Universiteit Leiden

# NATO and Cyber Security:

***Critical Junctures as Catalysts for Change***

MA International Relations

Candidate: Roger André Tosbotn

Student number: s1707752

Email: roger.tosbotn@umail.leidenuniv.nl

Thesis Supervisor: Dr. Eugenio Cusumano

Word count: 11371

# Abstract

This thesis does two main things. It contributes to the academic debate on the relative prominence of the cyber domain in security, and analyses the change in NATO's conceptualization of "cyber" over time. These pertinent questions are addressed through quantitative and qualitative analyses. The review of existing scholarship on the topic provides insight into NATO's strategic development, major cyber-security incidents, the issues relating to Article 5 of the NATO treaty and cyber security, and the effects on the security environment that stems from technological developments in society. By employing the approach of constructivism, the framework of strategic culture, and methods of content analysis, this thesis tracks the change in prominence and conceptualization in official NATO documents from 2002-2016. As a result, this thesis contributes to an understanding of digital-age security from the point of view of NATO. Finally, it suggests that an awareness of one's own strategic culture can aid in preparing for new challenges in a security-oriented environment.



Keywords: International Security, Cyber Security, NATO, Constructivism, Content Analysis, Strategic Culture, Article 5, CCDCoE.

# Table of Contents


Abstract ..... 2

Introduction ..... 1

NATO, Cyber Security, and a rapidly changing security environment ..... 1

Thesis aims and structure ..... 3

Methodology and Framework ..... 3

Constructivism and Cyber Security ..... 4

A Theoretical Framework of Identity and Strategic Culture ..... 5

Hypotheses ..... 6

Conceptual and Relational Content Analysis ..... 7

Software and Approach ..... 7

Selecting a Corpus: Official Documents ..... 8

Limitations of Content Analysis ..... 9

Existing Scholarship: NATO meets Cyber Security ..... 9

The Development of NATO and Cyber Security ..... 9

Cyber Security: Critical Junctures in the Cyber Domain ..... 10

Article 5 and The Problem of Attribution ..... 12

Societal Developments and the Information Revolution ..... 13

Gaps and Implications from existing literature ..... 15

Content Analysis Results: Findings of Prominence and Conceptualization ..... 15

The Increasing Prominence of Cyber(Security) as perceived by NATO ..... 16

Table 1: Word Frequency ..... 17

The Relative Prominence of Cyber ..... 17

Qualitative examination of quantitative findings ..... 18

Graph 1: Linear Cyber Over Time ..... 19

Graph 2: Exponential Cyber Summits ..... 20

Conceptualization: Cyber - a volatile concept ..... 20

Genealogy and Richness of "cyber" as a concept ..... 21

CyCon 2016 and Article 5 – Imminent Change ..... 23

NATO's Strategic Culture and Norms ..... 25

Who is the threat? Actors in Cyberspace ..... 27

Conclusion ..... 28

Bibliography ..... 31

Body of Documents ..... 36

Appendix A ..... 38

R-Script ..... 38

Appendix B ..... 40

Coding Scheme ..... 40

Conceptualization over time: Output ..... 46

*"The brain carries the memory of yesterday, which is tradition, and is frightened to let go, because it cannot face something new. Tradition becomes our security, and when the mind is secure it is in decay."* Jiddu Krishnamurti, 1969

# Introduction

## NATO, Cyber Security, and a rapidly changing security environment

At the Cyber Conference in Tallinn, Estonia in June 2016, North Atlantic Treaty Association (NATO) high officials discussed the idea of implementing cyberspace as the fifth domain of warfare as an expected outcome of the July 2016 Warsaw summit. Implications of this would necessarily include both a re-thinking of cyber defence for NATO, and an update of the 5th article of the Washington Treaty regarding its collective defence component. Recent developments have confirmed the agreement to recognize cyber as a domain at the Warsaw summit[1], which means that in the future, cyber-attacks could be treated the same as military attacks; any attack on one is an attack on all member countries, and must be responded to accordingly.

Rapid technological developments and an on-going process of further interconnecting the digital environment with society have spurred a whole range of new security challenges that link cyber security and societal developments together (Granville 2003). The information revolution refers to the changes as a result of a transition from the mechanical to the digital in societies. The proof is found in its impact on economic, social, and technological progress in a post-industrial society (Castell 2010). The information revolution is central to the topic of cyber security, cyber warfare, and cyber terrorism (Arquilla and Ronfeldt 1997), as it has facilitated advancements in how critical infrastructures, economic sectors, and communications take place. Moreover, the most technically developed countries experience a disproportionate relation between publicly and privately owned business, and the subsequent problem of diffusion when it comes to whose responsibility it is to attend to the security of societal critical infrastructure (Herrington and Aldrich 2013). At the same time, the development of capabilities in cyber-space is increasingly more diverse and complex in its manifestations (Choucri 2012: 125-126). Cyber-war in a modern technological age intensifies developments in warfare that

[1] See article at http://nato.int/cps/en/natohq/news_132356.htm?selectedLocale=en

alter the centrality of the state as a security actor, as previously introduced by guerrilla war and terrorism. Non-state actors such as individuals and organizations are becoming increasingly relevant (Sigholm 2013). Additionally, surveillance, propaganda, and espionage have found new life through digital means (Singer and Friedman 2014: 91-92). With the examples of Tallinn in 2007, Georgia in 2008, and the current conflict in Ukraine, new hybrid approaches have quickly taken centre-stage in debates about the future of warfare [2].

However, much of the scholarly debate surrounding cyber security and cyber warfare centres around definitional problems of what "cyber" is (Singer and Friedman 2014: 12-66), the potency of cyber warfare (McGraw 2013; Junio 2013), whether a cyber war will or will not take place (Stone 2013; Arquilla and Ronfeldt 1993; Rid 2012), the role of the cyber component in military organizations (Eom 2012), the extent to which critical infrastructures are endangered by the digitalization of societies (Granville 2003; Herrington and Aldrich 2013; Klimburg 2012: 36-39), and definitional or legal problems regarding cyber-attacks, attribution of attacks (Rid and Buchanan 2015), and "acts of war" (Hughes 2010; Roscini 2014). There has been a lack of independent research on defence organizations like NATO and their stance on and interpretation of the prominence and conceptualization of cyber and security[3]. One theoretical approach that specifically focuses on conceptualization of events from the perspective of actors is social constructivism.

