distance and location - transactions take place between people, between computers and between people and computers' [27]. Furthermore, it is explained in this paper, that the Cyber spectrum, in addition to a technical layer, also consists of a socio-technical layer in which the interaction between man and machine takes place. The study as a whole actually describes a third layer, namely the governance layer. This is analogous to the model of van den Berg et al [28], which is revisited later in this study.

It is also stated that Cyberspace as a concept is not one single entity, but an assembly of different Cyberspaces, each based on its own, possibly different, technique and application. This definition is also valid and usable within the military domain. The fifth domain, as Cyberspace in the military world is defined, has a wide variety of appearances both in the technical field and in use. Therefore, several players use this new dimension, each in their own way while performing their operations.

Military Operations

The Dutch dictionary ‘Van Dale’ describes a military operation as a 'series of planned activities, carried out by an Armed Force to achieve a special result during a war'. Although this definition still holds up, considering the three main tasks of the Dutch Ministry of Defense, it is nowadays better to talk about 'deployment' instead of ‘war’. Contrary to what is regularly found in military articles or Defense documentation relating to Cyber, the concept of 'operation' should be regarded in a broader context than just offensive Cyber activities.

Actions that are of a defensive nature, activities that are planned in the context of intelligence or deployment of military units within the framework of Law Enforcement are also classified as military operations. The Dutch Defense Doctrine [29] deals with operations in more detail and, in addition to the aforementioned forms of operational action, also describes forms of appearance such as maritime-, land- and peace operations. For this thesis, the concept of ‘Operations’ refers to the full spectrum of possible deployment. This implies that the term 'Operations' refers to both the offensive, the defensive, the intelligence and the Law Enforcement domain.

Governance

Governance means to control or steer. It stems from the Latin word ‘gubernáre’, which was in turn borrowed from the Greek language. In order to control and steer one has to have the whole of skills, knowledge, culture and resources to be able to incite adaptive and reforming initiatives [30]. In the study by Adams et al the term governance is explained by contrasting the concepts of government and governance and by mirroring governance to the concept of regulation [24].

In the discussion in the study of Adams et al on government and governance it is indicated, that these days top-down government authority is no longer valid, but that the classic top-down model is complemented by more actors influencing policy in a horizontal or bottom-up fashion. Adams et al argue that government may be a form of governance, which has consequences for the relations. Where there used to be a hierarchical relationship between state, market and society, nowadays there is more of a network structure with horizontal and vertical relations. In order to understand the influences in the policy arena, it is important, according to the writers, to understand the interactions between all the elements [24]. This has also been described by Broeders who mentions that Cyber Security Governance in the Netherlands is very much in flux and that finding a role in this crowding field is an ongoing concern for the Dutch MoD [31]. Although his research report mainly focuses on the relationship between the Armed Forces and other public and private parties and the possible issues, a translation to the internal relations of Defense in regard to the Cyber playing field is easy to make, and is very valid as well.

If government is a form of governance, as mentioned by Adams et al, governance effects the understanding of regulation and mechanisms to regulate. In the elaboration in Tilburg's study, it is explained that regulation can be seen as an alternative form of governance [24]. This, while regulation can also be seen as an instrument in support of governance as described by Lessig [32]. Although the reasoning of Adams et al can be challenged in itself, the outcome of this debate is very useful. Adams states 'When discussing governance, the combination of actors, structures and processes, as well as the direct and indirect relations between them and ideas underlying their interactions, must be taken together' [24].

The study of Adams et al then proceeds to the re-conceptualization of governance. Although this study considers governance broader than this thesis does, the starting points of the study are certainly usable. Adams et al, consider government, market and society and its mutual dependencies [24], while this thesis only considers the internal governance of Defense. However, the following aspects as discussed by Adams et al, play a significant role in both studies. First, when several players play a role at more than one level, responsibility and accountability become unclear. An issue that was also recognized by Tuohy [33]. In addition, uncertainty about who is in charge affects elements of command and control. Secondly, legitimacy issues play a role in both studies. The introduction of new players in an already existing domain, raises questions about how the new roles and responsibilities should be fitted into existing strategies and policies [24].

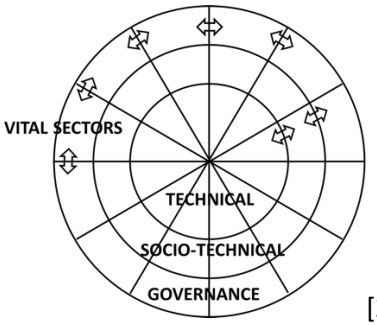
Working definition
Adams et al try to find a useful definition of the concept 'Cybersecurity Governance'. They recognize that this is difficult, because the three focus areas Cyber, Security and Governance are open to multiple explanations and interpretation. A composite definition of these three fuzzy concepts is therefore difficult. Nevertheless, based on their research, they come up with a useful working definition [24].

For this thesis this definition has been translated into *'Governance of Military Cyber Operations'*. This is defined as follows: 'Governance of Military Cyber Operations', 'references to the approaches used by multiple stakeholders within the Military Cyber arena to identify, frame and coordinate (pro) active and reactive responses to potential threats to the technical-, socio- technical and governance aspects of Cyberspace, the conceptual space that affords digitized and networked human and organizational activities' [24].

5.3 Three Layer Model

Van den Berg et al conceptualize Cyberspace on the basis of their 'Three Layer Model' [28]. For years, the paradigm of Information Security was based on purely technical principles. These were symbolized by the concepts Confidentiality, Integrity and Availability, the so-called CIA-triangle [25] [26]. In a study, van den Berg indicated that the interaction between man and machine, the so-called socio-technical aspects, and governance are equally important to ensure security in Cyberspace in a responsible and safe manner [28].

The three-layer model of van den Berg (figure 2) describes Cyberspace in three circles or layers, from the center described, first the technical layer, then the socio-technical layer and finally the governance layer. (See Figure 2). Every layer has its own concerns. This implies that the technical layer is responsible for Information Security, the socio-technical layer for Cyber Security and the Governance layer is responsible for rules, regulations and ethics and compliance. The Model of van den Berg has sections, representing the vital sectors as defined by the governing authority. For the Netherlands this is the National Coordinator for Counterterrorism and Security of the Ministry of Justice and Security [34][35].



[28]

Figure 2: Three Layer Model

The Ministry of Defense is also a vital sector. This implies that it must also invest on all three aforementioned layers. This not only applies to Cyber Security within the vertical 'resilience' of the framework as shown in figure 4, but to all facets of the Cyber domain in which Defense is active. In this perspective, this study emphasizes that governance must be well invested in the vertical areas such as ‘resilience’, ‘law enforcement’, ‘intelligence’ and ‘offensive’, but also that horizontal governance in the form of coordination across these pillars must be properly tuned. This insight will be examined further in the next section.

5.4 The origin of the Dutch Defense Cyber Framework

Within the scope of the 'Strategic Outlooks' of the Ministry of Defense [36], NOASR [3] conducted a study in 2010 into 'Cyberspace as a military dimension' [37]. In this research the various forms of 'violence' in Cyberspace have been defined and positioned, by plotting 'perpetrator' and 'goal' in one graph. In a study by the American Defense Science Board (DSB) of 1997 [38], this is done with the parameters 'impact' and 'probability' on the axes. By combining best of both studies, a possible division of four paradigms within the Cybersecurity field can be created. See figure 3.

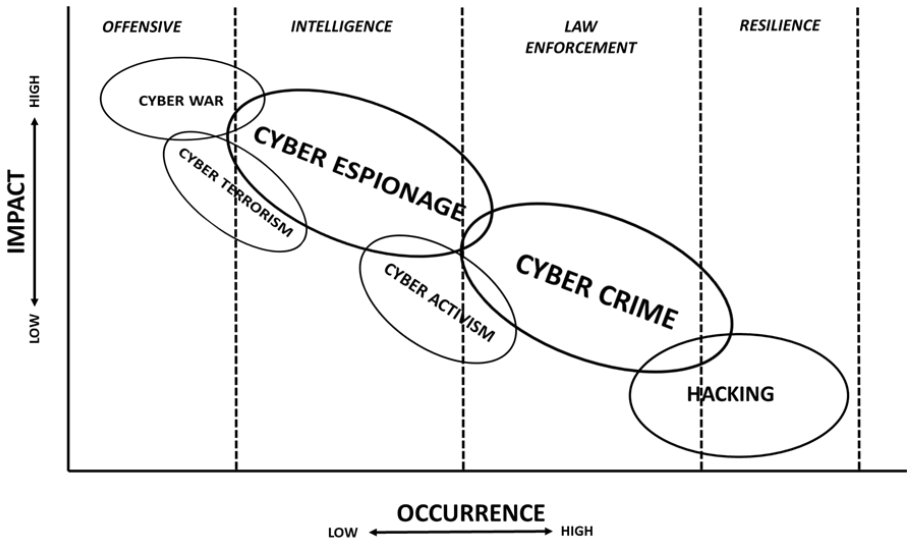


Figure 3: Impact & Occurrence of Cyber threats

[3] In the Netherlands NOASR (Netherlands Organization for) Applied Scientific Research known as (NO) TNO – (Nederlandse Organisatie voor) Toegepast Natuurwetenschappelijk Onderzoek

In a 2011 report of the Advisory Council on International Affairs (ACIA) [4] and the Advisory Committee on Issues of Public International Law (ACIPIL) [5], three roles for Cyber capabilities in the military spectrum are recognized [39]. This concerns defensive, intelligence and offensive activities. In this report, based on the formulated principles, the attention for the Cybercrime phenomenon is little to none. In this respect 'Law Enforcement' is only grazed upon and not included in the further elaboration of the report. This can also be said for the first edition of the Defense Cyber Strategy for which this study served as input.

Ducheine elaborates on the aforementioned basic principles and, based on the Defense Cyber Strategy 2012, states that the three main tasks of Defense also apply in the digital domain for the efforts of the Armed Forces [2]. When these efforts are translated, four paradigms are identified, namely protection, law enforcement, intelligence and conflict. Ducheine also indicates that the paradigm of 'Law Enforcement' is underexposed in the Defense Cyber Strategy of 2012 [40]. These paradigms can be translated into 4 roles with associated players, each with their own legal and administrative framework. The four described paradigms have, in addition to internal dependencies, also a mutual coherence because there are many dependencies between these areas of interest. Coordination or governance is needed in that perspective. This is further examined and elaborated in this study.

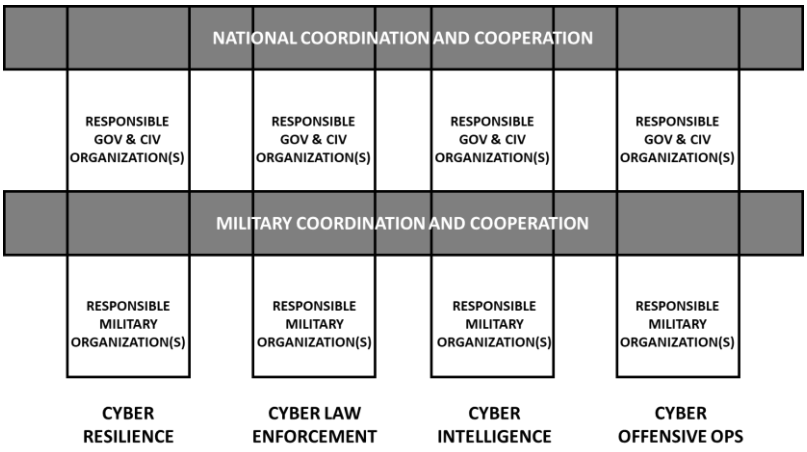


Figure 4: Cyber Governance Framework

In addition to the relationships between organizations within the Dutch MoD, there are also links to other (external) organizations, such as the National Police [6], the National Cyber Security Center[7] and the General Intelligence and Security Service [8]. All these parties play a role within the National Cyber Security approach and by combining these elements, a framework arises that will serve as a basis for the further considerations in this thesis (See figure 4). In this framework, the verticals are the identified paradigms or the roles with their players and the horizontals are the alignment or the governance across all pillars. Although the study focuses in particular on the playing field of Defense,

[4] In the Netherlands ACIA is known as AIV – Adviesraad Internationale Vraagstukken
[5] In the Netherlands ACIPIL is known as CAVV – Commissie van Advies inzake Volkenrechterlijke Vraagstukken
[6] In the Netherlands NP (National Police) is known as NP – Nationale Politie
[7] In the Netherlands NCSC (National Cyber Security Center) is known as NCSC – Nationaal Cyber Security Centrum
[8] In the Netherlands GISS (General Intelligence and Security Service) is known as AIVD – Algemene Inlichtingen- en Veiligheidsdienst

coherence with overarching national cyber interests are also important. This certainly applies to the German situation where national security is primarily the responsibility of the Ministry of the Interior and not of the Ministry of Defense.

5.5 The paradigms defined

As a reference for the continuation of this study, it is necessary to use clear definitions for the four paradigms: resilience, law enforcement, intelligence and offensive cyber. The definitions used are similar to those described by Ducheine [2]. He based these definitions on the roles mentioned in the Defense Cyber Strategy [40] [41]. Resilience, the first paradigm, concerns the protection (or security) of the internal operations in peacetime and the support of command and control during deployment. In addition to the (physical) protection of the IT resources, this also concerns the awareness of the personnel and the individual measures. The second paradigm concerns law enforcement on the basis of the Police Act 2012 [42]. This is carried out by the Royal Netherlands Marechaussee (RNLM). The RNLM is a police organization with a military status that makes part of the Ministry of Defense. For the majority of its law enforcement tasks, it operates under the Ministry of Justice and Security. Third, there is the intelligence paradigm. Within the Dutch Defense organization, this role is performed by the MISS and the Joint Sigint Cyber Unit (JSCU), a mutual unit from MISS and GISS. The task package consists of acquiring and providing access to data from technical sources, the support for analysis and the delivery of Signals intelligence and cyber capacity at strategic level. The fourth and final paradigm concerns the offensive Cyber operations. This is in the Netherlands the domain of the Chief of Defense (and the operational commands) and is executed by the Defense Cyber Command. The activities from this role concern the influencing of actors via the digital domain, which can eventually lead to disruptive actions against opponents [2].

5.6 Governance dynamics

The framework elaborated

The outlined Cyber Governance Framework is a frame of reference in which different paradigms can be visualized and where underlying phenomena can be compared with each other. This is important for the following chapters, because problems and possible solutions can be explained and substantiated in this way. Vacca states that the cultural values of the different branches of the Armed Forces may be supportive for solving the problems of the Cyber Security domain, by placing order, framing matters and evaluating policy options [43]. The input from the different branches can certainly offer advantages, but can also be disadvantageous. This is because the different units and commands of the Armed Forces do not have one culture, but a lot of subcultures depending on type of force, geographical location, rank and civilians. In the course of often hundreds of years of existence, they have built up their own cultures. This fact, together with organizational structure and legal frameworks, form the most important, non-visualized principles of the framework within Defense, which should make the complexity of governance clear and open to discussion.

The definition of governance has already been described and is positioned in two ways in the framework. There is governance in the vertical pillars as well as in the horizontal bars. The vertical pillars symbolize a paradigm as well as the relevant player (s) within this paradigm. These players, including their organization, have a form of governance. Because these individual players also have to work together and coordinate with each other, there is a coordination layer. This is shown in the horizontal bar.

Organizational structure

The organizational structure, or also the way in which an organization is set up, aims to achieve an organization's goals as efficiently and effectively as possible. To define such a structure, variables such as division of tasks, responsibilities and powers and coordination play a role. According to Mintzberg, organizations can be divided into three primary dimensions. These are the organizational part that contributes most to success, the main coordination tool and the degree of decentralization [44]. The classification based on these parameters leads to five structural classification forms. The Ministry of Defense is originally a hierarchical organization and is characterized according to Mintzberg's criteria as a machine bureaucracy, leaning towards a professional bureaucracy mixed with the divisional structure [45].

The vertical pillars within the outlined framework are characterized by the aforementioned structure and associated characteristics such as standardization, limited degree of delegation and in a number of areas professionals with a specialization within a field. However, the horizontal alignment layer of the model is formed by several Defense organizations, each with their own characteristics from the vertical columns. In light of the necessary cooperation, another organizational structure is created. A network of organizations is formed, each with its own modus operandi that must coordinate to a greater or lesser extent and work together to achieve their common goal, the security of the Netherlands. Provan and Kenis [46] characterize a network as a group of organizations that work together to not only pursue their own goals, but also to pursue collective goals. This phenomenon is often investigated in a context in which interdepartmental- or public-private cooperation takes place. However, the outcome of these investigations is also valid for the situation within the Ministry of Defense.

The structure and culture of an organization influence the manner of governance. Governance also influences how an organization is shaped and how the culture manifests itself. Research into networks, cooperation and the necessary governance is not new, as the research of Jones et al shows in October 1997 [47]. They state in 1997, already 20 years of research has been carried out into the advantages of network collaboration and governance. In this article they indicate that: 'the network form of governance is a response to exchange conditions of asset specificity, demand uncertainty, task complexity and frequency' [47].

The organizations within Defense that deal with Cyber operations can be considered as a network of nodes. The network theory as defined by Provan and Kenis can be used to clarify and understand the relationships between the different nodes or parties [46]. They distinguish three basic forms of network governance namely: participant-governed networks, lead-organization-governed networks, and a network administrative organization. A participant-governed network is characterized by shared governance of all the network members together. With regards to importance, all members are equal and they trust each other in their behavior. In the second model, the lead-organization model, a lead agency is responsible for the decisions and coordination. This is a more hierarchical and centralized model. The last model is the network administrative model. In this mode of governance a separate and external entity governs the network activities [46] [48].

A fourth form of governance was proposed in one of the interviews held to support this research [49]. It was indicated that for each identified phase in the realization of a product in the processes preparation, construction and execution of a cyber weapon, one of the organizations involved should be given lead control. In other words, 'the lead organization' changes during the realization process.

This does not imply a different model, but is a variation on one of the three models already described.

Organizational Culture

Organizational culture is characterized by norms, values and behavioral statements that are endorsed by all members of an organization and that ensure an internal connection. Culture plays an important role in Defense. In an article by Reger et al, it is stated that 'to the extent that a culture includes a language, a code of manners, norms of behaviour, belief systems, dress, and rituals, it is clear that the Army represents a unique cultural group' [50] [51]. Hall, complements this opinion with the comment that 'while the article written by these authors focuses on the Army, each of the military services have components that are both unique to that service, as well as common across the military' [51].

The armed forces and their components have existed for a long time. The Dutch Navy was founded in 1488, while the Army and the Marechaussee have existed for more than 200 years. The youngest part of the Armed Forces, the Air Force, has been in existence for more than 100 years. All services in the Armed Forces can be considered as private communities. They have developed their own corporate subculture during these periods of existence, which is expressed in their own language, customs and mentality, but also in doctrines, strategies and modes of action. Personnel receive these doctrines and methods of action in their initial training and are embedded in it from that moment onwards. This corporate culture with all views becomes deeply rooted within people, and it is very difficult to change or to get rid of deeply ingrained beliefs. Vacca illustrates this on the basis of the rational choice theory. This theory assumes that people regularly update their beliefs when new relevant information becomes available. In practice, this is less the case and people tend to dismiss information discordant with antecedent ideas [43].

These beliefs are important when a new phenomenon such as Cyber operations is introduced. The desired way of acting or approaching this new form of action differs for each part of the armed forces and is based on the experiences with the old doctrines. Reasoning is based on their own viewpoints which traditionally focus on acting in their own dimension: land, sea or air. Aspects of the existing doctrines are projected onto a new phenomenon such as Cyber operations. Such a mentality resulting from culture is not necessarily conducive to cooperation, a shared view at the approach or in the end, a joint action with associated doctrines, strategies and Standard Operational Procedures.

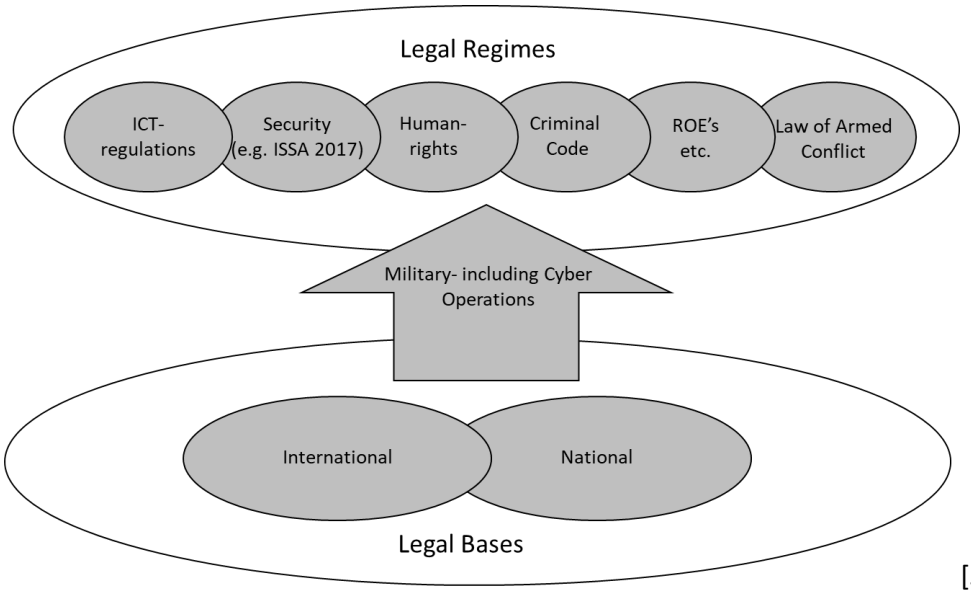
Legal Framework

In most countries the Armed Forces derive their right to exist from the constitution. In the case of the Netherlands, Article 97 of the Dutch Constitution [52]. This article states that in order to defend and protect the interests of the Kingdom, as well as for the maintenance and promotion of the international legal order, a military force is necessary and that the government has the supreme authority over these Armed Forces. The Dutch Constitution also mentions the three main tasks of Defense. The first task is the Defense of its own territory. The second task concerns the maintenance of the international legal order, which manifests itself mainly in (peace) missions. The third and final task is the support of national civil activities [52] [53].

Countries can have their Armed Forces only carry out tasks or operations if there is a 'legal base' [53]. This 'legal base' can have a national or international basis. An example of a Dutch national 'legal base'

is, for example, the Kingdom Act. This Act allows, under conditions, the use of violence by an armed guard while protecting the barracks. An international 'legal base' for the use of force is, for example, the Charter of the United Nations which states that a sovereign country has the right to self-Defense. This again under defined conditions. If a legal 'military' operation is performed on the conditions as mentioned above, various regimes apply which impose requirements and preconditions on the implementation. These are the so-called 'legal regimes' [53].

Legal regimes occur in different forms. They may consist of laws such as criminal law, treaties or agreements such as the rules of engagement during a mission, but also matters such as ICT regulations may apply during the execution of operations. Together, the ‘legal base’ and the ‘legal regimes’ form the ‘legal framework’ as shown in figure 5 under which conditions Armed Forces can perform their operations.



[53]

Figure 5: Legal Framework (Ducheine/Voetelink)

While performing operations within the Cyber Spectrum, the aforementioned bases and regimes apply. Players within the outlined paradigms of the Cyber Governance Framework must act according to this 'legal framework' as shown in figure 5. Each paradigm has its own 'legal base' and its own regimes to which it must conform. It should be noted that the separation between the paradigms is not equally sharp in all cases. Countering Cyber Terrorism, for example, can fall within the paradigms 'law enforcement', ‘Intelligence’ and in the paradigm 'offensive operations'. This depends on the nature and intensity of the conflict and several other factors. Although the concept of Cyber Terrorism is not unambiguously defined, as explained by Jarvis et al [54] [55], if an act defined as a possible terrorist Cyber-attack occurs, it will be necessary to find a definitive answer under which consultation the operation will be concluded. With such issues, well-organized governance is of great importance.

6 Dutch Defense Cyber Structure

6.1 Introduction

In this chapter the Dutch Defense Cyber Structure is presented. First the historical context of cyber within the Dutch Defense is explained. Next, different parties with a relation to cyber and their cyber role within the Dutch MoD are described after which they are plotted on the proposed framework. Finally, implications of the current governance structure is described.

6.2 Cyber: historical context explained

Since the eighties, Defense organizations have been busy developing Cyber capabilities. The most appealing examples are the United States, the United Kingdom and Israel. The Netherlands lagged far behind in that respect. It is not until 2009, after the media reported on this subject [56], that a signal regarding Cyber was picked up politically. Motions from members of Parliament, Mr. Knops (2009) and a second from Mr. Hernandez (2010), requested the then Minister of Defense to develop a 'Cyber Security Strategy' and to give substance to Cyber Warfare [57] [58] [59]. Mr. Hernandez requested that Defense would be given the leading role in developing the Dutch Cyber Security Policy. The government did develop and release a National Cyber Security Strategy, but decided that the Ministry of Justice & Security (J&S) should coordinate.

In the first National Cyber Security Strategy (NCSS 1) published in 2011 [60], the National Cyber Security Center (NCSC) took an advance on developments in Defense. This was referred to as 'response capacity' in this document, and it endorsed the possible offensive deployment within the Cyber Spectrum by Dutch MoD. A problem in developing the first Defense Cyber strategy was, according to Ducheine, the lack of an integral national strategic vision, a so-called 'grand strategy' [53]. Despite this fact, Defense had to develop a Cyber strategy. Therefore, in addition to the Constitution, which describes the three main tasks of Defense [52], the report 'Cyber Warfare' of the Advisory Council on International Affairs (AIV) [39] and the NCSS 1 [60] were used as the basis for the first version of the Defense Cyber Strategy. In the report of the AIV a triad of activities was mentioned which Defense should be able to develop in the Cyber domain. These were defensive, intelligence and offensive activities. Activities in the area of 'law enforcement' were not mentioned.

Meanwhile, 'Strategic Explorations' had taken place within the Ministry of Defense which described an integrated approach in the context of digital resilience for the first time within the Netherlands [36]. Also, the legal embedding, and thus the possible unconscious reference to 'law enforcement', was mentioned. Eventually the first version of the Defense Cyber Strategy was published in 2012 [40]. In this strategy, as a result of the use of the aforementioned source documents and developments, two more paradigms and the responsible units were mentioned, in addition to the offensive paradigm and the DCC. These are 'Intelligence' performed by the Military Intelligence and Security Service (MISS) [9], and 'Resilience' to be carried out by the Joint IT Command (JITC) [10] to be established. The duties of Royal Netherlands Marechaussee (RNLM) [11] were underexposed. The reason for this is most likely the organization's absence in the political and policy discussions regarding Cyber at the Ministry of Defense.

[9] In The Netherlands MISS is known as MIVD – Militaire Inlichtingen- en Veiligheids Dienst
[10] In The Netherlands JITC is known as JIVC – Joint Informatie Voorzienings Commando
[11] In The Netherlands RNLM is known as KMar – Koninklijke Marechaussee

To give substance to the main goals and the implementation measures arising from the Defense Cyber strategy, a Cyber Task Force was set up. The command over this Task Force, as well as the command over the newly created Defense Cyber Command, became a responsibility of the Army. This was probably also a decision based on political interests, to compensate the Army for the loss of its tanks in the previous Defense cuts.

In the revised Cyber Strategy of Defense of 2015, more attention was paid to the RNLM [41]. The task of the RNLM was seen as law enforcement in the context of public order and safety, and the testing of the legality of the deployment of the operational commands. With this, the fourth paradigm, as acknowledged by Ducheine, was formally endorsed. Also the Dutch 'International Security Strategy' had become a fact, in which the importance of the first two main tasks of Defense were endorsed, as well as the necessary attention for digitization and Cybersecurity [61]. The aforementioned principles justified the four paradigms and their players within the Cyber domain of Defense.

6.3 Dutch MoD, parties and their characteristics

Introduction

Although the Ministry of Defense as a department is founded on one shared objective, namely 'the security of the Netherlands', it is physically not one organization. Defense consists of various collaborating organizational units and sub-units, each with its own history and entrusted with highly specific tasks. In addition to the operational commands that are responsible for executing operations in their own dimensions, Defense also has a governance layer that is responsible for the policy making and two supporting elements (figure 6).

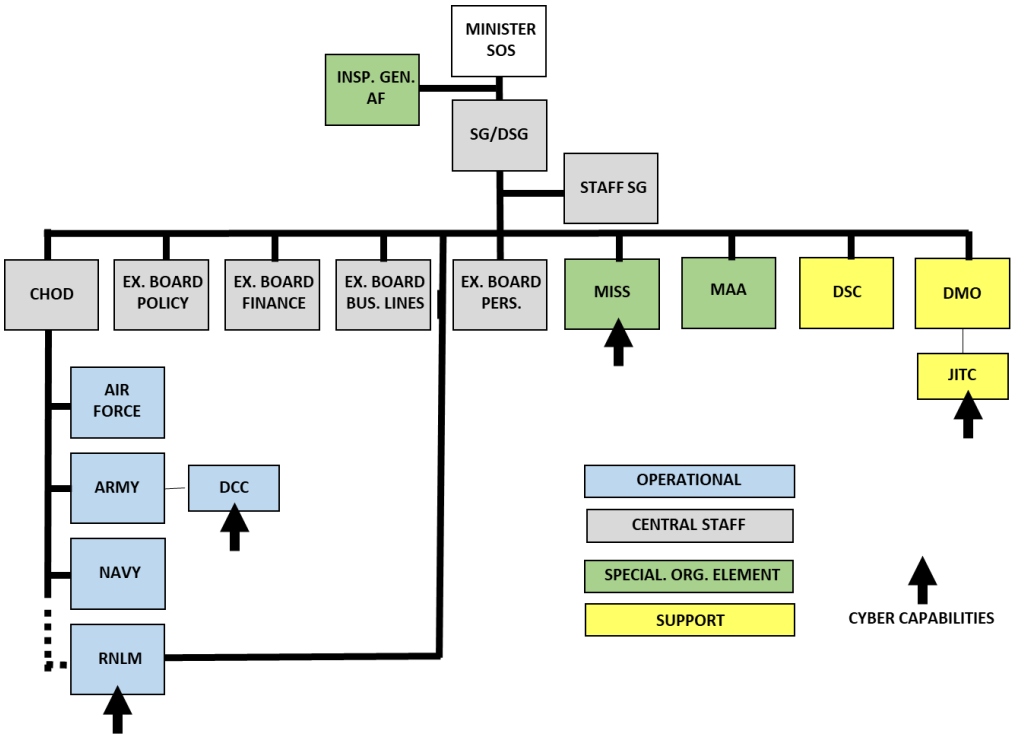


Figure 6: MoD structure & Cyber elements

The players within the four paradigms of the Cyber governance framework are spread over various parts of the organizational chart. See figure 6. In addition to 'their role' within the Cyber domain, they also fall hierarchically under a parent unit and thus also have all the characteristics of that unit or command.

As a result, the governance of the Cyber Spectrum within Defense does not consist of one organization or part of an organization. Because there is not one command line, the governance of cyber operations is spread out over different boards, of which the 'Cyber Governance Board' is the highest level. The name of this board used to be the 'Cyber Platform Defense'. Decision-making within this board takes place on the basis of consensus. The largest administrative contribution takes place through the 'Executive Board Policy' of the Central Staff. The board is either chaired by a member of the aforementioned department or by a Director of the Chief of Defense. Every player in the Cyber domain knows its own characteristics. The characteristics of all Cyber players within the Dutch MoD will be further elaborated in the following paragraphs.

Joint Information Technology Command (JITC) [12]
The JITC is responsible for the maintenance of all IT resources within the Dutch MoD. This concerns the operational and military IT resources that contribute directly to the execution of the tasks of the Armed Forces such as means of communication on ships and in vehicles. In addition to operational IT, there is also office automation and supportive IT. This concerns all IT resources indirectly contributing to Defense's primary tasks such as workplaces, printers, telephony and data centers.

The IT organization and the supporting IT services of Defense have a turbulent history. Since the creation of the Defense Telematics Organization (DTO) in 1997, the Ministry of Defense has centralized and merged the various IT elements. Defense does this for various reasons such as efficiency, cost reduction and to cope with the shortage of personnel. The last major reorganization took place in 2013, when JITC emerged in its current form. A couple of prominent characteristics of the current organization are that it has between 2,500 and 3,000 employees and that the age of the average employee is 54 years [62]. This means that JITC has a substantial and rather old workforce for an IT company. Most of the staff are no longer able or willing to follow all the trends in the market. This has consequences for the necessary IT services to Defense in relation to its primary tasks. Reorganizations, several attempts at sourcing of which the last one is currently taking place and the pressure of the market have taken their toll. In that perspective, the question is whether having an own IT company for Dutch MoD remains a viable goal. This, also in regard to the increasing importance of IT for an information processing company such as Defense.

Regarding Cyber, the JITC has two important elements, namely the Defense Computer Emergency Response Team (DefCERT) and the Security Intelligence Operations Center (SIOC) [13]. DefCERT exists since 2013. The main task of this organization is 'incident response' on location. SIOC was founded in 2014. SIOC's tasks are to gain insight, to monitor and detect and to mitigate the threat or attack in collaboration with the Network Operations Center (NOC). DefCERT and SIOC have recently been merged into the Defense Cyber Security Center (DCSC), bringing together all the functionalities to mitigate Cyber threats in the context of Cyber Resilience [63].

[12] In The Netherlands JITC is known as JIVC – Joint Informatie Voorzienings Commando
[13] The functionalities of the SIOC are similar to those of a Security Operations Center (SOC)

In a draft of the most recent version of the Defense Cyber Strategy (2018) [64], it was foreseen that this DCSC would be placed under the Defense Cyber Command. This was done in order to accommodate offensive and defensive cyber capabilities in one organization [63].

The JITC has a hierarchical structure with a large number of (sub)departments. These departments arose on the basis of their specialization in the IT field and the type of support they have to offer to the operational and supportive Defense units. Its structure can be classified as a mix of a 'professional bureaucracy' with the 'divisional structure' according to Mintzberg [45]. The processes to produce the desired IT products have to a large extent been standardized on the basis of (inter) national IT standards and agreements.