A constructivist approach to research that engages with the digital sphere allows for investigation of identity based perspectives and framing, and can through quantitative methods reveal patterns of meaning in large bodies of text (Eriksson and Giacomello 2014: 206). This approach has formed the backbone of work analysing the construction of threats within political discourse (Eriksson and Giacomello 2007; Dunn Cavelty 2008; Deibert 2013). Klotz and Lynch (2007) suggest content analysis as a means to analyse the large amounts of text available in the digital age. Employing a constructivist approach focused on language and the meaning behind rhetoric, serves as a means to discovering patterns or trends that relate to ideas and identity (Eriksson and Giacomello 2014: 209). A constructivist approach combined with the content analysis method allows for a study of the political communications and culture of NATO (ibid.). Strategic culture theory contends that ideas and beliefs within a dominant culture, or *milieu*, within an organization, shapes the way in which the organization perceives the world, and the

[22] See Grant (2008) on Hybrid Warfare at http://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/

[3] See Fidler, David, Pregent, Richard, and Vandurme, Alex (2013) *"NATO, Cyber Defense, and International Law"* for one of the few examples of the type of research that is done on the topic.

extent to which it is willing to change or adapt to new problems. Strategic culture is further discussed in the methodology and framework section, and guides this thesis towards a generation of testable hypotheses.

### Thesis aims and structure

The aim of this thesis is to contribute to two debates on cyber security. Firstly, how prominent is cyber security in NATO's official documents? This will take place in the form of a quantitative content analysis. Secondly, this thesis examines the way in which NATO's (outwards) understanding of "cyber" has changed over time. This examination follows a coding process of key words and associations of official NATO documents. Both content analyses are performed on a body of official NATO documents in a time period from 2002 to 2016, not including the coming 2016 Warsaw summit. The Prague summit in 2002 is the first summit where the word "cyber" is specifically mentioned, and serves as a logical point of departure. Due to the deadline of this thesis, the timeframe stops at Secretary General Stoltenberg's April speech in 2016. The research questions guiding this thesis are the following, *"how has NATO's perception of the prominence of cyber security changed from 2002-2016", and, "how has NATO's conceptualization of 'cyber' changed in the same timeframe?"*

This thesis sets out by accounting for the chosen methodology and framework in the first section. The second section provides an overview of existing scholarship on NATO and cyber security. The following section is twofold; first, it discusses the findings of the quantitative content analysis. Second, it presents results from the qualitative content analysis. The aim of this section is to evaluate the claims of the research questions and hypotheses that guides this research. The thesis concludes by stressing the implications of the research.

## Methodology and Framework

This section presents the theoretical framework of the thesis. The framework forms the basis of hypothesis generation by discussing constructivism as an approach, and strategic culture as the applied theoretical framework.

## Constructivism and Cyber Security

A defined theoretical framework allows for the construction of conceptually informed hypotheses regarding the research questions. Additionally, it helps in guiding research and placing its consequential findings within a theoretical frame. The choice of theoretical framework in this thesis is guided by *The Information Revolution* (Eriksson and Giacomello 2006) and *Strategies for Research in Constructivist International Relations* (Klotz and Lynch 2007), in which constructivism is argued to be best suited to deal with security issues related to recent developments in society; the information revolution and the interconnectedness that follows security in the digital age (Eriksson and Giacomello 2006). While realism and liberalism offer valuable angles on security, both fall short when examining the intricacies of cyberspace and security. Realism, while primarily concerned with security, suffers from an overly state-centric perspective (Reardon and Choucri 2012: 5). This focus limits the questions one would ask about the impact of "cyber", as well as the methods of study, as it fails to account for the increasing relevance of non-state actors, and adheres to a more rigorous positivist ontology. Liberalists on the other hand, have not engaged with the topic of cyber security (ibid: 6). This may be the result of liberalist scholars' emphasis on cooperation, development, and the spread of ideas, rather than the security aspects of cyberspace (ibid.). Since constructivism contends that beliefs shape identities, which in turn shape interests (Eriksson and Giacomello 2006: 233; Katzenstein 1996; Eriksson and Giacomello 2014: 2006), the constructivist approach helps explain the developments of NATO and cyber security from an ideational point of view: change in interests comes from a shift in identities and norms (ibid). Furthermore, since constructivists "emphasize (…) [the] significance of interpretation (…) [and how] perceptions of reality are always "filtered" and shaped by particular values, identities and interests (…)" (Eriksson and Giacomello 2014: 206), it is suited for threat perception analysis. Implied when examining a shift in identities and norms, is an historical outlook that allows for the change to be studied in the given time period: 2002-2016. Since this thesis deals with how NATO perceives cyber and security, it is useful to employ threat perception examination through a constructivist lens that accounts for ideational factors. As a result, this research delves

into questions about NATO's perceptions of the prominence and conceptualization of "cyber" over time. The theoretical framework emphasizes the interplay between interpretation of reality, identities, norms, and decision-making, and contributes as a versatile and strong toolbox in dealing with the research agenda.

## A Theoretical Framework of Identity and Strategic Culture

Lantis (2002) provides key concepts for the research on NATO and its culture. Notably, the ideational foundations of security policy are accentuated as a product of political and strategic culture (ibid: 87-88, 106). Such a culture comes from history and geographical conditions (Gray 2006: 10-11), and is found in interpretive codes of language and symbolism. It contains the set of beliefs, ideas, and values of individuals and collectives (ibid; Biava, Drent and Herd 2011: 2.). Moreover, these codes encompass assumptions of the political world that determine which problems are identified, the way they are perceived, and the range of alternatives available to deal with them (Elkins and Simeon 1979: 127). Furthermore, Hudson (1997) argues that constructivism provides an understanding of culture as an ever-evolving system through shared meaning to the studies of security. This system governs perceptions, communications, and actions that become the output (practice) of foreign policy. Berger specifies political-military cultural interpretations as static and change-resistant. This because,

*"First, existing political culture is widely shared, so 'alternative' sets of ideas (…) enjoy little support (..) second, standard elements of strategic culture, especially the evaluative and affective components (…) [are] difficult to disconfirm. Third, (…) information that reinforces existing images and beliefs are readily assimilated, while inconsistent data tend to be ignored, rejected, or distorted"* (1994:24-25).