The culture of JITC is characterized by its specialized discipline and the personnel composition of each specific (sub)unit. JITC's IT field has a wide variety of specialist fields in which the staff work on a solo and task-oriented basis. In general, this type of employee, who can partly be described as 'nerdy', may not adhere to the traditional military culture. Furthermore, the JITC has a large number of civilian employees in the workforce compared to the number of military personnel. This influences the working method and the culture in several ways. Whether this is positive or negative depends on who is asked.

Due to the defensive nature, no legal framework, with the exception of the generic provisions, for example from the GDPR, is required for the execution of the tasks of the JITC in relation to Cyber Operations. In general, no legal restrictions are imposed on the protection of 'private' IT networks. This also applies to the Defense network. The DCSC, as part of the JITC, does not go further in its task performance than the identification and mitigation of digital threats. After securing the Defense Environment, DCSC will report the incident to the RNLM or the MISS who will take care of further processing.

Royal Netherlands Marechaussee (RNLM) [14]

The RNLM was founded in 1814 by King William I. He wanted to form a police corps following the example of the French Gendarmerie. The RNLM is a police force with a military status. The latter guarantees a thorough training and armament, but also strict discipline. This is why the RNLM distinguishes itself from the National Police. Until 1969 the RNLM was a full part of the Army. In 1998 the RNLM was granted the status of independent Armed Forces.

Because the RNLM performs an important part of its duties for departments other than Defense, it operates under different mandates and legal frameworks. The majority of the job responsibilities of RNLM, fall under the Ministry of Justice & Security (J&S). In addition, the Ministry of Interior Affairs also plays an important role. The previous commander of the RNLM stated that the main organizational purpose of the RNLM is the guarantee of the security of the state [65]. This stands in sharp distinction with the organizational purpose of the National Police that guarantees security on the streets.

Since 2005, the RNLM has been working on the transformation of its organization from a 'geographically oriented organization' to an 'information-driven organization'. One of the main goals for this change was that no RNLM-personnel goes out on the street, without bespoke instructions. To

[14] In The Netherlands RNLM is known as KMar – Koninklijke Marechaussee

make that happen, every single employee will be supported by the essential information systems, necessary for the performance of his or her specific task. This allows the organization to become nimbler and more adaptable, and thus meet the demands of the ever-changing surroundings in the public safety and security domain. In this way, the RNLM can continue to act at the highest level, and give substance to its three strategic goals formed by the 'border police task' or 'border control task', 'security and surveillance' and the 'international and military police tasks'.

No Cyber strategy has yet been developed that adequately supports the RNLM's tasks. The RNLM must be able to give substance to the objectives set out in its strategic vision in an adequate manner, with both conventional and Cyber resources. In addition, the RNLM is responsible for checking whether a deployment of the Armed Forces was proportional and lawful. Even when this concerns an engagement with cyber weapons. This movement is currently under development and a first memorandum to claim budget and to give substance to this evolution has been written. With regard to the Cyber discipline, the RNLM is still in an immature stage [66].

The RNLM, as part of the Defense organization, has a hierarchical structure. Due to recent developments, this hierarchy has evolved to a relatively 'flat' organization. Using Mintzberg's concepts [45], the organizational structure can be characterized as a mix of 'professional bureaucracy' with the 'divisional structure'. The RNLM has a high standard of processes that must be carried out according to established procedures. Nevertheless, a high degree of specialist knowledge is required from employees and managers. This is expressed in the organization by two staff elements at tactical and strategic level and a number of operational or executive organization elements spread over the country.

The culture of the RNLM is largely characterized by its historical establishment, which is, obviously, military by nature. General characteristics in military organizations are loyalty, team spirit, discipline and flexibility. However, because the RNLM is also a police organization, it also has the characteristics of such an organization. Matters such as individualism, (healthy) distrust, secrecy and autonomy can be found in such a culture [67]. Uniting cultural aspects of both military and police organizations in the RNLM renders a rare blend of aforementioned cultural aspects. This blend, creates an environment in which an employee of the RNLM can become an expert law enforcement official, who can additionally be deployed in unstable situations where higher levels of the spiral of violence may be needed.

The RNLM carries out its police duties on the basis of Article 4 of the Police Act 2012 [42]. This constitutes the legal base as described by Ducheine et al. The legal regimes that apply are the Criminal Code [68], the Code of Criminal Procedure [69] and the Aliens Act 2000 [70]. In the context of Cybercrime, the Computer Crime Act III is applicable.

Military Intelligence and Security Services (MISS) [15]

The Military Intelligence and Security Service (MISS) was established in the 1980's, by merging the intelligence services of the three Operational Commands of the Army, Air Force and Navy. In this way, in 1988 the Military Intelligence Service (MIS) was originated. With the introduction of the Intelligence and Security Services Act 2002 (ISSA 2002) and under influence of the 'supervision body' on the 'services', in 2002, the name was changed to MISS.

[15] In The Netherlands MISS is known as MIVD – Militaire Inlichtingen- en Veiligheids Dienst

Within the Ministry of Defense (MoD), the MISS is a so-called Special Organization Element (SOE) and is directly placed under the Secretary General of Defense (SG). In addition to the management of the SG, political guidance is also exercised by the Prime Minister assisted by the Council for the Intelligence and Security Services (CIS) [16] [71]. Supervision of the activities of MISS is carried out by various boards and committees, including the Committee on the Intelligence and Security Services (CISS) [17] [72].

The MISS works closely with the general security service, the GISS. They have a common unit, the Joint SigInt Cyber Unit (JSCU) that originated from the National Signal Intelligence Organization (NSO). In various areas within the intelligence spectrum, there is cooperation and exchange of information with foreign services [66] [73]. The MISS is a respected player within the Cyber discipline. In addition to the JSCU, the MISS itself also focuses on Cyber Intelligence. That this is not without merit, has been shown by two recently booked successes which have been made public. This is a joint success of GISS and MISS concerning the penetration of the systems of a Russian hacker group called 'Cozy Bear' [74] and very recently the thwarting of a hack at the Organization for the Prohibition of Chemical Weapons (OPCW) [75].

The organizational structure of the MISS is a hierarchical structure with a large number of (sub) departments. These departments are organized on the basis of their specialism or area of special interest. The MISS, like almost all professional organizations within the Dutch MoD, can be characterized as a mix of professional bureaucracy with the divisional structure [45].

With regard to the culture that prevails at the MISS, it can be noted that, due to the often highly classified activities, there is a ‘closed’ culture. There is certainly a high degree of shielding from the outside world. In many cases, this shielding also applies internally between the various employees. During an interview for this thesis it was indicated that this way of working, where employees can’t discuss their work (or even the fact that they work at MISS) with other people, and not even at home, puts a lot of pressure on the employees. The culture can therefore be characterized as closed whereby employees collaborate and share information on the basis of 'need to know' [76].

The legal base for the tasks of the intelligence services as described by Ducheine et al [53] is formed by the ISSA 2017 [77]. This law describes in Article 8 and 10 why intelligence services exist. The legal regimes that indicate the activities, including the authorities of the intelligence services, are also described in the ISSA 2017. This ISSA applies exclusively to the Intelligence Services. Only people who are employed by such a service or who carry out work for one of these two services can, for the time they work at the service, claim the authorities arising from the law.

Defense Cyber Command (DCC) [18]

The Defense Cyber Command (DCC) was established in 2014. However, it took until 2017 (initially planned for 2016) before this unit was fully operational. The first plans to form the DCC took shape in the policy memorandum ' Defense after the credit crisis: a smaller Armed Force in a troubled world’ [78] and in the Defense Cyber Strategy of 2012 [40]. In order to further develop these plans into an

[16] In The Netherlands CIS is known as RIV – Raad voor de Inlichtingen- en Veiligheidsdiensten
[17] In The Netherlands CISS is known as CTIVD – Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
[18] In The Netherlands DCC is known as DCC – Defensie Cyber Commando

actual formation of DCC, a Task Force Cyber was set up. Despite the cutbacks at that time at the Ministry of Defense, funds were assigned for the strengthening of Cyber capabilities, thus substantiating the political will to invest in the Cyber field.

From 2012, the Task Force initially focused on operationalizing the Defense Cyber Expertise Center (DCEC) in 2014 and then the Defense Cyber Command. The current DCC consists of 3 departments. These are the DCEC as knowledge center, Operations (Ops) as the unit that provides support to the operational units of Dutch MoD and Technology (Tech) as the unit that develops the Cyber applications. With these units, the DCC gives substance to the offensive Cyber capacity of Defense. Although the ambitions for the DCC at MoD ranged from the overall coordination of Defense Cyber capabilities to the support of missions, the focus now seems to be placed on the latter.

The DCC is currently engaged in two organizational movements. This concerns the organizational transfer of the DCC from the Army to the Chief of Defense (CHOD) and an internal reorganization. As of January 2019, the DCC will be under direct command of the CHOD. The expectation within Defense is that this will create an unambiguous owner and thus better coordination within the Cyber Domain of Defense. The internal reorganization involves the merging of the Ops and Tech departments into one new Cyber Operations department (CyberOps) and the renaming of the DCEC department to a more common name within the Ministry of Defense, the Cyber Warfare & Training Center (CWTC) [79].

Within the Cyber Governance Framework, DCC is responsible for offensive Cyber operations. Due to several reasons an actual deployment within this area by DCC has not yet taken place. One reason is that the unit has only recently become operational. Additionally, the DCC still lacks a large amount of specialist staff and there are uncertainties about the modus operandi of the DCC. In regards to the last, the issue is, that for both the development and the preparation for deployment of an offensive cyber weapon, strategic intelligence is necessary. Based on the current legal frameworks, the DCC itself cannot provide for this [66]. Furthermore, during its existence, the Defense Cyber Command was lacking a large mission and the possibility for an actual deployment. All this has meant that no real operational offensive achievements can be reported yet.

The DCC shares the traditional Defense organization structure, a hierarchical line-staff organization. The Defense Cyber Command can be typified as a mix of professional bureaucracy with the divisional structure, as well as most other Defense units within the Dutch MoD [45].

In terms of culture, the image that is sketched by the interviewees varies. Some of them indicated that the culture of the DCC had characteristics of the Army culture, namely a formal, procedural culture [80]. This could possibly have been caused by the founding of this unit. Especially at the start, the Task Force Cyber which was responsible for the foundation, was mainly led by Army officers. Another part of the respondents indicated that there was clearly a mixed culture of all Armed Forces including civilian workers [79]. In view of the short period of existence, it seems that a true corporate culture has yet to develop. Elements such as professionalism and specialism will certainly play a role here.

For the DCC, the 'legal framework' consists of legislation that applies to every operational Defense unit. A deployment of the Armed Forces is only possible after political decision-making and permission. This applies to all three tasks defined in the Dutch Constitution [52]. In this respect, the 'legal base' for acts of war, is formed by the Dutch constitution and the UN charter [52] [81]. This is

considered as the right to wage war (Jus ad bellum). During a mission or war (Jus in bello) the legal regimes apply such as the 'Law Of Armed Conflict' (LOAC) and the Rules of Engagement (ROE's) [53]. Offensive Cyber Operations to be executed by the DCC, can only take place under the aforementioned legal framework.

6.4 Position within the framework

When the Units of Defense that have just been described are plotted on 'the framework', it becomes clear that all paradigms as described by Ducheine et al [2] are provided with an organizational unit within Defense, as shown in figure 7. This concerns the current situation (plot date December 2018). What is not shown, are the possible shifts that are currently taking place, as a result of reorganizations and changes. These reorganizations will, as it appears now, not cause any shifts within the paradigms but more shifts in the horizontal governance layer of the MoD.

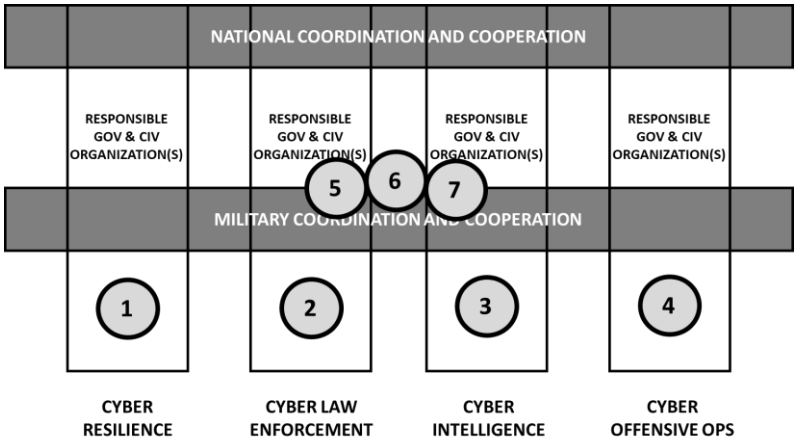


Figure 7: The framework versus the players

1. Joint Information Technology Command (JITC)
2. Royal Netherlands Marechaussee (RNLM)
3. Military Intelligence & Security Service (MISS)
4. Defence Cyber Command (DCC)
5. Cyber Governance Board (CGB)
6. Cyber Coordination Council (CCC)
7. Central Staff: Executive Board Policies

6.5 Implications of current governance structure

Introduction

In 2017, the Defense Cyber Strategy [40] [41] was evaluated on behalf of the Ministry of Defense. This evaluation, which was carried out by an external agency, resulted in an internal report [82]. In this report a number of problems were identified, which in this study have been combined into three major areas of attention. These are 'Personnel', 'Equipment' and 'Collaboration'. The findings from this report will be used in this study to see whether the identified issues are due to governance, or related aspects such as structure, culture or legal framework. It will also be examined whether the same problems were also observed in the German situation. The problem areas will be elaborated and explained in the following sections.

Personnel

Due to the economic boom, getting and retaining well-qualified and motivated staff is a problem for Dutch MoD. Attracting good Cyber or IT specialists is even more difficult. Educated staff in the Cyber field is in high demand in the commercial sector that can additionally offer candidates far better wages. In that sense, the Ministry of Defense cannot match the private sector. The difficulty of obtaining new recruits applies to all categories of Cyber related personnel within the Dutch MoD, i.e. professional soldiers, civilian personnel and reservists. The problem touches all four paradigms within the Cyber Governance Framework. With regard to recruiting personnel, the four Defense organizations are therefore looking for the same specialists and are in a sense competitors of each other. In daily practice it is also observed that good staff are lured away and taken over by the most attractive employer. This does not benefit the Defense organization as a whole. The personnel problem goes even further than just the Cyber branch. The staff working in the Cyber field is in the basic IT staff with a number of specific skills. Taking measures alone to recruit more Cyber personnel or taking measures to retain Cyber personnel leads to sub-optimization within the required amount of personnel needed for both the Cyber and Information Technology fields [82].

Human Resource processes within Defense are not flexible enough to recruit staff quickly. Due to fixed and rigid processes and regulation it is also hard to apply tailor-made solutions for recruitment and retention. This way of working does not make it easy to build a healthy and flexible workforce for the Cyber- and IT domain [82].

Equipment

With regard to the problem of equipment, it can be said that the acquisition of equipment is a difficult process. Due to the cutbacks, processes have been set up to prevent unnecessary expenses. These bureaucratic processes have manifested itself in a large number of control layers. This difficult acquisition of required resources and their implementation within the MoD does not benefit the management and innovation within the Cyber discipline; a field in which technological developments advance quickly and innovations follow each other in rapid succession. Standing still means moving backwards, certainly in relation to a potential, malicious and rich opponent who can afford the latest state of the art technology. Again, this is not only a problem for the Cyber field, but also for Information Technology in general [82].

Collaboration and cooperation

In the Cyber strategies of Defense of 2012 and 2015 [40] [41], goals were set in regard to collaboration and cooperation between the organizations of MoD in regard to a common Cyber approach. In practice, despite all political attention, these matters are more difficult to achieve than initially assumed. From the interviews which were held as input for the VKA-report [82], it appears that Cyber, its definitions and its necessity for the MoD processes, is not clear to all parties involved. At the same time, the tasks, responsibilities and authorizations, as envisaged for the various parties, are not clear to all players. Mandates that form the basis for the tasks, are not unambiguously understood. These matters affect mutual understanding and cooperation. The assumed legal frameworks offer no solution to this, but in fact they bring out the contradictions and responsibilities more clearly to the parties involved. For two organizations, a legal framework is in place, concerning the MISS and the RNLM. For the DCC this is not the case. The deployment during missions is supported by the Constitution, Article 100 and additional agreements such as Rules of Engagements (ROE's). However, a legal basis for obtaining the intelligence and information supportive to all three

main tasks of Dutch MoD, demands a broader legal framework including mandates. This is also expressed in the comments from DCC, stating that cooperation with countries such as the UK and Denmark is difficult because these countries have organized their Cyber Capacities within the Intel Community.

7 German Defense Cyber Structure

7.1 Introduction

In this chapter the German Defence Cyber Structure is presented. First the historical context of cyber within the German Defense is explained. Next, different parties with a relation to cyber and their cyber role within the German MoD are described after which they are plotted on the proposed framework. Finally, implications of the current governance structure is described.