In other words, the dominant culture within a military organization resists alternative ideas and interpretations as a result of its own identity that is reproduced through action. Therefore, one would expect NATO's development to tie to its interpretation to be inherently change-resistant. These actions are guided by historical and geographical conditions. Path-dependent models of foreign policy shape the development of foreign policy in a long-term perspective (Banchoff 1999:1-2), and the concept of strategic culture, "particularly those concerning decisions to go to war, preferences for offensive, expansionist or defensive modes of warfare, and levels of wartime casualties (..)" (ibid.).

Johnston (1995) outlines cultures as *milieus* that consist of shared assumptions, with an internal dominant culture of preserving the status quo. Elites are often the "purveyor of the common historical narrative" (Lantis 2002: 107); a narrative that shapes identities and beliefs over time. However, external shocks can fundamentally challenge existing beliefs by undermining historical narratives. An intense external shock that disables the culture to provide solutions or proper responses, can create internal doubt and space for alternatives. This can introduce changes both in a short and a long-term perspective (ibid: 106-112).

In NATO's case, the strategic culture would thus be primed to maintain its original goals of collective defence policies and deterrence. The dominant culture within the organization would be expected to resist change and new ideas, unless catalysts for change such as "dramatic events or traumatic experiences", or external shocks serve fundamental challenges to existing beliefs and undermine historical narratives within the alliance. Therefore, one cannot expect significant alteration of ideas and identity outside of extraordinary incidents that shake the foundations of the set of beliefs of values of NATO, but rather a steady change over time with a spike in changing measures at critical junctures.

## Hypotheses

Based on the theoretical framework above, one would expect the following hypotheses to hold true:

**H1**: The frequency in mentions of "cyber" in NATO official documents has increased in the time period 2002-2016.

**H2**: Critical junctures in the period of 2007-2009 and in 2014 provides reason for higher frequency in mentions of "cyber".

**H3**: Once a critical juncture is reached, the milieu and operation of NATO is transformed and thus forced to reformulate "cyber" as a conspicuous security dimension.

**H4**: The rapidly developing security environment has led to a richer association of the concept of "cyber" over time.

These hypotheses are tested through one quantitative and one qualitative content analysis as outlined below.

## Conceptual and Relational Content Analysis

Conceptual content analysis is a research method that establishes the existence and frequency (prominence) of concepts by words or phrases in a text. In short, a conceptual content analysis looks for the presence of words in a given body of documents to measure its prominence, and can be performed over time, in relation to other words, or both (Palmquist, Carley, and Dale 1997). This thesis employs conceptual content analysis to measure the relative prominence of "cyber" in NATO's discourse through quantitative analysis in the time period 2002-2016.

Relational content analysis goes beyond the identification of concepts in texts by exploring the relationships between the concepts identified. Furthermore, it allows for semantic analysis. The variant of relational analysis employed in this research is proximity analysis. Proximity analysis is concerned with interrelated, co-occuring concepts, and informs us about the overall meaning of the text. (Palmquist, Carley, and Dale 1997). In sum, relational content analysis allows us to infer characteristics of a communication by examining a concept's associations in a text (Holsti 1969). Relational content analysis forms the background of the examination of the change in NATO's conceptualization of "cyber" from 2002-2016.

## Software and Approach

The software used in executing these content analyses was R 3.3.1, by making use of the tm package, and the xpdf engine. In order to run a content analysis through R 3.3.1, the usage of the tm package is threefold: first, it provides functions for scanning the text(s). Secondly, it allows for converting the body of 21 documents into a corpus. Thirdly, the tm package's readpdf function in combination with the xpdf engine allows for scanning the corpus for the data requested. Furthermore, there are two parameters for the xpdf engine: info, and text. The purpose of this is to maintain the original physical layout of the text as well as possible. The readpdf function reads the text. This is the first step, and allows the software read the text. The second step, is to clean the corpus with commands including conversions of all text to lower case, removal of white spaces, and removal of punctuation. This makes for more consistent

output when scanning the text. Finally, the r-script writes the findings into two different spreadsheet files (.csv). The first file, named "prominence", presents word frequencies in columns based on the different key-words; cyber, new threats, regional stability + regional security + regional defence, proliferation of weapons of mass destruction, biological + nuclear + chemical weapons, Russia, and Article 5. The second file, named "paragraphs" prints a table that shows all paragraphs including the word "cyber", the name of the document they are extracted from, and the line number of the document they are found.

The choice of keywords for the quantitative analysis was made through a random selection of five NATO-documents, with manual reading and coding by relevance to cyber security, and to frequency. The qualitative content analysis output is available in its entirety in appendix B.

See appendix A for the r-script used in these analyses.

## Selecting a Corpus: Official Documents

In applying content analysis to political communication, it is necessary to limit and justify one's choice of sources. This research examines how NATO sees itself and the security environment. Therefore, the primary sources have to comprise of official NATO statements or documents. The primary sources of this thesis are the bi-annual summit declarations from NATO summits between 2002-2014. Moreover, to expand the body of documents of analysis, speeches by NATO secretary generals and official statements add to the quantity of the research, and stretches the timeline by additional two years to 2016. The choice of official documents follows Sowers' (2009: 25) logic; if the goal is to see how NATO projects itself and therefore also how it sees itself in relation to a problem, or an "other", official documents serve as excellent primary sources. This thesis assumes that NATO-published documents and statements are carefully drafted, and can uncover recurring themes and messages in their communication as a reflection of their self-image (ibid.). This body of documents allow for two things: Firstly, it enables a quantitative analysis that highlights the increasing prominence of "cyber" vis-à-vis other domains in NATO's discourse. Secondly, it allows for a qualitative analysis that draws from data to infer about NATO's conceptualization over time.