7.2 Cyber: historical context explained

Germany, like the Netherlands, has high ambitions regarding 'digitization' or 'digital transformation'. Both countries want to play a leading role in Europe when it comes to the use, but also the production of digital resources. Obtaining a leading European position will strengthen respective economies, but ultimately also that of Europe as a whole. In Germany, the Chancellor, Angela Merkel has personally asked for attention for the digital spectrum, actively taking part in various forums to strengthen digitization in Germany [83]. In addition to the positive effects that a high degree of automation can yield a country, downsides can also be observed. A high degree of digitization leads to a multitude of digital vulnerabilities. Digital resilience is therefore absolutely essential to realize the ambition of 'digital transformation' [84].

To give substance to the resilience of Germany in the digital domain, a first edition of the Cyber Security Strategy was issued in 2011 [85]. The latest version appeared in 2016 [18]. In Germany, the coordination of National Cyber Security is a responsibility of the Ministry of the Interior. In the latest version of this strategy, it is indicated how this Ministry intends to give form to the protection of citizens and businesses with respect to Cyber Security. The overall purpose is translated into four so-called 'Handlungsfelder' or 'action areas', namely:" 'safe and independent use of the digital environment', 'cooperation between the German state and the economic sector in the cyber field', 'building an effective cybersecurity architecture in the public sector' and 'making Germany a central actor in the European and global cyber policies' [18] [84].

In order to fulfill its Cyber Security tasks, the German Ministry of the Interior has three dominant parties within its organization. These are the Federal Criminal Police Office (FCPO) [19], the Federal Office of Information Technology Security (FOITS) [20] and the Federal Constitutional Protection Office (FCPO) [21] [84]. The FCPO, is a police organization charged with fighting Cybercrime [86]. The FOITS investigates security risks associated with the use of IT and develops preventive security measures [87]. In relation to cyber security, the FOITS has two important elements in its organization. These are the National CERT [22] [88] and the National Center for Cyber Protection [23] [89]. The National Center for Cyber Protection is responsible for sharing information about Cyber security between all relevant players in Germany, including the German MoD and the intelligence services. The last party is the Federal Constitutional Protection Office (FCPO). This organization is a Security Service and in terms of tasks it is comparable to the Security Section of the Dutch GISS. Its task in general is the Protection of the Constitution [90].

[19] In Germany FCPO is known as BKA – Bundes Kriminal Amt
[20] In Germany FOITS is known as BSI – Bundesamt für Sicherheit in der Informationstechnik
[21] In Germany FCPO is known as BfV – Bundesamt für Verfassungsschutz
[22] In Germany National CERT is known as CERT Bund
[23] In Germany the National Center For Cyber Protection is known Cyber Abwehr Zentrum

In 2016, next to the National Cyber Security Strategy, a 'White Paper' was issued by the German Ministry of Defense [91]. This paper describes the German Security Policy and the future of the 'German Armed Forces'. In the Security Policy, the challenges that Germany faces in the Cyber and Information Domain are specifically addressed. In the future vision of its Armed Forces, it is indicated that Germany wants to develop capabilities in the Cyber- and Information Domain in order to anticipate to this Cyber threat. These plans have already been partly realized and will be further elaborated on in the following paragraphs.

The German Ministry of Defense already wrote its own Cyber Strategy in 2015 [92]. However, this has never been made public. This is due to the sensitive information contained within this document [6]. In particular, the information about offensive cyber operations is politically sensitive. Various political activist associations managed to obtain this strategy and published it on their websites [93] [94]. The Defense Cyber Strategy, like the National Cyber Strategy, makes clear what the German MoD aims for with its Cyber capabilities, using five so-called action fields. These fields are: 'the contribution to national security', 'participation in international frameworks, e.g. NATO', 'the development of Cyber space as field of operations', 'the use of opportunities that cyber space offers' and 'reducing the risks of Cyber space'. In addition to Cyber defense, the strategy also deals with offensive Cyber deployment. Initially, this offensive deployment is described as part of the defense. Additionally the deployment of offensive Cyber resources is explained as complementary to conventional weapon systems [93] [94].

National coordination of Cyber security is complicated by Germany's history and by its federal institutions. Both state organization and legislation hamper effective decision-making and therefore prevent cooperation. This also influences the role that Defense can and may play in the field of Cyber security in a national perspective. This is partly due to the history of Germany [3] [5]. After the Second World War, both the German establishment and German legislators had to prevent Germany to ever start a war again. Although this approach has proven to be successful, it frustrates the decision making- and cooperation process. This situation is not likely to change soon. Where modern times and society offer room for reforming the state system and the legislation, internal layers of governance make it difficult to change the status quo. The current administrative layers offer work and status to many civil servants, who are in effect not eager to change [5].

7.3 German MoD, parties and their characteristics

Introduction

The German Armed Forces in its current form have only developed since 1955. After the Second World War, a discussion took place about whether or not it would be morally responsible to let Germany have their own Armed Forces. From 1956, the construction of the independent German Armed Forces took shape. The reunification of Germany in 1990, led to many reforms within the German MoD, including the dissolution of units on the basis of a large-scale cutback and a reorientation of its tasks. After 2001, changes of Germany's Security Policy have resulted in further reforms that have led to today's MoD [95] [96].

Due to its history, Germany is very reluctant to deploy its Armed Forces. In terms of the task of the German MoD, the operational deployment is performed by military personnel. Support for the Armed Forces is provided by Defense organizations which are mainly staffed by civilian workers [3] [97]. This support includes 'infrastructure', the 'purchase of equipment and material', '(national) IT

support' and 'HR services'. The implementation of this support is often accompanied by complex and bureaucratic procedures. In addition to organizational restrictions, the German Armed Forces also have restrictions that arise from legislation. These restrictions consist of laws that directly concern the Armed Forces, but also legislation that indirectly restricts the powers of the German MoD [98]. In the first place there is the Constitution (Art. 24 & 87a GG) [99]. This imposes restrictions on the deployment of the Armed Forces. In general, only defensive deployment is permitted and the legislature must give permission at all times. The composition and mission of the German MoD is also established in the Constitution [100]. This is in contrast to the other departments. Changes to these issues are therefore difficult, cost a lot of time and must be approved by Parliament [5]. The division of competencies can also be seen in the organizational structure of German Defense. There is no direct command relationship between the Ministry and the operational organizations. In the context of missions, the required troops are transferred to the 'Operations Command' [24] by means of a 'Transfer of Authority'. In case of war, the final responsibility lies with the Chancellor. All commanders involved in execution and command hold the same rank. At the strategic level, there is therefore no 'real' command structure. Delivery of services takes place mainly on the basis of negotiation and consensus [101]. For the structure of the German MoD, see figure 8.

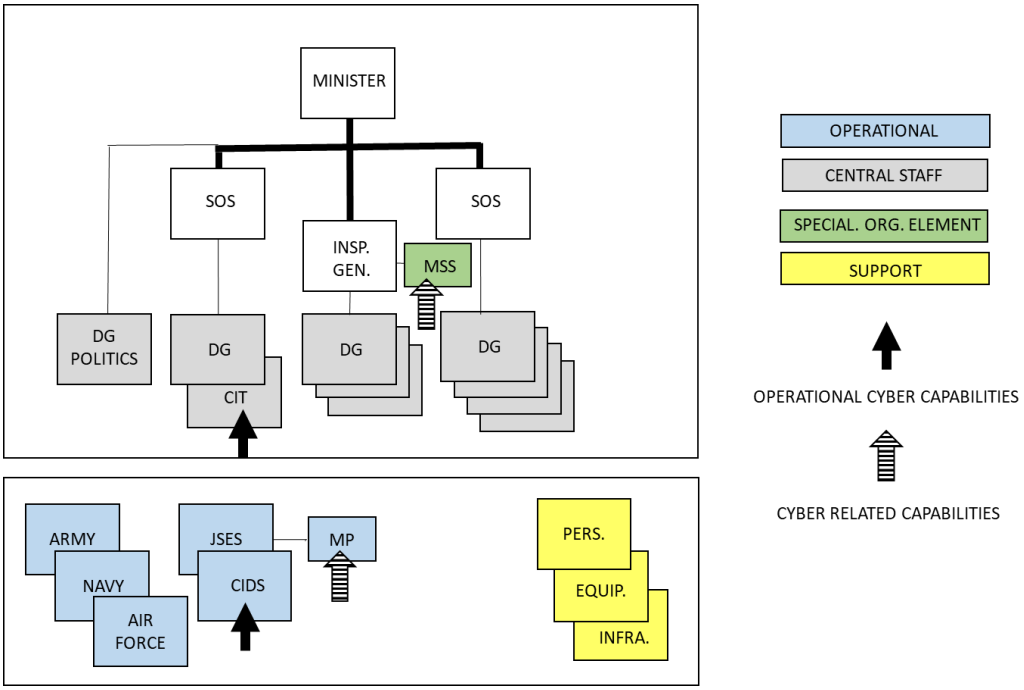


Figure 8: German MoD structure & Cyber elements

The national emergency response is a responsibility of the Ministry of the Interior, including in case of a Cyber-attack. This department is responsible for the protection of vital processes including infrastructures and national emergency response [3] [4] [5]. The National Center for Cyber Protection as part of the Ministry of the Interior, coordinates with many public and private parties [102] including the MoD. Assistance from the MoD in case of National Security can only be provided on the basis of Article 35 of the Constitution and after approval of Parliament [99]. Germany acknowledges strict separation of responsibilities between military and civilian services. There are a lot of aspects

[24] In Germany 'Operational Command' is known as 'Einsatz Führungs Kommando'

which have repercussions on the formation and embedment of Cyber units within the German MoD. These are, the formation of the German Armed Forces in relation to its history, the restrictions it knows from legislation, organizational limitations and the ambition from the German government in the field of the Digital transformation. How these aspects reveal themselves within the paradigms as interpreted by Ducheine et al. [2] is explained in more detail in the following paragraphs.

Cyber- and Information domain of German MoD

The National Security Strategy and the vision for the future of the German Armed Forces (White Paper 2016) [91] state that the Cyber and Information Domain require special attention in relation to the ambitions of Germany as a country. In order to give substance to this vision, a so-called Day Order [103], two plans or 'Leitlinien' [92] [104] and a report were written [105]. Based on these documents the realization of the necessary units was started. These (partly) new units concern the Directorate General Cyber and Information Technology (CIT) and the Cyber and Information Domain Service (CIDS). The latter concerns a new independent Armed Forces section that will ultimately consist of approximately 15,000 people.

There were three basic thoughts underlying the structure of the units and the way in which they had to cooperate. First, there was the idea that the German Armed Forces had to set up a complete planning and maintenance cycle for the Cyber and Information Domain in order to function properly. This was interpreted as: 'plan, build and run' [3], not to be confused with the internal set-up of the CIT department. The second thought concerned the units that were required to fill in the cycle. These units were the DG CIT [25] at the strategic level, the FOEITISS [26], at the executive logistics level and the CIDS [27] at the executive tactical / operational level. The basis of the IT landscape of the German MoD is, as in any modern organization, formed by office automation. This layer is standard equipment for the units that work in the Cyber and IT sector, but is also a link in the Cyber chain. It is supplied by AFI [28], the IT Company of the German MoD and the German Government. In order to defend and maintain the entire IT environment of Defense, this layer must not be forgotten and therefore AFI is an integral part of the process [104]. The process and associated units are visualized in figure 9.

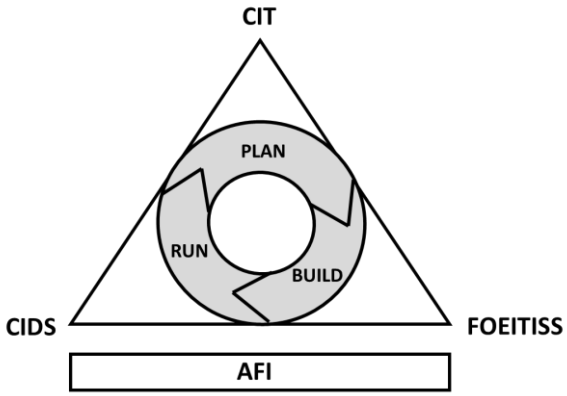


Figure 9: 'Plan, Build, Run-cycle' & involved units

[25] In Germany DG CIT is known as Abteilung CIT – Abteilung Cyber und Informations Technik

[26] In Germany FOEITISS (The Federal Office of Armed Forces Equipment, Information Technology and In-Service Support) is known as BAAINBw – Bundes Amt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr

[27] In Germany CIDS is known as Kdo CIR – Kommando Cyber- und Informationsraum

[28] In Germany AFI (Armed Forces IT) is known as BWI – Bundeswehr Information Technologie

The final thought underlying the structure of the units and the way in which they had to cooperate concerned the way in which German MoD wanted to give substance to information dominance in the operational and tactical domain. The basic idea was that by combining two elements, 'Strategic Reconnaissance' and 'IT Operations', the complete electromagnetic spectrum could be controlled from one source and thus one vision. From this line of thought, the establishment of the new Armed Forces has arisen, namely the CIDS [4].

Directorate General Cyber and Information Technology (CIT) [29]
In order to be able to support the 'plan, build and run' cycle on a strategic level, the Directorate General Cyber and Information Technology (CIT) became fully operational in 2017. This new DG within the Ministry of Defense originated from the already existing DG Equipment, to which a number of new elements have been added [3] [105]. DG CIT is headed by a Chief Information Officer, a new role that has been introduced in the German Armed Forces together with the CIT. The CIT consists of two departments, the CIT 1 department which is charged with the 'strategic planning' and the CIT 2 department, which takes care of the 'build' and the 'run'. The various subsections of CIT 1 and 2 respectively are structured in such a way they can contribute to the total process for which the department is responsible [3] [6].

One of the goals of the DG CIT is to ensure the entire Armed Forces become aware of the fact that Cyber and IT are more than just digital commodities and not only of crucial importance for the IT department [104]. The CIT has also set itself the goal of implementing three issues in the field of Defense IT management. This primarily involves standardizing the existing resources and then evolving. The latter means that the configuration is kept up-to-date. Finally, the DG CIT wants to innovate, which means that IT resources that the Armed Forces cannot think of themselves are added to the resources that Defense has at its disposal [3] [104].

CIT 1 includes a couple of notable sub-departments. The Digital Transformation Bureau, which deals with the role of CIT in relation to the digitization of the German Armed Forces, is one of them [83]. In addition, CIT 1 also has a sub department which is responsible for Innovation [106]. In this way the innovation process within CIT 1 is supported by the strategic level of the IT organization. Within CIT 2, sub departments are created which, from the role of 'build' and 'run', create conditions for the protection of the IT systems of the Armed Forces, the implementation of defensive Cyber protection and Encryption [6].

Cyber and Information Domain Service (CIDS) [30]
From 2016, the German MoD is working on the construction of the Cyber and Information Domain Service (CIDS). The expectation is this new part (Command) of the Armed Forces will be fully operational by 2021. It will consist of approximately 15,000 employees. The CIDS is designed in such a way it can perform the complete information value chain and execute so-called 'effect-based operations'. In other words, the CIDS can create effects and deliver results on the battlefield without the use of conventional weapons [3] [4] [105].

[29] In Germany DG CIT is known as Abteilung CIT – Abteilung Cyber und Informations Technik
[30] In Germany CIDS is known as Kdo CIR – Kommando Cyber- und Informationsraum

The CIDS actually consists of three units that complement each other in terms of task execution within the information domain. The first unit is the 'Strategic Reconnaissance Command' with the task of reconnaissance and the creation of operational effects. The second unit is the 'Communication & Information Systems Command' (CIS Command). Their task is to support the 'command & control' and the support of troops in general by providing IT services. The third unit is a 'Geo element'. This unit is seen as a binding factor and also includes the presentation layer. These three units are governed under singular command, so that all proceedings in the entire information domain are carried out under the responsibility of one commander. This commander is also responsible for the personnel aspects of all staff within the CIDS. This concerns, among other things, training and career counseling [3] [4].

The CIDS can carry out operations and obtain ascendancy in all areas of the electromagnetic spectrum. By making its communication systems resilient the CIDS thinks it can resist enemy attempts of intervention. The effects are achieved by being dominant in three areas:

- Electronic warfare is the military action involving the use of electromagnetic energy to control the electromagnetic spectrum or to attack the enemy. It can be used within all Operational Commands. EM Warfare can be used to influence confidentiality (by listening and sounding) and to influence the availability (by disturbing);
- Information Warfare can be used as a tactic to spread fake news in order to mislead opponents and or even influence allies or other foreign countries and is proven to be a very effective tactic to manipulate;
- Offensive operations within the cyber domain are operations with digital means in order to disrupt, deny, degrade, manipulate or destroy the opponent's systems, infrastructure and data.

These three areas combined creates an information dominance that should help win the battle in this spectrum [3] [4]. For a visualization of this vision: see figure 10.