### Limitations of Content Analysis

The limitations of content analysis are first and foremost found in its descriptive nature. As the research can only produce data that allows for inferences, and not "hard facts", it inherently limits the ability to generalize and solidify theory. However, content analysis is an unobtrusive, inexpensive, and easily replicable research method (McNamara 2003; Neuendorf 2002) Furthermore, it is an excellent tool for observing change over time. It allows for systematic coding and evaluation of the use of communication for each year of the time-period selected; through looking at context associated words. Its findings do not tell us about the underlying reasons for the phenomena observed, however it spurs a range of new questions and allows for fact and data-based reasoning. This research combines qualitative and quantitative approaches as a means to answer H1-H4 as well as derive new hypotheses from the findings.

## Existing Scholarship: NATO meets Cyber Security

### The Development of NATO and Cyber Security

NATO's main purpose during the Cold War was maintaining sufficient military strength to act as a deterring force, and to assure a 'balance of forces' by creating and maintaining stability and security (Yost 2010: 490). Since the end of the Cold War, NATO adopted further purposes by vowing to oppose proliferation of Weapons of Mass Destruction (WMD), supporting EU-led crisis management operations under the "Berlin-Plus" arrangements[4], and assisting general ad-hoc security operations (ibid: 492). The notion of security was further broadened in 1999 when The North Atlantic Council proclaimed that terrorism could affect the security interests of NATO, and in 2001 this was put to practice when Article 5 was invoked after 9/11 (Yost 2010: 494). Article 5 proclaims that an armed attack against one or more of the countries in the alliance shall be considered as an attack on them all, and is an agreement that collective self-defence, in accordance with Article 51 of the United nations charter, that enables NATO to

[4] Read more about the Berlin-Plus arrangements and NATO-EU cooperation at http://www.nato.int/summit2009/topics_en/21-nato-eu_strategic_partnership.html

"restore and maintain" the security of the North Atlantic area.[5] This implies a willingness to retaliate if it is deemed necessary in order to restore and maintain the security of NATO members. Where NATO previously emphasized WMDs, followed by an increased participation in peacekeeping missions both within and outside of the Euro-Atlantic regions; 2008 marked the addition of yet another element to NATO's collective defence – Cyber-defence (Yost 2010: 509). This point, however, lacks further scholarly examination.

The term "cyber" refers to a digital environment where data is created, stored, and shared. It is a distinct domain that has developed into encompassing both virtual space, and the physical space that allows the virtual to flow (Singer and Friedman 2014: 13). The understanding of this interconnectedness has been rapidly emerging, and while early instances of cyber-threats and security was associated with "computers and the internet", technological developments and critical security incidents have broadened the concept of "cyber" to virtually anything connected to digital and electronic platforms (ibid: 14-15).

It is in between the realms of technological development on the one hand, and security on the other, that NATO and cyber security find common ground. If one accepts the notion that cyber security has gained prominence and relevance in society, then NATO as a defence alliance must deal with the emerging issues that follow.

## Cyber Security: Critical Junctures in the Cyber Domain

The examples of Estonia in 2007 (Herzog 2011), Georgia in 2008 (Hollis 2011), the Stuxnet worm in 2010 (Herrington and Aldrich 2013; Singer and Friedman 2014: 114-118), and Ukraine in 2014 (Rid and Buchanan 2015; Geers 2015) serve as important cases of critical junctures with regards to cyber security and warfare.

As historical, ethnic, and political tensions rose in Estonia, the Estonian government implemented policies with the purpose of limiting Russian influences on Estonian culture (Herzog 2011: 49-50). On April 30, 2007, the government moved a Bronze Soldier statue from one part of Tallinn to another, which resulted in rioting among the Russian-speaking community in Estonia. Accompanying the following weeks of riots were denial-of-service (DDoS) attacks targeting the websites of government ministries, banks, and political parties (ibid: 51). Estonia relies on the internet for its critical infrastructure to run smoothly; "electronic networks are

[5] The North Atlantic Treaty from April 4. 1949 last accessed 14.7.16 from http://www.nato.int/cps/en/natolive/official_texts_17120.htm

integral to (…) government operations, electric power grids, 97 percent of bank transactions (…)" (ibid.). The attacks against Estonia signalled the vulnerability to cyber-attacks in a modernized society.

In August the following year, the long-standing conflict between Russia and Georgia led to a five-day war between the two nations. As was experienced in Tallinn, cyber-attacks on government networks, finance and communications took place. Additionally, Russian cyber-attacks were highly coordinated and synchronized with movements on the ground, and the ability to deny Georgian communication further tipped the conflict in favour of Russia. This approach combined more traditional military approaches with the denial of services of the opponent, and acts as a showcase of how a hybrid approach can yield great advantages in conflicts. The cyber-component's role in the conflict has, in hindsight, solidified the idea about hybrid warfare as a blend of methods of confusion and aggression (Wirtz 2015: 31-35).

The urgent need for revision and bolstering cyber-resilience became evident in the wake of the Stuxnet worm. It was a sophisticated cyber-attack on the Iranian nuclear programme, a programme that was thought to be heavily protected against breaches (Herrington and Eldrich 2013). The worm held extraordinary capabilities; it was created to target specific configurations in the industrial equipment that would disable atomic centrifuges, and consisted of several zero-day exploits (Farwell and Rohozinski 2011: 23). The attacks were investigated, and the conclusion was that such an attack would not be possible without state-support. Evidence points towards both the United States and Israel as the perpetrators (Herrington and Eldrich 2013: 305).

As an extension of previous approaches in neighbouring countries, the Russian invasion and occupation in Ukraine 2014 once again brought the concept of hybrid warfare into debate. The cyber incidents that occurred in Ukraine are most relevant for this thesis. Ranging from sporadic skirmishes of DDoS-attacks and website defacements, to cyber-espionage, cell phone network disruptions, and institutionalized and targeted efforts of propaganda, Russian military has drawn on an impressive arsenal of weaponry in order to control the information and narrative in Ukraine (CCD CoE 2015: 10-11). Cyber can no longer be considered as a temporary edge on the battlefield, but must be examined in a context of strategic effects (Geerts 2015: 13). As a key component of the overall strategy of Russian warfare, cyber has become a tool which primarily dictates the flow of information; not only by blocking access to the communications of its targets, but also by flooding information channels with misinformation and propaganda (ibid.). Russia employed several methods as a means to achieve the latter. Firstly, the ownership of Ukrainian email services by Russian business meant that intercepting Ukrainian government

officials' emails was an easy task (Giles 2015: 23-24). Secondly, malware was employed to showcase pro-Russian video-clips and adverts. Thirdly, Russia isolated Crimea from news sources of the outside world. This was done by selectively disrupting cable connections to the mainland (ibid: 25-26)). These methods combined into what has been described as a "successful information campaign" (ibid.), and helped Russia in controlling the narrative of their involvements in Crimea.

These examples serve as illustrations of critical junctures regarding NATO and the cyber domain. The attacks on Estonia, Georgia, and Ukraine, were effectively attacks on a NATO member country, an aspiring NATO member country, and a dithering aspirant country. Conjointly, the attacks did, to varying degrees, have a confrontational impact on NATO. Therefore, it would be expected for the data analysis to show a spike in associations to "cyber" the periods of 2007-2008, and 2014.

## Article 5 and The Problem of Attribution

International law with regard to cyber warfare may be considered insufficient to serve its purpose for the cases mentioned above. This has been further examined in relation to the Russian cyber operations in Ukraine (Stinissen 2015). However, discussions of invoking Article 5 during the 2007 and 2008 cyber-attacks in Estonia and Georgia did not amount to direct response from NATO. The Wales Summit in 2014 proved to be a paradigm shift in this regard, as NATO ratified a policy stating that cyber-attacks may lead to an invocation of Article 5 (NATO 2014; Limnell 2015: 149). There is however no agreement of the specifics of what may constitute such an attack. So far, attacks have been "dealt with on a case-by-case basis" (NATO declaration Wales Summit 2014), NATO officials have nonetheless voiced concerns about the need to establish a clear framework to deal with cyber-attacks. A step in this direction is likely to be made at the July 2016 Warsaw Summit (CyCon 2016).

Another problem relating to Article 5 is tied to the very nature of the cyber domain. A shift in routing information through one or several Internet access points creates difficulties in tracing where the attack or malware comes from (Singer and Friedman 2014: 75). This is termed the "attribution problem", and has been the source of much trouble for actors when their systems have been attacked. Not only can the process of identifying and proving the perpetrator's guilt be time-consuming, but it can also range from difficult to impossible (Hughes 2010: 528-529). Furthermore, if the attack is a worm or malware, it can be constructed in a way that deletes

traces of its entry. Additionally, malware and worms can stay within a system for a long time, only to be activated based on a certain action of the user of the infected system, or the creator of it (Singer and Friedman 2014; Rid and Buchanan 2015). In effect, this means that anyone reading this paper could have an infected computer that is ready to act as a vessel for DDoS attacks towards someone else at the command of its creator, or that at the command of its creator, the malware is set to corrupt the computer's hard drive. Recent scholarship on the topic, however, disputes these difficulties. Some problems that add to the difficulty of cyber security in general, and the attribution problem in particular, is a fundamental lack of understanding of cyber security. A telling example in this respect is the targeted disruption and espionage of a private sector executive in Ukraine. Further research into the executive showed him as a former high-ranking government official (Koval 2015: 56). In the same vein, Russian attacks in Georgia were impressively coordinated with movements on the ground, which shows at the very least cooperation between Russian military and the hackers (Hughes 2010: 529).

This difficulty of attributing cyber-attacks, and NATO's internal difficulties in determining the scope of Article 5 applied to offenses carried out in the cyber domain are connected. This adversity adds to the problem of hybrid approaches; where methods are mixed and the tracing of i.e. Russian intervention and occupation of Ukraine proved blurry (Geers 2015). This lack of clarity favours the perpetrating actors (ibid.), which adds to the very potency of cyber approaches as a means to achieve military victories (Limnell 2015).

## Societal Developments and the Information Revolution

The role of NATO with regards to cyber security must be seen in a context of an increasingly complex and interconnected society. The openness and connectivity of the Internet is both its greatest strength and vulnerability. On the one hand, it promotes technical innovation and serves as the backbone of what is dubbed the "information" or "knowledge" age. This knowledge-based society acts as a modernizing mechanism of how information is created, shared, and communicated, and acts as a driving force for social evolution (Humbert 2007). As such, cyber connectivity is "the lubricant and catalyst for ever more sophisticated and elusive organised crimes" (Granville 2003: 102). On the other hand, in terms of security, cybercrime stems from this increasing technological progress and digital interconnectedness within and across states. The lack of equally developed security measures and training means that there are a growing number of vulnerabilities for hackers to exploit (ibid: 105). The increasing digitisation follows

the societal development in which Information Technology (IT) is a driving force. Many processes are dependent on IT - to varying degrees - depending on the level of digitisation of a given country, banking services, governmental services, communications, and the storage of personal data (CSAN-4 2014: 7). Moreover, the sheer amount of devices connected together creates "more ways in" for cyber criminals and professionals to exploit. Medical equipment, vehicles, cell phones, etc., are often connected to one-another, and a security vulnerability in one device can often be an entry point for another (ibid.). The prominence of the "information" revolution is thus both a threat to national and international security (Eriksson and Giacomello 2006: 222), as well as for businesses (Lindsay 2015).

Furthermore, the developments of cyberspace and its culminating relevance have elevated its influence into the arena of global politics (Reardon and Choucri 2012: 2-3). This relevance is linked with cyberspace's entry into how politics is run. Not only is a majority of NGOs, international organizations, governments and ministries now present on digital platforms as sources of information; they are also exposed to influence from anyone else that is also digitally connected (ibid.). As a result of the interconnectedness of societies, the same effect has been present in the political aspects of a globalized world (ibid: 8). Essentially, this connectivity means that the increasing amount of actors connected in the digital sphere also increases the amount of exploitable vulnerabilities (ibid.).