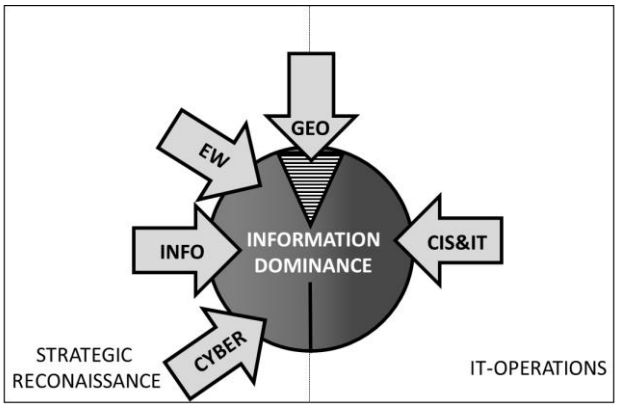


Figure 10: Obtaining Information Dominance by CIDS

The specific Cyber elements of the CIDS are both located in the Strategic Reconnaissance Command (SRC Cmd) and in the Communication and Information Systems Command (CIS Cmd). The Cyber Operations Center is located within the SRC Cmd. This is the part of the CIDS that deals with offensive Cyber operations as part of the Defense [4] [84] [105]. The latter must be specifically mentioned, because Germany is not allowed to carry out offensive operations under the constitution [99]. The

Cyber Operations Center has existed since 2009 and was known as the Computer Network Operations team also then residing under the Strategic Reconnaissance Command [84].

Within the Communication and Information Command the Cyber Security Center can be found, which is also the CERT of the German MoD. This organizational unit is responsible for the protection of the MoD IT systems. In addition, this center coordinates and disseminates information about Cyber-attacks internally, as well as externally Defense. This is done with the Cyber Defense Center of the Ministry of the Interior [4] [5] [6]. Furthermore, within the CIS Command there is also the Software Competence Center that develops and builds its own secure software for the German MoD [4] [105].

The remaining paradigms

The CIT and the CIDS mainly give substance to the 'Resilience paradigm' as introduced in the framework of Ducheine et al [2]. To a lesser extent, they are active in the Offensive Cyber and the Cyber Intelligence domain. There are units within the Strategic Reconnaissance Command of the CIDS that collect operational and tactical intelligence and there is a unit for the development of offensive cyber operations. This makes the Cyber and Information Domain Service active in three of the four paradigms. The paradigms of 'Law Enforcement' and 'Intelligence' in Germany remain underexposed within its MoD. Intelligence in this perspective is collected and processed by an Intelligence Service or an equivalent organization and not by an operational reconnaissance unit.

Law Enforcement

The German Defense does not conduct cyber activities in the 'Law Enforcement' paradigm. This is a task that has been assigned to the civil police in Germany. This can be at Federal level or at the level of a 'Bundesland'. This is laid down in the Constitution. The Military Police [31] may support an investigation by doing 'on site' research in case the Armed Forces are involved, for example in the context of an incident or a Cyber deployment by the Armed Forces. In that case the MP collects evidence and transfers this to the Public Prosecution Service [98]. The MP does not carry out independent investigations into the legitimate use of (Cyber)weapons. This, in Germany, is at the discretion of the military commander. When the military commander has doubts about legality, he makes a declaration to the Public Prosecutions Department, which then orders the prosecution [4] [5]. To this end, Germany has two sites of the Public Prosecution Service which are competent for this purpose. This concerns Kempten for general affairs and Karlsruhe for matters in which International Law (UN) is at stake. When necessary, the MP can assist with the on-site investigation. In the hypothetical case Cyber weapons were used, the forensic department of the CIDS can provide support since the MP lacks this kind of knowledge and experience [98].

Intelligence

The Military Counterintelligence Service (MCS) [32] is located within the German MoD. This service is responsible for the protection of Defense and its interests. The information that the MCS collects and processes should all be seen in light of contribution to this protection. The same applies to the activities that the MCS develops in the field of Cyber. These activities are deployed when malicious (internal or external) parties pose a threat to the German Armed Forces [107]. In this sense, this service cannot be compared to the Dutch MISS [66].

[31] In Germany the Military Police (MP) is known as Feldjäger Regiment
[32] In Germany the MCS is known as MAD – Militärische Abschirm Dienst

The role of the Federal Intelligence Service (FIS) [33] is to a certain degree more comparable with what the Dutch MISS does. In order to be fully operational in the offensive Cyber spectrum, the information from this service is crucial [66]. Distribution and sharing of FIS information products is difficult, because it is heavily regulated by law and is only permitted under special circumstances [5] [20] [98] [99] [108]. Offensive actions by the FIS are not permitted. This is also regulated by law, namely the law on intelligence services and the constitution [5] [98] [108]. The service may therefore collect information, even abroad, but may not commit offensive acts in the Cyber field. This action is a task of the police or the Armed Forces [98]. The former Minister of the Interior wanted the FIS to also act abroad and was already working on the necessary legislative changes. The current Minister of the Interior (coming from Bavaria, one of the large Bundesländer) does not want to go that far. Here, too, political interests play a role. As already indicated, both paradigms that have just been elaborated are less pronounced in the German Ministry of Defense than in the Netherlands. This will be shown in the next paragraph, where the organizations will be positioned in the Cyber Governance Framework.

Structure, Culture, Legal Base

In the case of the German Units involved in the Cyber domain, the explanation can be kept brief in respect to the aspects organizational structure, culture and legal frameworks. The reasons for this are explained in the respective paragraphs.

The post-war German armed forces have a relatively short history and have undergone several large organizational changes in that time of existence. The Cyber units are of even more recent origin and are not yet fully operational. This has an impact on all three topics. With regard to the organizational structure, the German units almost all display the structure of a traditional line-staff organization. Just like in the Netherlands, the units are usually filled with specialists, which leads to a mix of professional bureaucracy with a divisional structure as described by Mintzberg [45].

With regard to culture, especially for CIT and the CIDS, it should be noted that because of their relatively short existence, a specific corporate culture has not yet formed. As for the other organizational units working within the Cyber spectrum, their cultures are very similar to the cultures found in corresponding organizations in the Netherlands. It should be noted that the cliché views on German cultural characteristics like ‘Gründlichkeit’ or thoroughness, dutifulness and diligence, appear to be true, and have to be seen as a positive aspect of German (military) culture.

With regard to the 'legal framework', similar legislation applies to both countries. This certainly applies for operational deployment during missions and the Defense of own territory. Here too, the constitution and international law are leading [5] [81] [99]. In many cases, as already indicated in this study, German legislation lays down stricter standards than in the Netherlands. This stems from history and political considerations [3] [5] [6] [98]. In addition to general legislation, the German intelligence services have their own legislation per service to which they must comply [107] [108] [109]. Finally, the Military Police also has its own legislation [98]. This is not the Criminal Code and the Code of Criminal Procedure which form the framework for the civil police. For the Military Police, legislation is applicable which also applies to security services [110]. This legislation is only applicable within Defense [98].

[33] In Germany the FIS is known as BND – Bundes Nachrichten Dienst

7.4 Position within the framework

If the German units operating within the Cyber domain are plotted on the framework as defined by Ducheine et al. [2], the image as shown in figure 11 is created. As can be seen, the CIDS is active as an executive unit in three of the four paradigms. The role the CIDS fulfills through the 'CIS Command' within the paradigm 'Resilience' is clear. Where it does not carry out these activities itself, there is close consultation with AFI, in order to keep the ranks closed and to safeguard the protection of Defense's IT systems [3] [4]. Since 2017, the AFI has been an IT company that, under the name BWI GmbH, works for the entire government and therefore as such is not plotted in the framework.

The comparison of the units is no longer completely applicable when it comes to the other three paradigms. The Cyber activities carried out in the German MoD by the CIDS in the context of 'Intelligence' are actually more activities in the field of operational and tactical reconnaissance [4]. They are therefore not comparable with the activities of the Dutch MISS. In addition, the offensive activities developed by CIDS are carried out as part of the Defense of IT or IT related systems and in the context of missions [4]. The comparison does not match with the Dutch ambition in the field of 'Offensive capabilities'.

In the paradigm 'Law Enforcement' the German MoD is completely absent. The fact that the MP is displayed here, is because the Military Police may carry out work in the context of the support of investigations [98]. This is also the reason why the MCS is shown within the paradigm 'Intelligence'. The interviews showed that the MCS do not actually play a significant role within the Defense Cyber domain [66]. Because they do offer support in the context of the protection of the troops and possibly also deploy Cyber activities because of this, they have been made visible in the framework.

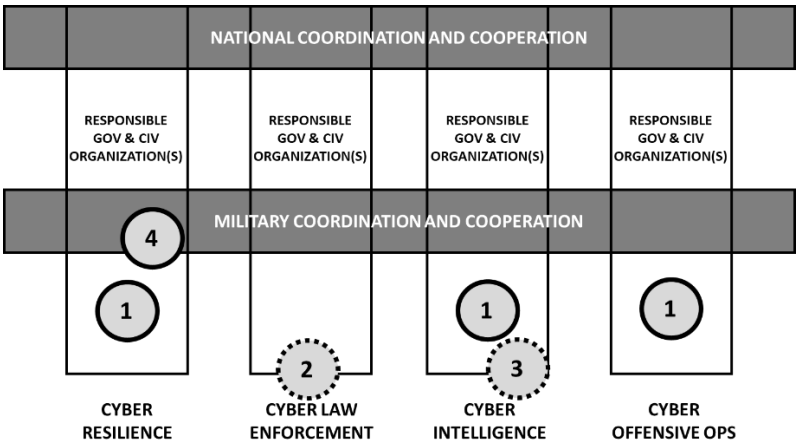


Figure 11: The framework versus the players

1. Cyber Information Domain Service (CIDS)
2. Military Police (MP)
3. Military Counterintelligence Service (MCS)
4. Cyber Information Technology (CIT)

7.5 Implications of current governance structure

Because the Cyber domain within the German MoD is still relatively young, no formal reports have yet been published that describe implications in regard to its governance structure. However, adjacent aspects were mentioned in the various interviews, which can be considered as gaps in the current approach. This concerns the following matters.

Personnel

The current set-up of the CIDS with a staff volume of approximately 15,000 men, independent education facilities and sufficient career prospects was seen as the solution to the shortage of expert personnel. However, a recent article indicated that the German MoD should still look for external sources to fill in its personnel shortages [111] [112].

'Law Enforcement'

The lack of an own 'gendarmerie corps' within the German MoD is experienced as an absence for several reasons not only in relation to Cyber investigations [5]. In order to properly safeguard the military legal status during a mission, the presence of 'own national police' is a 'must'. The presence of civilian police cannot always be guaranteed by Germany. Besides this, the military forensic capacity in the form of a sworn investigative officer is also experienced as an absence in the military Cyber chain [5].

'Intelligence' versus 'Offensive deployment'

To be able to actually deploy an offensive Cyber weapon, two things are essential, as was indicated in an interview, time and strategic information [5]. For more than one reason, the current Cyber concept of the German MoD does not provide for these matters. The offensive deployment then goes no further than actively defending, and the operational or tactical support of a mission [5].

8 Findings and Analysis

8.1 Findings

Ambition

Germany and the Netherlands are similar in several aspects, and have similar ambitions in the same areas. For example, both countries have a strong economy and want to give this economy new impetus with the aid of 'digital transformation'. In addition to using digital means to improve the existing economy, they also want to play a leading role within the digital segment itself. They want to develop new and modern ICT products for third parties and also want to develop supporting IT and security services to offer these ICT products internationally. Innovation is high on the economic agenda of both countries. Both Germany and the Netherlands have the ambition to play a major role in the field of digitization and cyber security. In terms of digital infrastructure and political willingness, the Netherlands is ahead compared to Germany. This may have to do with the size of the country in the case of the installation of optical fiber and mobile accessibility. However, the political guts and the willingness to go against existing principles and starting points also speak in favor of the Netherlands [113].

To give execution to these ambitions, both Germany and the Netherlands participate in various European and global consultation groups and forums. Examples include membership of the Global Forum on Cyber Expertise (GFCE), participation in the United Nations Group of Governmental Experts (UNGGE) and membership and participation in the European Union Agency for Network and Information Security (ENISA) [114] [115] [116].

Developments such as 'digital transformation' in a broad sense and supporting the economy with digital means not only have a positive side, but also have a downside. Criminals and state actors abuse the weaknesses of these developments in Cyberspace to improve their own position. This can be through industrial espionage to improve their own economy. Another way is to disrupt the society of another nation by developing subversive activities such as influencing news and elections. Examples of subversive activities against a nation include the hack on the German parliament in 2015 [117] and more recently the theft and the release of private data from German politicians [118]. The Netherlands is also subject to various threats as well, both politically and economically. These are annually inventoried and published by the National Cyber Security Center of the National Coordinator for Security and Counterterrorism (NCSC) [119].

Strategy & interests

Both countries have published several documents to translate ambitions into policy. In Germany, the latest version of the national ‘Cyber Security Strategy’ was issued in 2016 [18]. This strategy has four 'action areas', in which is described how Germany wants to fulfill its digital ambitions and provide protection for its industry and its population. The Ministry of the Interior plays a major role in this. Under this Ministry there are various bodies that play a role in coordination and information exchange, information security, the determination of regulations relating to the Cyber spectrum or emergency response. All these organizations contribute to national Cyber security and awareness. In 2016, the German Ministry of Defense issued a 'White Paper' in which the National Security Strategy for Germany was formulated [91]. Cyber security is mentioned in this document as a national focus area. The second part of this 'White Paper' describes how Defense sees its role within the Cyber Domain. Its Defense Cyber Strategy, which was written in 2015, has not been publicly announced

[92]. Interference of the German Defense with regard to national security is still under social pressure, partly due to history in which the Second World War left its marks. However, the current social and political debate still shows a difference in opinion with regard to what can and cannot be done by the Armed Forces [5]. Other restrictions regarding the deployment of Defense are determined by legislation. Making decisions to adjust this legislation is difficult. This is due to the (political) structure of Germany and due to legislation. Deployment by the German Armed Forces, both nationally and internationally, remains problematic in terms of decision making as a result of the aforementioned issues [4] [5].

Various Cyber strategies have also been issued in the Netherlands, both nationally by National Cyber Security Center as part of the Ministry of Justice and Security, and by the Ministry of Defense. In 2013, the second 'National Cyber Strategy' was published [120]. By means of so-called 'Cyber Security Assessments', issued by the NCSC, the most common threats and the most effective approach from the Dutch perspective are outlined annually. The most recent version of such an assessment is the NCSC Cyber Security Assessment 2018 [17]. The Dutch MoD also released its most recent version of the Defense Cyber Strategy in 2018 [64]. The strategy describes how the Dutch MoD sees its role within the (national) Cyber domain. Together with the Dutch National Cyber Security Agenda (NCSA) [121], the National Cyber Security Research Agenda III (NCSRA III) [122] and the Integrated Foreign and Security Strategy (IFSS) [123], these are the four documents that are seen as essential in how the Dutch government intends to shape the Cyber Security approach.

Compared to Germany, The Netherlands has a more integrated approach between the civil and military domain, when it comes to Cyber Security. The NCSC, which falls under the Ministry of Justice and Security, has the national responsibility and coordinates Cyber Security events. Several forums have been created for this coordination, in which the Dutch MoD also participates. This approach is similar with the Cyber approach of Germany. Within the Cyber Defense Center of the Ministry of the Interior there are also participants from the German MoD. The German MoD role within Cyber realm will grow in the future [3] [4], especially with the more serious scenarios. In the Netherlands, the cooperation between military and civilian is somewhat simpler. Even in peacetime, the Ministry of Defense is already working closely with the civilian security regions. Activities are practiced and tackled in a coordinated way without the need to make a political decision. This is in contrast to Germany.

Framework and paradigms

In order to interpret the Cyber capacities within the Dutch MoD, Ducheine et al have developed a framework [2]. Within this framework, partly on the basis of a scientific report from the Netherlands Organization for Applied Scientific Research (NOASR)[34] [37], they come up with four paradigms within the Cyber domain. These are resilience, law enforcement, intelligence and offensive operations. By identifying these activities, describing them and defining the relationships, Ducheine et al have mapped the entire Cyber domain from the perspective of Defense. This also appears to be correct in practice. During the literature studies and the interviews it appeared all activities developed by the German and Dutch MoD can be traced back to these four paradigms. The framework is therefore an excellent frame of reference for comparing countries and their Cyber deployment.

[34] In the Netherlands NOASR is known as TNO – Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek

The paradigms and therefore also the framework can also be used at national level. At this level the four paradigms are recognized as activity and responsibility. For some countries, the emphasis of a deployment is sometimes more on national than on Defense level. For example, the national coordination of Cyber security in Germany is held at the Ministry of the Interior. In the Netherlands this is a responsibility of the Ministry of Justice and Security. In order to gain insight into the relationships between the various parties, the framework must be expanded with an extra level, in order to interpret the entire national playing field. Because this study only draws a comparison between the Cyber activities of the German and Dutch Ministries of Defense, the analysis is limited to comparing the paradigms of these organizations. Only where there is a very strong dependency on the national domain, this relationship will be described.

When comparing the two countries, a number of issues are important. In the first place, it was compared whether the paradigms occurred in both countries. In addition, these paradigms only could be compared if they are of the same order of magnitude. This implies that aspects such as the definition of the paradigm, task fulfillment, organizational structure and responsibilities are important criteria. This differs for each paradigm in both countries. The following paragraphs describe the similarities and differences for each paradigm.

The Paradigm Resilience

The definition of Cyber Resilience of both countries is broadly similar. Cyber Resilience means an organization can maintain the ability to deliver the intended outcome of its IT environment and other (operational) Defense equipment that depends on IT in case of a Cyber threat or attack, and that it has the ability to restore afterwards. Resilience is an area for which in both countries no specific legislation is applicable other than the normal provisions and laws such as the General Data Protection Regulation (GDPR). In contrast to the Netherlands, Germany argues that offensive activities may be carried out in the context of protection or self-Defense [4] [5] [91] [92]. To what extent this is the case is not made explicit. The Netherlands explicitly does not do this [63]. With regard to Cyber Resilience, both countries recognize this to be an important topic.

Resilience within Defense is in the first place a responsibility of the Defense units and the employees themselves. The Defense organization must then make itself and the employees aware of the risks from the Cyber domain and indicate how they want the employees to behave. The more specific tasks arising from this paradigm are carried out both in Germany and in the Netherlands by units traditionally from the communication and IT domain. As part of their tasks within Cyber Resilience, they have special units within their ranks such as a CERT, a SOC, a Coordination Center or a Software Development department, which are more specialized than the rest of the organization.

In the Netherlands, the Defense IT Command (JITC and the DCSC) mainly focuses on the work from this paradigm. The Operational Commands must carry out this work in their specific domain. When necessary, support will be provided by the Defense Cyber Command. Germany goes much further and has set up a specific command (CIDS), of which 50% is engaged in both operational and stationary Cyber Resilience activities. Furthermore, coordination between the operational CIDS and the stationary AFI is guaranteed by the session of CIDS on the board of directors of AFI. In this way the communication and therefore the resilience chain is secured end-to-end.

The Paradigm Law Enforcement

No real in depth comparison can be made between the two countries with regard to the law enforcement paradigm, because Germany does not have a unit within Defense that carries out police tasks on the basis of Criminal Code and Code of Criminal Procedure. This task is reserved for the civil police [5] [98]. When necessary, an appeal is made by the Prosecution or Defense on the civil police. The Military Police of the German Defense sometimes assists in an investigation by collecting evidence on the spot. However, this is not a thorough specialist research, because the knowledge of the German MP is missing [98]. The presence of a gendarmerie corps within the German MoD is missed, as indicated in an interview [5]. This is because the boundaries between the different paradigms are thin and there is not always a clear transition between, for example, a criminal act and an inter-state offense. Having all the specific Cyber knowledge under one roof would be a good thing in that sense.

The Netherlands does have a Gendarmerie Corps in its ranks. The Royal Netherlands Marechaussee is authorized, on the basis of the Dutch Police Act 2012 (article 4), to perform tasks in accordance with the National Police. This also applies in the area of Cyber. The RNLM has a number of task fields where Cybercrime may play a role. The RNLM also plays a role in the investigation into the legitimate use of Cyber weapons by the Dutch Armed Forces. Within the total portfolio of the RNLM, there are more tasks to be appointed within the Law Enforcement paradigm where the RNLM should play a role. There is a lack of a clear internal vision of these tasks. Initiatives have been made, but these have to be further developed.

The Paradigm Intelligence

In the Netherlands, the MISS is responsible for Cyber Intelligence. As 'Intelligence and Security Service', it carries out its tasks under the Intelligence and Security Service Act 2017 (ISSA 2017) [77]. This law gives this Service extensive powers, and makes it possible, after obtaining permission from the Government, to conduct clandestine operations [66]. These activities can be technical actions, such as hacking a computer or a system, or supportive activities, like social engineering which can contribute to a hack. These activities take place in the socio-technical layer of the ‘van den Berg’ model [28]. In this way and with the support of these resources, the MISS is able to operate successfully in the Cyber domain.

The Dutch MISS works closely with the GISS. They have a joint unit for Cyber Operations, called the Joint SigInt Cyber Unit. The successes of the Dutch intelligence services was already described in chapter six [74] [75]. Collaboration between the MISS and the other players within the Dutch Cyber domain of Defense is difficult [82]. The information obtained under the ISSA 2017 can only be shared under special conditions. This means that the use of this information or 'Intell' is reserved for 'the services' and for advice of authorized (parts of) organizations, which is similar to Germany [5] [20] [84].

The activities as deployed by the MISS are similar to those of the German Federal Intelligence Service (FIS) which falls under the Chancellor's Office. Under its own legislation, this Service is authorized to carry out the same activities as the Dutch MISS. The FIS serves, as far as the possibilities allow, both the civil and the military part of the government with information. The FIS may not, or only under special conditions, pass information to third parties.

There are units that deal with Intelligence within the German CIDS. These are the units that fall under the Strategic Reconnaissance Command (SRC). If the level of intelligence collected by these units is compared with the Netherlands, they collect information at the tactical and operational level [97]. In the field of intelligence, the tasks performed by Strategic Reconnaissance Command (SRC) as part of the CIDS are comparable to what is performed in the Netherlands by the Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance (JISTARC) battalion. JISTARC is an intelligence unit. The command collects, analyzes and disseminates information to support a mission. In the Netherlands, this unit is not directly included in the Cyber spectrum.

Regarding the Intelligence Paradigm, the German and Dutch units within the military spectrum cannot be compared on a one-to-one basis, because they are of a different order of magnitude. The MISS has more extensive powers and possibilities than the units of the CIDS. Because the FIS is not a military unit, it is not included in the elaboration of this study. This service has also not been made visible in the German Framework.

The Paradigm Offensive Operations

According to the Dutch Cyber Strategy [40] [41], offensive Cyber means are meant to influence the actions of the opponent or to make these actions impossible. These offensive resources are only used against military targets. The latter can also be civil targets with strategic military value or importance. In order to be able to develop these activities, the Defense Cyber Command (DCC) was established in 2017. The task of the DCC is to integrate offensive Cyber operations within the conventional military operations. In addition, the DCC is expected to play a coordinating role within the Cyber Domain of the Dutch MoD. In Germany, the Cyber Operations Center (COC) as part of the Strategic Reconnaissance Command (SRC) of the CIDS is responsible for offensive Cyber operations [3] [4] [5] [84] [91] [92] [97]. This COC has been active in the offensive domain already since 2009. It then also fell under the SRC and was called Computer Network Operations team [84].

To perform Offensive Cyber Operations, three factors are essential. These are time, strategic intelligence and political will and courage.
In order to develop a good Cyber weapon, which only focuses on a specific goal, sufficient time is needed for preparation and development. This implies that investments must already be made in peacetime for a potential deployment of a Cyber weapon, with all possible consequences.

For the development of a Cyber weapon aimed at a specific goal, information is needed that goes beyond information from the operational or tactical domain. The techniques required to collect this information are also of strategic value and are only allowed to specific intelligence units. These operate under legislation that only applies to them and then under strict conditions [77] [108]. In the Netherlands this is the MISS. In Germany this is the FIS.

The last condition concerns political will and courage. The question is whether Dutch and German politicians are prepared to let Cyber develop weapons and make a preparation for deployment. This with all possible risks of political escalation if something goes wrong. A recent example of hesitation is the statement by the Dutch Minister of Defense Bijleveld, who stated in the TV program 'WNL op Zondag' that the Netherlands is in cyber war with Russia [124]. This claim was already weakened that same day because the impact of the word war can have serious diplomatic consequences [125]. The Netherlands and Germany are too 'politically correct'. Both countries want to be an example in all respects at European and global level. Where countries such as Russia and China either by

themselves or through proxies are guilty of violations of espionage and interference in foreign policy, Germany and the Netherlands continue to operate within the legal and socially accepted boundaries of Western civilization.

In both Germany and the Netherlands, the definition of offensive Cyber operations is not completely clear and controversial in a number of aspects. In Germany, partly based on history, offensive operations can only take place in support of 'defensive operations' or resilience. Offensive operations should be seen as a form of active defense [3] [4] [5] [6] [84]. This is laid down in the Constitution. The Constitution states that if a military operation is not defensive, Parliament must give its consent [99]. Such a procedure makes activities in the volatile Cyber domain almost impossible. The ambition of the German Ministry of Defense to develop and deploy Cyber weapons has already led to a social and political discussion. A second obstacle to the deployment of offensive Cyber weapons is the impossibility of sharing information between intelligence services and other agencies. This is also legally established. In Germany, a debate is currently held on this subject [98]. If the exchange of information between 'services' and other organizations is granted, this will also require changes to legislation. The last obstacle is cooperation at a strategic level. In Germany, three ministries or parts of them are necessary to create good cooperation for the development of offensive Cyber resources. These are the Ministry of the Interior, the Chancellor's Office and the Ministry of Defense. Given the differences of insight and ambitions, this will be difficult [84].

Although the obstacles in the Netherlands appear to be less than those in Germany, they are certainly present. Dutch politicians have indicated a need for offensive Cyber capacity within Defense. However, in the Netherlands, both on a national and a MoD level, the discussion is about who has what responsibilities within the Cyber domain [82]. This has an impact on the collaboration and the results. Within the Dutch MoD the necessary strategic information can only be obtained by the MISS. In the Netherlands legislation provides the Intelligence Services with the authority to do so [77]. However, this 'Service' cannot share all information. This makes the effective development of a Cyber weapon difficult. The actual deployment of a weapon system in the Netherlands can only be done by the CHOD, because it has this authority [126] [127]. This creates the discussion whether the deployment of an Offensive Cyber operation is a responsibility of the intelligence domain or of the operational domain. This is a well-known discussion and is being conducted in more countries [128]. This discussion should actually have taken place prior to the creation of a new unit because this forms the basis for implementation and cooperation within the Cyber domain.

In order to empower the DCC in the Netherlands and to ease preparations of offensive Cyber operations, this unit is currently being moved from the Army to the CHOD [129]. This measure will not contribute to the aforementioned objectives. This is because the MISS is a unit that falls under the Secretary General. Because of this, the DCC is hierarchically still subordinate to the MISS. The effective development of offensive Cyber resources, and hence the effective deployment of the DCC remains problematic. This has also been recognized by the current commander of the DCC. In an interview, she indicated that the DCC does not independently deploy, because the Netherlands is not in a state of war [130]. She outlined the DCC as an employment agency for Cyber staff and capabilities. The question here is to what extent this is effective. When staff are posted to or the RNLM or MISS, the personnel will have to operate under their specific legislation (Police Act 2012 or ISSA 2017) [42] [77]. The ambition of the Netherlands in the field of 'offensive Cyber operations' initially seemed intended at a strategic level. In the Cyber strategy of 2018, it seems that this ambition has been adjusted downwards. This document mentions the support of operational

missions [64]. This brings the ambitions for 'offensive cyber operations' of both countries closer together.

Paradigms and organization(s)
In the Netherlands, every organization is embedded in a separate paradigm. These organizations are located within different branches of the Armed Forces [2]. This results in a split Cyber landscape without a clear final responsibility. Within the Dutch Cyber landscape, there are four organizations with four cultures that have to work together. The coordination takes place on the basis of consensus. The various parties take part in several boards, where, on the basis of equality, they coordinate the activities that take place within the Cyber domain of Defense. Responsibilities and financial aspects are also discussed in these boards. The Defense Cyber organization is a network of players, where the input from all parties is equal. The main board is chaired by the Central Staff, which can be considered as a lead agency according to Provan and Kenis [46].

Consideration has been given to assigning the role of lead agency within the Defense Cyber spectrum to the Defense Cyber Command. However, the legal frameworks to fully perform this task with respect to Intelligence and Law Enforcement are missing. It is therefore difficult for the DCC to give substance to this role. Also the position of the DCC in the Defense hierarchy is too low to properly fulfil the coordination between all players. The current reorganization, in which the DCC as a unit will be placed directly under the Chief of Defense (CHOD) will not change this low position [129]. The position under the CHOD is still hierarchically lower than under the Secretary General, where the position of the Military Intelligence and Security Service is. It will be necessary to think carefully about the integrated governance of the Cyber domain of the Dutch MoD.

In Germany, the players of three paradigms have been brought together in one unit, the Cyber and Information Domain Service (CIDS). With regard to the paradigms: resilience, intelligence and offensive operations, management takes place by one commander. The governance of these units is therefore in one hand which makes coordination between the various players easier.

This observation seems to be correct, however, the German situation cannot fully be compared with the Dutch situation. Zooming in on the levels of the players within the paradigms, it must be noted that these levels and the work executed at specific levels, do not correspond. In that perspective there is a difference in definition. Particularly with regard to the paradigms of 'intelligence' and 'offensive operations', there are differences in what both countries mean by these concepts. Germany and the Netherlands give substance to this paradigm, either at another place or at another level within the Defense organization. In Germany it is also an option an organization outside Defense is responsible for handling Cyber. It is too complex to interpret all the possible differences and options in this study. In addition, this study has chosen to compare the Defense organizations of both countries and not to involve external organizations. With regard to paradigms versus the organization, no further elaboration will be made with regard to this issue.

The Dutch implications in regard with Collaboration & Cooperation, Equipment and Personnel
With the establishment of the German CIDS, Germany seemed to have overcome the three problem areas that had been detected in the Netherlands. These problem areas were cooperation, 'acquisition and purchase' and the 'recruitment and retention of personnel' [82].

The problem of the degree of cooperation in both countries is difficult to compare because the units involved in the Cyber domain are not the same. When only considering the CIDS, internal cooperation and coordination will be easier. If the Cyber Governance Frameworks of both countries are compared, filled with equivalent units, cooperation in Germany may even be more difficult. This is because the German MoD must then fall back on national capacities outside the Defense domain. Because this thesis only describes both Defense domains, this subject is not in scope and will not be further elaborated.

With the founding of CIT and CIDS and by implementing the 'plan, built and run' principle within the Cyber and Information domain as described in chapter 7, Germany could largely have the acquisition and purchase of IT-related material coordinated by the CIT [3] [4] [5] [104] [105]. This would allow an acceleration in the purchase process of IT resources. During the interviews it was indicated that the final budget allocation in Germany is done by the DG Planning. The needs from the CIT and CIDS come within the total need of Defense and are dependent on DG Plan for setting priority. This seems to partially offset the gains in time and efficiency [106].

The CIDS is a part of the Armed Forces with 15,000 employees. This offers ample and improved career opportunities. The training and education of personnel in the Cyber and Information domain up to university level is in-house. This seemed to solve the problem of recruitment and retention of personnel in comparison with the Netherlands where every unit within the Cyber domain takes only responsibility for itself. However, personnel filling and retention in Germany also appears to be a problem. The first graduated Defense Cyber workers within the German MoD are only expected in three years. It takes a long time before the staff filling is complete. A recent article indicated that Germany is looking at other European countries to solve the personnel problem at Defense [131] [132]. This shows that Germany, with the possibilities offered by the CIDS, also faces the same problems as the Netherlands.

8.2 Analysis

Germany and the Netherlands both recognize that Cyber security needs attention, both in the civil as in the military domain. This study is specifically aimed at the military domain. In this domain, both countries have fulfilled the assignment from their respective governments and have formed units that, each based on their own expertise, fulfill a specific purpose within the Cyber domain. This concerns 'resilience', 'law enforcement', 'intelligence' and 'offensive operations'. The two countries have not implemented the organization and governance of the Cyber domain in the same way. The reason for this is obviously a difference of opinion. Also history and a legal framework determine how and to what extent the aforementioned paradigms can be given shape.

The German Ministry of Defense has concentrated its Cyber units in a newly established part of the Armed Forces. The Netherlands has accommodated the paradigms of those units or Armed Forces that were already specialized in that field. A new unit was set up for the new field that had to deal with offensive Cyber operations. Concentration of units makes governance in principle easier. One-headed management provides clarity. The responsibility lies with one person. In the Netherlands, more coordination is needed in this sense. The players form a network of parties that are basically equivalent.

The question is whether the assumptions and observations above are correct for the comparison of the military Cyber domain of both countries. The Ducheine framework is an excellent tool for making this comparison. The comparison shows that the plotted Cyber units of both countries are not comparable in all respects. This applies in particular to the paradigms of intelligence and offensive operations. Germany has no gendarmerie corps within the military organization. With this, this paradigm falls off for further comparison.

The paradigms of intelligence and offensive operations in both countries are of a different magnitude. In Germany, they are either not implemented by the Defense organization or implemented in another form. Intelligence operations that are comparable to those of the Dutch MISS are carried out in Germany by the FIS. This organization falls under the Chancellor's Office. This also makes the German alignment and thus the governance in the Cyber domain a lot more complex, because not directly controllable dependencies are involved in the coordination. If information from the FIS is required for a Cyber operation, this must be coordinated via the level of the Chancellor.

With regard to offensive operations, the question is whether the definition of these operations in the Netherlands and Germany is the same. In fact, there is a lack of clarity about the details of offensive operations in both countries. Germany states offensive operations are intended as active defense in the context of the protection of Defense IT and IT related material. Legislation, but also social and political discussions do not leave much room for maneuver. This way of thinking is also in line with the way of thinking of NATO. The Dutch ambition with regard to offensive cyber operations was initially higher. This led and leads to problems with regard to the realization of this type of weapon and governance. A number of things are essential for offensive Cyber operations. This concerns time (prior to deployment), strategic intelligence and political will and courage. The question is whether these ingredients are sufficiently available in both countries.