## Critical Infrastructure

Some examples of exploitable vulnerabilities are tied to the notion of "critical infrastructure"; an all-encompassing term that refers to all systems that power "modern-day civilization", i.e. electronically driven manufacturing, communications, emergency services, financial services, and transportation sectors.[6] The future of cyber defence and resilience of critical infrastructure hinges upon several factors. Some of the most conspicuous ones include an improved cooperation between the public and private sector when it comes to security, adequate training of personnel, defined information and communications policies, and a successful transition and facilitation of "system diversity"; which mixes digital, analogue, and manual systems (Herrington and Aldrich 2013; ibid.: 306).

[6] As defined by Homeland Security. Read more about the 16 critical sectors in the US at: https://www.dhs.gov/critical-infrastructure-sectors

Attacks on critical infrastructure mean that "cyberspace [is] play[ing] an increasingly important role" (Ionatamishvili and Svetoka 2015: 103-104). A targeted attack on computerized systems is imperceptibly accepted as an attack on the very systems that run the daily lives and business of people, sustain critical infrastructure and runs financial transactions (ibid.). Additionally, attacks on – or infiltration of - strategic communications have taken a leading role in offensive cyber strategy. In effect, this means that cyber-attacks have the potency to greatly affect the lives of the civil population in a given country, and that with a security definition that goes beyond the infantile: afflict the security of people in their ability to communicate, travel, use basic digital and electronic services, and access money (Granville 2003; Herrington and Aldrich 2013). If NATO is unable to protect these sectors of its member countries, it is failing at its original aims; safeguarding liberal principles, and preserving peace and security.[7]

### Gaps and Implications from existing literature

The review of existing scholarship accentuates a range of different aspects of cyber and security. In NATO's case the things that engage with its reason for existence is of especially high relevance. Yost (2010) accounts for NATO's development and purpose; a purpose in which adapting to security trends is at the heart of the organization. The lack of research on how NATO is prepared to deal with cyber security trends must be considered a gap in the literature. Although there is NATO-published literature such as the Tallinn Manual[8] and other CCDCoE publications, there is no prevalent academic literature on this topic; a void this thesis aims to help fill. Moreover, the incidents in Estonia, Georgia, and Ukraine all bring expectations of a change in NATO. This is based on the framework of strategic culture. As this thesis measures both word frequency (prominence) and change over time (conceptualization), it tests the expectations of strategic culture on NATO's outward communication between 2002-2016. The research method this paper uses has not been used in earlier investigations into the topic.

## Content Analysis Results: Findings of Prominence and Conceptualization

[7] The North Atlantic Treaty from April 4. 1949.
The manual is available at https://ccdcoe.org/tallinn-manual.html

This section deals with the findings of the quantitative and qualitative analyses. The results of the quantitative analysis illustrate two main points: firstly, it shows the relative prominence of "cyber" vis-à-vis other aspects NATO deem as important. Secondly, it elucidates several aspects of NATO's strategic culture. Namely, the continuation of Russia as NATO's main concern, the multidimensional nature of which NATO has increased its focus into several domains of warfare, and the spike in frequency of "cyber" in the wake of major, critical incidents. The research questions this section tackles are,

*"how has NATO's perception of the prominence of cyber security changed from 2002-2016",* and*, "how has NATO's conceptualization of 'cyber' changed in the same timeframe?"*.

Moreover, this section tests the following four hypotheses,

**H1**: The frequency in mentions of "cyber" in NATO official documents has increased in the time period 2002-2016.

**H2**: Critical junctures in the period of 2007-2009 and in 2014 provides reason for higher frequency in mentions of "cyber".

**H3**: Once a critical juncture is reached, the milieu and operation of NATO is transformed and thus forced to reformulate "cyber" as a conspicuous security dimension.

**H4**: The rapidly developing security environment has led to a richer association of the concept of "cyber" over time.

## The Increasing Prominence of Cyber(Security) as perceived by NATO

This section ensues a discussion based on the findings of the quantitative content analysis.

| Year | Cyber | New Threats | Stability & Security The Region | Terrorism | Proliferation WMD | Biological,Nuclear, Chemical Weapons | Russia | Article 5 |
|---|---|---|---|---|---|---|---|---|
| 2002 | 2 | 1 | 3 | 19 | 8 | 2 | 46 | 2 |
| 2003 | 1 | 0 | 0 | 1 | 0 | 1 | 3 | 0 |
| 2004 | 1 | 3 | 2 | 36 | 17 | 7 | 16 | 0 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2005 | 1 | 0 | 0 | 4 | 0 | 0 | 21 | 0 |
| 2006 | 2 | 0 | 2 | 13 | 9 | 2 | 14 | 0 |
| 2007 | 6 | 2 | 0 | 3 | 1 | 1 | 1 | 0 |
| 2008 | 9 | 0 | 1 | 12 | 16 | 8 | 22 | 1 |
| 2009 | 7 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 2010 | 20 | 0 | 3 | 8 | 16 | 8 | 19 | 2 |
| 2011 | 3 | 1 | 0 | 1 | 0 | 1 | 4 | 0 |
| 2012 | 15 | 0 | 2 | 14 | 15 | 9 | 35 | 1 |
| 2013 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 |
| 2014 | 20 | 0 | 2 | 13 | 13 | 14 | 46 | 3 |
| 2015 | 9 | 0 | 0 | 0 | 0 | 0 | 8 | 1 |
| 2016 | 2 | 0 | 1 | 3 | 0 | 0 | 42 | 1 |
| Total | 100 | 7 | 18 | 130 | 95 | 55 | 277 | 11 |

**Table 1: Word Frequency**

## The Relative Prominence of Cyber

As shown in table 1, "cyber" ranks third in mentions (100) behind "Russia" (277) and "terrorism" (130). In relative terms, "cyber" is perceived as one of three key issues for NATO. However, mentions of "Russia" still dominate the discourse of NATO summits and speeches, with recurring counts of "terrorism" keeping "cyber" in third place.