Offensive Cyber operations are a grey area in terms of decision making and implementation. This is especially the case for civilized countries such as Germany and the Netherlands where political correctness and conformation with international regulations are highly valued in contrast to, for example, countries such as Russia and China. These countries do either not adhere to the international rules of conduct, or they create work-arounds by deploying proxy organizations that seem to operate independently. After further research it appears then, that there are ties with the government.

The governance of the Cyber domain of both countries is nevertheless complex from a different perspective. The solution is not easy. Change in this respect must be done by changing laws and shifting mandates between units that have been in place for years. Solving such problems is also known as a so-called 'wicked problem' [133] [134]. There are many parties and players involved within this problem, the matter is complex, and with solving part of the problem new problems arise which are different, but not less complex.

9 Conclusions and Recommendations

9.1 Conclusions

Germany and the Netherlands show great similarities in both the economical as social area, which also shows in the area of cyber -and information technology. The Netherlands wants to be a pioneer in the Digital spectrum and wants to be 'market leader' in Europe. For this reason, the Netherlands has designated its IT-infrastructure and resources as vital infrastructure which needs to be protected. In addition to the view of the Netherlands, Germany also has economical motives and also aims to become the market leader of the cyber spectrum in Europe.

Both the Dutch as the German MoD have a responsibility in the protection of the IT infrastructure which is formalized in legislation. Besides the protection of its own infrastructure, the knowledge and expertise of the MoD is also used as 'last resort' for the protection of the vital infrastructure. Because the Netherlands and Germany have a shared army corps, with shared mutual working processes it is in the line of expectation to also make these agreements in the cyber realm. This expectation was used as motive to perform this research. The goal of this thesis was to research the governance model for German Military Cyber operations and to compare the German procedures and frameworks to the Dutch situation.

The Cyber Governance Framework developed by Ducheine was used as base of this thesis. This framework shows four paradigms in the military cyber realm; resilience, law enforcement, intelligence and offensive operations. This framework can be interpreted as a governance framework, in order to stimulate collaboration and cooperation and was used to compare the Dutch and German MoD's. Literature on governance, organization structure and culture were abundantly available, however this was not the case concerning the internal processes and procedures of both the Netherlands as for Germany, because of the classification of this information. With anonymous interviews, two case studies were performed, one in the Netherlands and the other in Germany, after which these case studies were used for comparison. The information gained from these interviews was then used to fill the gap in the body of knowledge.

The roles defined by Ducheine; resilience, law enforcement, intelligence and offensive operations are used within the cyber realm in both the Netherlands as in Germany. The Netherlands executes all four roles defined by Ducheine within its MoD. When comparing this execution of tasks with Germany, the difference is Germany doesn't give execution to law enforcement, as this is the legal role of the civil police.

Although both the Netherlands as Germany both give execution to the other three roles, the actual interpretation of these roles differs on a variety of points. The Netherlands knows four different units within the cyber governance and organization structure, the JITC, the RNLM, the MISS and the DCC. These units form a network structure in which the coordination is done through multiple boards. The decision making is done by using consensus. In Germany there is one unit which gives execution to the three tasks within the cyber domain, the CIDS. Together with the strategical unit CIT and a logistical unit they govern the 'plan, build and run' cycle of the German Cyber and Information domain under the flag of one chief in command. It was expected this approach would counteract problems within the cyber and IT domain.

However, after finalization of this research it was discovered that although on paper the approach of the Netherlands and Germany seemed to be very similar, this was not the case in real life. Dutch ambitions are primarily focused on the area of intelligence and offensive operations on the strategical level. The execution of these ambitions of Germany is more on the operational and tactical level. The latter makes a good comparison between both approaches difficult. What is more, Germany stated it will legally only use offensive cyber capacities for the protection of its own infrastructure and IT. Although comparison of the two countries was difficult, the framework of Ducheine made the comparison possible. It appeared in general level, both counties show similarities in problems in the cyber realm. However, the Netherlands and Germany show no problems concerning resilience by taking defensive measures if standard international legislation like the GDPR is obeyed. The problems arise because of the paradigm's intelligence and offensive cyber operations and the relation between these paradigms.

In order to execute offensive cyber operations and to develop cyber weapons in both countries, three aspects are essential; time, strategic intelligence and political will and courage. It is essential a cyber weapon is developed long before its effectuation. Strategical intelligence is needed, because this intelligence goes beyond operational and tactical intelligence. In order to allow the intelligence, development and preparation of these cyber weapons, political approval and legislation is needed. It is the question if this political approval and legislation will become effective due to the risks and political consequences of these cyber weapons. Both the Netherlands as Germany are known for their political correctness and confirmation with European and global rules of political behavior.

In order to develop a cyber weapon in the Netherlands, close cooperation between the MISS and the DCC is needed. The complexity of this cooperation is twofold, the MISS is the only authority which may collect intelligence based on the Intelligence and Security Services Act. This law prescribes the gained information can only partially be shared. The lack in will of sharing information with other services is the second problem, because there is a difference in culture and acceptance of unexperienced stakeholders within the cyber realm. In the hypothetical case Germany wants to develop an offensive cyber weapon, cooperation outside the German MoD is needed, with the Chancellor's Office and the Ministry of the Interior. This results in the rise of a network organization which is even more complex in comparison with the Netherlands.

These observations concerning the deployment, the coordination and governance of an offensive cyber weapon lead to a 'wicked problem', with a lot of different parties involved and with a high complexity. When these wicked problems are resolved, new problems arise which are evenly complex. The complexity of 'offensive cyber operations' is likely to be underestimated. It is the question if operational units or intelligence services are in the lead in the development and deployment of a cyber weapon, as intelligence services play a crucial role due to their lead in the collection of necessary information. It is vital the question who is in the lead in cyber operations is answered.

9.2 Recommendations

Multiple observations were made concerning the similarities and differences in the Dutch and German governance in cyber. The most important observation is the difference in level of units and execution of tasks. It is recommended to perform further research in the formation of the cyber domain, to discover the cyber ambitions and national and international cooperation in the Netherlands and Germany.

Especially in the safe resilience paradigm, sharing of information and cooperation is advised. The sharing of established threats and countermeasures can be an advantage of both countries. Further cooperation in intelligence and offensive execution is still too far-fetched, but needs further investigation. Academic research, cooperation with the business and government (the triple helix approach) is advisable.

10 Glossary and abbreviations

No.	Definition or abbreviation	Explanation
1.	ACIA (in Dutch – AIV)	Advisory Council on International Affairs (in Dutch – Adviesraad Internationale Vraagstukken)
2.	ACIPIL (in Dutch – CAVV)	Advisory Committee on Issues of Public International Law (in Dutch – Commissie van Advies inzake Volkenrechterlijke Vraagstukken)
3.	C&C (C2)	Command & Control
4.	CHOD (in Dutch – CDS)	Chief of Defense (in Dutch – Chef Defensie Staf)
5.	CIDS (in German - Kommando CIR)	Cyber and Information Domain Service (in German – Kommando Cyber und Informationsraum)
6.	CIS (in Dutch – CIS)	Communication and Information Systems (in Dutch – Communicatie- en Informatie Systemen)
7.	CIS (in Dutch – RIV)	Council for the Intelligence and Security services (in Dutch – Raad voor de Inlichtingen- en Veiligheidsdiensten)
8.	CIS Command (in German KIT Bw)	Communication and Informationsystems Command (in German Kommando Informationstechnik der Bundeswehr)
9.	CISS (in Dutch – CTIVD)	Committee on the Intelligence and Security Services (in Dutch – Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)
10.	CIT (in German – CIT)	Cyber and Information Technology (in German – Cyber und Informations Technik)
11.	COC (in German – COC)	Cyber Operations Center
12.	CSAN (in Dutch – CSBN)	Cyber Security Assessment Netherlands (in Dutch – Cyber Security Beeld Nederland)
13.	FCPO (in German – BfV)	Federal Constitutional Protection Office (in German – Bundesamt für Verfassungsschutz)
14.	FCPO (in German – BKA)	Federal Criminal Police Office (in German – Bundes Kriminal Amt)
15.	FIS (in German – BND)	Federal Intelligence Service (in German – Bundes Nachrichten Dienst)
16.	FOITS (in German – BSI)	Federal Office of Information Technology Security (in German – Bundesamt für Sicherheit in der Informationstechnik
17.	GDPR (in Dutch – AVG)	General Data Protection Regulation (in Dutch – Algemene Verordening Gegevensbescherming)
18.	GISS (in Dutch – AIVD)	General Intelligence and Security Service (in Dutch – Algemene Inlichtingen- en Veiligheids Dienst)
19.	IFSS (in Dutch – GBVS)	Integrated Foreign and Security Strategy (in Dutch - Geïntegreerde Buitenland- en Veiligheidsstrategie)
20.	ISSA 2017 (in Dutch – WIV 2017)	Intelligence and Security Services Act 2017 (in Dutch – Wet op de Inlichtingen- en Veiligheidsdiensten 2017)
21.	JISTARC (in Dutch – JISTARC)	Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Command
22.	JITC (in Dutch – JIVC)	Joint Information Technology Command (in Dutch – Joint Informatie Voorzienings Commando)
23.	JSCU (in Dutch – JSCU)	Joint SigInt Cyber Unit
24.	MCS (in German – MAD)	Military Counterintelligence Service (in German – Militärische Abschirm Dienst)
25.	MISS (in Dutch – MIVD)	Military Intelligence & Security Service (in Dutch - Militaire Inlichtingen- en Veiligheids Dienst)
26.	MoD (in Dutch – MvD)	Ministry of Defense (in Dutch – Ministerie van Defensie)
27.	MP (in German - Feldjäger)	Military Police (in German - Feldjäger)
28.	NATO (in Dutch – NAVO)	North Atlantic Treaty Organisation (in Dutch – Noord Atlantische Verdrags Organisatie)

29.	NCSA (in Dutch – NCSA)	National Cyber Security Agenda (in Dutch – Nationale Cyber Security Agenda)
30.	NCSC (in Dutch – NCSC)	National Cyber Security Center (in Dutch – Nationaal Cyber Security Centrum)
31.	NCSRA (in Dutch – NCSRA)	National Cyber Security Research Agenda (in Dutch – Nationale Cyber Security Research Agenda)
32.	NOASR (in Dutch – TNO)	Netherlands Organization for Applied Scientific Research (in Dutch – Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek)
33.	NP (in Dutch - NP)	National Police (in Dutch – Nationale Politie)
34.	OPCW	Organisation for the Prohibition of Chemical Weapons
35.	RNLM (in Dutch – KMar)	Royal Netherlands Marechaussee (in Dutch – Koninklijke Marechaussee)
36.	SOE (in Dutch – BOE)	Special Organization Element (in Dutch – Bijzonder Organisatie Element)
37.	SRC (in German – KSA Bw)	Strategic Reconnaissance Command (in German – Kommando Strategische Aufklärung der Bundeswehr)
38.	UK	United Kingdom
39.	US	United States (of America)

11 Appendix 1: Interview Questions & Interview Details

Questionnaire thesis J. van Veenhuizen – August 2018.

1. The Netherlands recognizes four areas, or so called columns within the Defense Cyber Domain: Resilience, Law Enforcement, Intelligence and Operations (see slide). Do you also recognize this classification within German Defense? And if so, can you explain the relations they have?

2. Within the Dutch MoD, legal frameworks exist to a greater or lesser extent for these four columns. For example, there is criminal law / criminal procedure for law enforcement and for the Intell Services, the Intell and Security Act. Can you explain the legal frameworks that are valid for the German MoD per column?

3. During execution, units may need contacts with other parties in the Cyber Domain. For example, during the execution of resilience (protecting the German IT environment), the SOC may detect a criminal offense or an apparently state subversive activity. How does this work internally or, if applicable, with an external party such as the Federal Police?

4. (If applicable) How does the Intell relate to the operations (or warfare) in Germany?

5. What role does the German MoD Cyber Capacities play in National perspective? How do the 'Bundesländer' relate to the 'Bundesregierung'? How do national capacities (Civil) relate to those of German MoD?

6. There is a large diversity of units within the Information Command (CIR), ranging from Intell, via Cyber to Information and Communication? What is the connection between these units? Do you consider this as Cyber Capacity or do you see it more as Hybrid warfare? What is the thought doctrine for this unit(s)? Is this doctrine valid for this unit as a whole or do parts of the doctrine apply exclusively to units in themselves?

7. Does the Informations Kommando operate as a unit or are parts deployed for specific objectives and how is the command management arranged? Supporting, under orders, as part of a chain?

8. What is the basis for the creation of this command (the CIR as a whole) looking at the great diversity? Is there a specific goal and are the units selected for this?

9. Are there any other people to be interviewed both inside and outside the unit that are interesting for my thesis that you can think of? E.g. within the Law Enforcement or the Intell column? And can you help me to get in contact with them?

10. Is there any interesting literature that applies to this matter e.g. at the Military University in Munich (München)?

Elucidation on the interviews:

The interviews that were held for the elaboration of the two cases contain information that is personal and confidential. They also contain information about military procedures and regulations that are classified. It has been agreed with the interviewees that, for the sake of this fact, the interviews are not made public and that the processing of the data in the thesis would be done anonymously.

The reports of the interviews, as well as a copy of the recordings of the interviews, are in the possession of the first supervisor. This is to verify the conversations held.

12 Bibliography

[1] Redactie Army News, “Zijn er grenzen aan de steeds intensievere Duits-Nederlandse militaire samenwerking?,” 2018. [Online]. Available: https://www.armynews.nl/nieuws/landmacht/163655/zijn-er-grenzen-aan-de-steeds-intensievere-duits-nederlandse-militaire-samenwerking.

[2] P. A. L. Ducheine, “Defensie in het digitale domein,” *Mil. Spect.*, no. 4, pp. 152–168, 2017.

[3] J. van Veenhuizen, *Interview A01 / 2018*. 2018.

[4] J. van Veenhuizen, *Interview A02 /2018*. 2018.

[5] J. van Veenhuizen, *Interview A03 / 2018*. 2018.

[6] J. van Veenhuizen, *Interview A04 / 2018*. 2018.

[7] C. A. Hazeu, *Institutionele economie*. Coutinho, 2014.

[8] NATO, “Warsaw Summit Communiqué,” 2016. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_133169.htm. [Accessed: 10-Nov-2018].

[9] J. A. Lewis, “The Role of Offensive Cyber Operations in NATO’s Collective Defence,” *Tallinn Pap.*, no. 8, 2015.

[10] T. Rid, “Cyber War Will Not Take Place,” *J. Strateg. Stud.*, vol. 35, no. 1, pp. 5–32, 2012.

[11] J. Stone, “Cyber War *Will* Take Place!,” *J. Strateg. Stud.*, vol. 36, no. 1, pp. 101–108, 2013.

[12] P. A. L. Ducheine, “Cyber warfare is taking place!,” vol. 2016, pp. 1–12, 2016.

[13] M. C. Libicki, “Cyberspace Is Not a Warfighting Domain,” *J. Law Policy Inf. Soc.*, vol. 8, no. 2, pp. 321–336, 2012.

[14] M. Laskar, “Summary of Social Contract Theory by Hobbes, Locke and Rousseau,” *Ssrn*, no. October 2017, 2014.

[15] J. Krüger, “Welt am Sonntag,” *Die Arena der Machtlosen*, 2002. [Online]. Available: https://www.welt.de/print-wams/article607749/Die-Arena-der-Machtlosen.html. [Accessed: 10-Nov-2018].

[16] D. Shea and F. Gottron, “CRS Report for Congress Received through the CRS Web Ricin : Technical Background and Potential Role in Terrorism,” *Intelligence*, 2004.

[17] National Coordinator for Security and Counterterrorism of the Netherlands, “Cyber Security Assessment of the Netherlands,” p. 76, 2018.

[18] BMI, “Cyber-Sicherheitsstrategie für Deutschland 2016,” 2016.

[19] IALANA, “Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg,” 2016. [Online]. Available: https://www.ialana.de/arbeitsfelder/frieden-durch-recht/neue-formen-der-kriegsfuehrung-und-voelkerrecht/cyberwarfare/1494-strategische-leitlinie-cyber-verteidigung-im-geschaeftsbereich-bmvg. [Accessed: 08-Oct-2018].

[20] J. van Veenhuizen, *Interview A10 / 2018*. 2018.

[21] UvA, “dhr. prof. dr. P.A.L. (Paul) Ducheine,” 2019. [Online]. Available: http://www.uva.nl/profiel/d/u/p.a.l.ducheine/p.a.l.ducheine.html. [Accessed: 12-Jan-2019].

[22] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.

[23] T. C. Folsom, “Defining Cyberspace (Finding real virtue in the place of virtual reality),” *Tulane J. Int. Comp. Law*, vol. 1, no. 2011, pp. 1–6, 2012.

[24] S. Adams *et al.*, “The Governance of Cybersecurity,” no. November 2015, pp. 1–166, 2015.

[25] S. Qadir and S. M. K. Quadri, “Information Availability: An Insight into the Most Important Attribute of Information Security,” *J. Inf. Secur.*, vol. 7, no. 7, pp. 185–194, 2016.

[26] S. Posthumus and R. Von Solms, “A framework for the governance of information security,” *Comput. Secur.*, vol. 23, no. 8, pp. 638–646, 2004.

[27] C. J. Hamelink, *The Ethics of Cyberspace*. Sage Publications, Inc., 2001, 2001.

[28] J. Van Den Berg *et al.*, “On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education,” *NATO STO/IST-122 Symp. Tallin*, no. c, pp. 1–10, 2014.

[29] NLD MOD, “Nederlandse Defensie Doctrine,” no. 6, pp. 11–15, 2013.

[30] J.A.P. Hoogervorst, *Understanding and Designing Enterprises*. 2016.

[31] D. Broeders, “Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance.”

[32] L. Lessig, “The Law of the Horse: What Cyberlaw Might Teach,” *Harv. Law Rev.*, vol. 113, no. 2, p. 501, 1999.

[33] Carolyn Hughes Tuohy, “Agency, Contract, and Governance: Shifting Shapes of Accountability in the Health Care Arena,” vol. 28, no. June 2003, 2015.

[34] G. A. van der Steur, “Nationale Veiligheid,” 2016.

[35] RIVM, “Nationaal Veiligheidsprofiel 2016,” 2016.

[36] NLD MOD, “Eindrapport Verkenningen,” 2010.

[37] H. A. M. Luiijf, “Cyberspace als militaire dimensie,” 2010.

[38] USA DoD, “The Defense Science Board DoD RESPONSES,” vol. I, no. October, 1997.

[39] W. van Bladel en mw mr MAJ Hector, “Adviesraad Internationale Vraagstukken Advisory Council on International Affairs,” *Digit. oorlogvoering*, no. 77, p. 41, 2011.

[40] Ministry of Defense, “Defensie cyber strategie,” pp. 1–18, 2012.

[41] J. A. Hennis-Plasschaert, “Actualisering Defensie Cyber Strategie,” pp. 1–7, 2015.

[42] MIN J&V, “Politiewet 2012,” *2018*, 2012. [Online]. Available: https://wetten.overheid.nl/BWBR0031788/2018-09-19. [Accessed: 23-Nov-2018].

[43] W. Alexander Vacca, “Military Culture and Cyber Security,” *Survival (Lond).*, vol. 53, no. 6, pp. 159–176, 2011.

[44] F. C. Lunenburg, “Organizational Structure: Mintzberg’s Framework,” *Int. J. Sch. Acad. Intellect. Divers.*, vol. 14, no. 1, pp. 1–8, 2012.

[45] H. Mintzberg, “The Design Parameters,” *Struct. Organ.*, pp. 65–181, 1979.

[46] K. G. Provan and P. Kenis, “Modes of network governance: Structure, management, and effectiveness,” *J. Public Adm. Res. Theory*, vol. 18, no. 2, pp. 229–252, 2008.

[47] C. Jones, W. S. H. Hesterly, and S. P. Borgatti, “A General Theory of Network Governance:

Exchange Conditions and Social Mechanisms," *Acad. Manag. Rev.*, vol. 22, no. 4, pp. 911–945, 1997.

[48] S. Boeke, "National cyber crisis management: Different European approaches," *Governance*, no. February, 2017.

[49] J. van Veenhuizen, *Interview B02 / 2018*. 2018.

[50] G. Reger, Etherage, Reger, "The ethical challenge of cultural competence," 2008.

[51] L. K. Hall, "The importance of understanding military culture," *Soc. Work Health Care*, vol. 50, no. 1, pp. 4–18, 2011.

[52] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, "De Nederlandse Grondwet." [Online]. Available: https://www.denederlandsegrondwet.nl/. [Accessed: 09-Nov-2018].

[53] P. A. L. Ducheine and J. E. D. Voetelink, "Cyberoperaties : naar een juridisch raamwerk," *Mil. Spect.*, no. 6, pp. 3–6, 2011.

[54] L. Jarvis and S. Macdonald, "What Is Cyberterrorism? Findings From a Survey of Researchers," *Terror. Polit. Violence*, vol. 27, no. 4, pp. 657–678, 2015.

[55] L. Jarvis, S. Macdonald, and L. Nouri, "The Cyberterrorism Threat: Findings from a Survey of Researchers," *Stud. Confl. Terror.*, vol. 37, no. 1, pp. 68–90, 2014.

[56] Security.nl, "'Nederland heeft cyberleger nodig,'" 2009. [Online]. Available: https://www.security.nl/posting/26683#posting223949. [Accessed: 14-Nov-2018].

[57] Tweede Kamer der Staten-Generaal 2, *Motie van het lid Knops, Tweede Kamer, vergaderjaar 2009–2010, 32 123 X, nr. 66*, no. 12. 2010, pp. 2009–2011.

[58] Tweede Kamer Der Staten Generaal, *Motie van het lid Hernandez, Tweede Kamer, vergaderjaar 2010–2011, 32 500 X, nr. 24*. 2010.

[59] Tweede Kamer Der Staten Generaal, *Gew motie Hernandez en Knops over een visie over de aanpak van cybercrime/cyberwarfare (t.v.v. 32500 X, nr. 24)*, no. 76. 2011.

[60] NCSC (J&S Department), "The National Cyber Security Strategy (NCSS) (The Netherlands)," 2011.

[61] BuZa, "Veilige Wereld, Veilig Nederland," pp. 1–20, 2013.

[62] Ministerie van Defensie, "Personeels rapportage midden 2018," 2018.

[63] J. van Veenhuizen, *Interview B06 / 2018*. 2018.

[64] Ministerie van Defensie, "Defensie Cyber Strategie 2018 - Investeren in digitale slagkracht Nederland | Publicatie | Defensie.nl," 2018.

[65] Dutch MoD, "Koninklijke Marechaussee," 2019. [Online]. Available: https://www.defensie.nl/organisatie/marechaussee. [Accessed: 13-Jan-2019].

[66] J. van Veenhuizen, *Interview B01 / 2018*. 2018.

[67] Ministerie van Defensie, *Rapport Onderzoeksraad van de Veiligheid*. 2018.

[68] MIN J&V, "Wetboek van Strafrecht," *2018*, 1881. [Online]. Available: https://wetten.overheid.nl/BWBR0001854/2018-10-16. [Accessed: 08-Dec-2018].

[69] MIN J&V, "Wetboek van Strafvordering," *2018*, 1921. [Online]. Available:

https://wetten.overheid.nl/BWBR0001903/2018-10-16.

[70] MIN J&V, “Vreemdelingenwet 2000,” *2018*, 2000. [Online]. Available: https://wetten.overheid.nl/BWBR0011823/2018-07-28. [Accessed: 23-Nov-2018].

[71] Inlichtingendiensten.nl, “RIV (raad),” 2018. [Online]. Available: http://www.inlichtingendiensten.nl/organisatie/riv-raad. [Accessed: 20-Dec-2018].

[72] CTIVD, “Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten,” 2018. [Online]. Available: https://www.ctivd.nl/. [Accessed: 20-Dec-2018].

[73] CTIVD, “rapport-22b.pdf,” 2015.

[74] INFO Security Magazine, “AIVD en MIVD gaven belangrijke informatie aan FBI over Russische inmenging verkiezingen,” 2018. [Online]. Available: https://www.infosecuritymagazine.nl/2018/01/26/aivd-en-mivd-gaven-belangrijke-informatie-aan-fbi-over-russische-inmenging-verkiezingen/.

[75] NOS, “MIVD: we hebben Russische hack van OPCW in Den Haag voorkomen,” 2018. [Online]. Available: https://nos.nl/artikel/2253313-mivd-we-hebben-russische-hack-van-opcw-in-den-haag-voorkomen.html. [Accessed: 20-Dec-2018].

[76] J. van Veenhuizen, *Interview B07 / 2018*. 2018.

[77] MIN J&V, “Wet op de inlichtingen- en veiligheidsdiensten 2017,” 2017. [Online]. Available: https://wetten.overheid.nl/BWBR0039896/2017-09-01. [Accessed: 09-Dec-2018].

[78] J. S. J. Hillen, *32733, Nr.1, Beleidsbrief Defensie*, no. 1. 2011, pp. 1–33.

[79] J. van Veenhuizen, *Interview B05 / 2018*. 2018.

[80] J. van Veenhuizen, *Interview B08 / 2018*. 2018.

[81] United Nations, *UN Charter*. 1953.

[82] VKA, “EVALUATION OF THE DUTCH CYBER STRATEGY,” 2017.

[83] J. van Veenhuizen, *Interview A08 / 2018*. 2018.

[84] O. Wechsler, “Germany ’ s Cyber Strategy — Government and Military Preparations for Facing Cyber Threats,” vol. 2, no. 1, 2018.

[85] BMI, “Cyber-Sicherheitsstrategie für Deutschland,” 2011.

[86] Bundeskriminalamt, “Bundes Kriminal Ambt,” *2018*, 2018. [Online]. Available: https://www.bka.de/DE/Home/home_node.html. [Accessed: 24-Dec-2018].

[87] Bundesamt für Sicherheit in der Informationstechnik, “Bundesamt für Sicherheit in der Informationstechnik,” 2018. [Online]. Available: https://www.bsi.bund.de/DE/Home/home_node.html. [Accessed: 24-Dec-2018].

[88] Bundesamt für Sicherheit in der Informationstechnik, “CERT Bund,” 2018. [Online]. Available: https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html. [Accessed: 24-Dec-2018].

[89] Bundesamt für Sicherheit in der Informationstechnik, “Cyber-Abwehrzentrum,” 2018. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html. [Accessed: 24-Dec-2018].

[90] Bundesamt für Verfassungsschutz, “Bundesamt für Verfassungsschutz,” 2018. [Online]. Available: https://www.verfassungsschutz.de/. [Accessed: 24-Dec-2018].

[91] BMVg, “Whitepaper on German Security Policy and the Future of the Bundeswehr,” 2016.

[92] DE-BMVg, “Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg ,” 2015.

[93] IALANA Deutschland – Vereinigung für Friedensrecht, “Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg,” 2016. [Online]. Available: https://www.ialana.de/arbeitsfelder/frieden-durch-recht/neue-formen-der-kriegsfuehrung-und-voelkerrecht/cyberwarfare/1494-strategische-leitlinie-cyber-verteidigung-im-geschaeftsbereich-bmvg. [Accessed: 26-Dec-2018].

[94] Netzpolitik.org, “Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar“ und offensive digitale Angriffe,” 2015. [Online]. Available: https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#1-Vorbemerkung. [Accessed: 26-Dec-2018].

[95] Bundeszentrale für politische Bildung, “Dossier Deutsche Verteidigungspolitik,” 2018.

[96] BMVg, “Die Neuausrichtung der Bundeswehr,” 2013.

[97] J. van Veenhuizen, *Interview C01 / 2018*. 2018.

[98] J. van Veenhuizen, *Interview A06 / 2108*. 2018.

[99] Parlamentarischer Rat, “Grundgesetz für die Bundesrepublik Deutschland,” *Bundesgesetzblatt*, vol. 1, no. 1, pp. 1–49, 2014.

[100] M.M. van der Pluijm, “Inzet van de Duitse Bundeswehr,” Utrecht, 2008.

[101] J. van Veenhuizen, “Interview A11 / 2018,” 2018.

[102] Bundesamt für Sicherheit in der Informationtechnik, “UP KRITIS Public-Private Partnership for Critical Infrastructure Protection, Basis and Goals,” 2014.

[103] BMVg, *Tagesbefehl*. 2015.

[104] Bundesministerium der Verteidigung, “Strategische Leitlinie Digitalisierung,” 2017.

[105] BMVg, “Abschlussbericht Aufbaustab Cyber- und Informationsraum,” no. April, pp. 1–49, 2016.

[106] J. van Veenhuizen, *Interview A05 / 2018*. 2018.

[107] Bundesministeriums der Justiz und für Verbraucherschutz, *Gesetz über den militärischen Abschirmdienst (MAD-Gesetz - MADG)*, no. 3. 2017, pp. 1–6.

[108] Bundesministeriums der Justiz und für Verbraucherschutz, *Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG)*, no. 2. 1990, p. 1.

[109] Bundesamt fü Justiz, “Bundesverfassungsschutzgesetz,” 1990. [Online]. Available: https://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html. [Accessed: 01-Jan-2019].

[110] Bundesamt fü Justiz, “UZWBWG,” 2018. [Online]. Available: http://www.gesetze-im-internet.de/uzwbwg/. [Accessed: 01-Jan-2019].

[111] RTL Nieuws, “Leger Duitsland wil mensen uit andere EU-landen kunnen werven,” 2018.

[Online]. Available: https://www.rtlnieuws.nl/nieuws/buitenland/artikel/4533156/duits-leger-werknemers-eu-landen-europese-unie. [Accessed: 01-Jan-2019].

[112] Süddeutsche Zeitung, “Bundeswehr will EU-Ausländer anwerben,” 2018. [Online]. Available: https://www.sueddeutsche.de/politik/bundeswehr-auslaender-eu-1.4267414. [Accessed: 01-Jan-2019].

[113] duitslandnieuws.nl, “Wat Nederlandse cybersecurity experts kunnen toevoegen in Duitsland,” *duitslandnieuws.nl*, 2018. [Online]. Available: https://www.duitslandnieuws.nl/blog/2018/10/02/wat-nederlandse-cybersecurity-experts-kunnen-toevoegen-in-duitsland/. [Accessed: 04-Jan-2019].

[114] GFCE, “Global Forum on Cyber Expertise,” 2018. [Online]. Available: https://www.thegfce.com/. [Accessed: 04-Jan-2019].

[115] GIP Digital watch, “UN GGE,” 2018. [Online]. Available: https://dig.watch/processes/ungge. [Accessed: 03-Jan-2019].

[116] European Union Agency for Network and Information Security, “ENISA,” 2018. [Online]. Available: https://www.enisa.europa.eu/. [Accessed: 04-Jan-2019].

[117] J. Götz and B. Strunz, “Braucht der Bundestag ein neues IT-Netz?,” *Tagesschau.de*, 2015. [Online]. Available: https://www.tagesschau.de/inland/bundestag-it-101.html. [Accessed: 04-Jan-2019].

[118] M. Götschenberg, “Hackerangriff auf Hunderte Politiker,” *tagesschau.de*, 2019. [Online]. Available: https://www.tagesschau.de/inland/deutsche-politiker-gehackt-101.html. [Accessed: 04-Jan-2019].

[119] NCSC-NL, “Cybersecuritybeeld Nederland 2018,” pp. 1–88, 2018.

[120] Netherlands, “National Cyber Security Strategy 2,” pp. 1–36, 2013.

[121] N. C. Agenda, “Nederlandse Cybersecurity Agenda: Nederland digitaal veilig,” *Rijksoverheid.nl*, 2018.

[122] Dcypher, “Ncsra Iii,” 2018.

[123] BuZa, “Wereldwijd voor een veilig Nederland Wereldwijd voor een veilig Nederland Geïntegreerde Buitenland- en,” p. 45, 2018.

[124] Buitenlandredactie AD, “Bijleveld: Nederland in cyberoorlog met Russen,” *AD.NL*, 2018. [Online]. Available: https://www.ad.nl/buitenland/bijleveld-nederland-in-cyberoorlog-met-russen~ac0b5320/. [Accessed: 08-Jan-2019].

[125] B. Paternotte, “Ank Bijleveld trekt keutel in: Nederland toch niet in cyberoorlog met Rusland,” *The Post Online*, 2018. [Online]. Available: https://tpo.nl/2018/10/14/ank-bijleveld-trekt-keutel-in-nederland-toch-niet-in-cyberoorlog-met-rusland/. [Accessed: 12-Jan-2019].

[126] J. van Veenhuizen, *Interview B03 / 2018*. 2018.

[127] J. van Veenhuizen, *Interview B04 / 2018*. 2018.

[128] A. E. Wall, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,” *Harvard Natl. Secur. J.*, vol. 3, no. 1, pp. 85–142, 2011.

[129] Ministerie van Defensie, *Nota Omhanging DCC*. 2018.

[130] L. van Lonkhuyzen and K. Versteegh, “Het cyberleger kan en mag nog weinig,” *NRC.nl*, 2018.

[Online]. Available: https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254. [Accessed: 01-Jan-2019].

[131] M. Becker and M. Gebauer, “Von der Leyen will Italiener, Polen und Rumänen anwerben,” *Spiegel Online*, 2018. [Online]. Available: http://www.spiegel.de/politik/deutschland/bundeswehr-mit-personalnot-ursula-von-der-leyen-will-italiener-polen-und-rumaenen-anwerben-a-1245523.html. [Accessed: 07-Jan-2019].

[132] ARD-aktuell / tagesschau.de, “Bundeswehr will EU-Bürger anwerben,” *Tagesschau.de*, 2018. [Online]. Available: https://www.tagesschau.de/inland/bundeswehr-auslaender-101.html. [Accessed: 07-Jan-2019].

[133] A. C. Edmondson, “Wicked problem solvers: Lessons from successful cross-industry teams,” *Harv. Bus. Rev.*, vol. 94, no. 6, pp. 52–59, 2016.

[134] J. C. Camillus, “Strategy as a Wicked problem,” 2008.