These findings relate to two different explanations in academic literature. Firstly, the context in which three nations with varying ties to NATO; Estonia, Georgia, and Ukraine, all experienced cyber-attacks. These attacks could be perceived as critical junctures for NATO, with the result being added pressures on the dominant culture in its *milieu*. In turn, this pressure challenges the validity of the pre-agreed upon solutions to deal with shocks, and can spur transformation in the strategic culture of NATO as a means to deal with new challenges. Secondly, NATO's incorporation and refinement of defence Article is consistent with the findings of table 1. The increase in mentions of "cyber", assumes a growth in the importance of "cyber". These findings speak to the validity of H1 and H2: H1 is, in accordance with the existing scholarship on societal developments and NATO's development alike, unsurprising. The boost in frequency over time affirms "cyber" as a prominent and aspiring dimension of the perceived security environment that NATO operates in. Moreover, it offers support for the claims of H2; the periods of 2007-2009 and 2014 serve as illustrations of spikes in the count of "cyber" mentions. Table 1 also displays a contrast that serves as falsification; none of the other terms experienced similar spikes

in the same time period. This constitutes as proof that it was the "cyber" term alone - not the whole range of concepts - that saw an increase in this period.

Moreover, as existing scholarship suggests, NATO's inclusion of "cyber" to its collective defence strategy in 2008 is reflected in the frequency of "cyber" mentions in table 1. This contributes to the framework of strategic culture in which shocks ultimately serve as catalysts for change. NATO's adaptation to the shocks following the 2007 and 2008 cyber-attacks, appears to have served as "dramatic enough" to fundamentally challenge the dominant culture, and thus result in the modification in behaviour; adding "cyber" as a dimension of collective defence. Additionally, these findings connect to H3 as the drastic change in policy is derived from an internal change based on external pressures. In order to prove H3, a qualitative analysis is required. The qualitative section examines H3 by looking at the change in conceptualization in the same time-period.

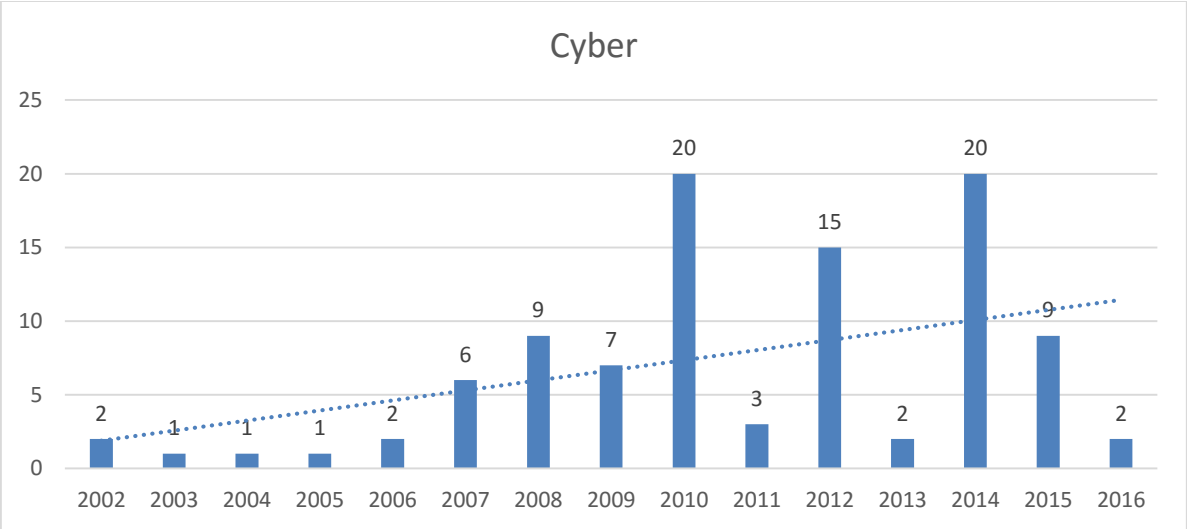
## Qualitative examination of quantitative findings

Table 1 shows a large increase in mentions of ''cyber'' in NATO summits from 2002 in Prague (1) to the 2014 Cardiff summit (20). When looking at speeches held by the secretary generals, however, mentions of ''cyber'' have remained at a consistently low level except for two outliers; Fogh Rasmussen's speech in 2009 and Jens Stoltenberg's keynote speech in 2015[9]. Fogh Rasmussen's speech must be seen in context of the 2007 and 2008 cyber-attacks in Tallinn and Georgia respectively. Stoltenberg's speech adheres to the assumption of an increase in emphasizing the cyber component in defence matters, and could be seen as a build-up to the assumed acknowledgement of cyber as the fifth domain of warfare in the 2016 Warsaw summit.

Furthermore, the control words used in the analyses show consistency in mentions of the "proliferation of nuclear weapons", "terrorism", and "Russia". These coincide with expectations from the framework of strategic culture in which large organizations, such as a military alliance, change slowly and over time if not fundamentally challenged by shocks. It also assumes the organization to preserve its agreed-upon conceptions about the world. The consistency of "Russia" as the main concern is inextricably connected with the very creation of the alliance, and thus its identity. As Yost (2010) argues, the very purpose behind establishing a North-Atlantic Treaty stems from the Cold War and the need to deter Russian influence and

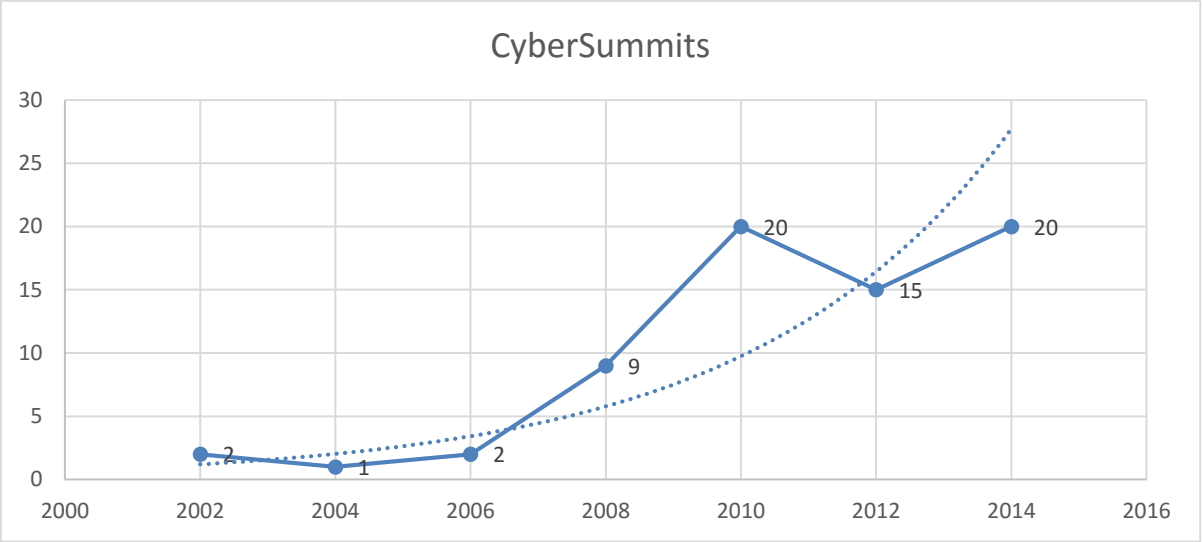
[9] See Literature list for links to the speeches.

aggression. Consequently, the *milieu* within NATO would be expected to hold a set of assumptions that leads to a preserving of the status quo. This implies a willingness to (re)produce the narrative of Russia as an "other", whilst also constituting how NATO sees itself vis-à-vis the security environment. Finally, since interest is shaped by a shift of identities and norms (Eriksson and Giacomello 2014), the NATO-Russian relationship is expected to remain as it is – or at most see a slow change over time.




## Graph 1: Linear Cyber Over Time

In graph 1, the substantial increase in word frequency for "cyber" serves as a representation for its growing importance for NATO between 2002-2016. The spike from 2006, to the 2007-2009 period and its following augmentation in 2014, supports the hypothesis that critical junctures between 2007-2009, and in 2014, manifested in the rhetoric of NATO.




### Graph 2: Exponential Cyber Summits

By isolating the bi-annual summits from 2002-2014 from the speeches in the odd years (2003-2015) and 2016, the growing importance of "cyber" experienced a skyrocketing starting in the time-period between the 2006 summit in Riga, and the 2008 summit in Bucharest. The exponential growth is elucidated in the dotted trend line, and implies continued growth in cyber mentions in the future whilst further bolstering the findings of 2007-2009 as a key period for NATO's cyber development. This solidifies the validity of H2 as it stresses the peaks while also highlighting the trend of cyber as an increasingly important concept for NATO.

This section presents strong support for the claims of H1 and H2. Expectations of a growing recurrence of "cyber" mentions between 2002-2016, as well as apparent peaks during critical junctures. Moreover, it indicates support of H3. This support is further examined in the section below.

## Conceptualization: Cyber - a volatile concept

The conceptualization tables[10] offer four main findings. Firstly, this section will discuss the genealogy of the "cyber" concept over the time period of the analysis (2002-2016). Secondly, a discussion of the change in strategic culture and norms transpires. Thirdly, the associations to

[10] See Appendix B for the coding scheme and entire output used in this section.

"cyber" within the body of documents is discussed; with an analysis of NATO and Article 5, and an analysis of the findings with regards to NATO's focus on states and non-state actors in its cyber discourse.

## Genealogy and Richness of "cyber" as a concept

The initial question the qualitative content analysis sets out to illuminate whether the "cyber"-term gained a richer association over time. As established in the quantitative analysis section, critical junctures have played an important role in challenging the dominant culture and norms of NATO. The section below explores the genealogy and richness of the "cyber" concept over time, and is employed in order to trace the evidence from the quantitative analysis through qualitative means.

The genealogy of the cyber dimension offers some interesting findings (Appendix B). Most remarkable, perhaps, is the timing of a richer and complex projection of NATO's understanding of cyber and associated terms in relation to the conjunctures of cyber-attacks on Estonia, Georgia, and Ukraine respectively. In 2007, for instance, the association of power grids, banking systems, government services and IT infrastructure was a major development from the vague mentions of "cyber-attacks" and "cyber-defence" in the preceding years. In 2008, the concept of cyber saw an expansion that built upon the 2007 developments, but also saw the interplay between cyber defence and energy security add to it, with an emphasis of protecting Information and Communications Technologies (ICTs). Since a broadened association adds took place, this finding supports H3.

In the time period between 2008-2014, the concept of cyber saw a more extensive understanding of the relationship between governments, private companies, and its potential impact on economies. Furthermore, an elucidation of the need for cooperation with both the European Union and the United Nations in not only defending against cyber-attacks and preventing cyber-crime, but also in carrying out common research and development strategies to better bolster defences against the new types of security threats. While briefly mentioned in earlier official documents, 2010 marked the year where NATO thoroughly demonstrated a more sophisticated stance on cyber policies. This projected an (outwards) approach and clarity in the necessity of breaking down the cyber dimension into bite-sized chunks; with detection, assessment, prevention, defence, and recovery as lone-standing as well as interlinked aspects

of NATO's cyber security. Additionally, this time-period was an acknowledgement of the growing numbers and sophistication of attacks done in cyber-space. All the above mentioned changes are consistently linked to the paramount importance of protecting the alliance and its member countries' critical infrastructure; as mentioned in relation to the potential impact of cyber-attacks, and how they have the potential to affect power grids, houses, cities, air traffic controls, and banking services etc.

From 2011-2012, the need for research and cooperation was yet again emphasized as a key step towards maintaining security. In an environment that is rapidly evolving, and where it can be difficult to separate piracy and cyber-crime from terrorist groups or non-state actors with digital weapons, the notion of borderless, trans-national threats was underlined. The Wales summit declaration marks a change in the concentration of attention for NATO. In the wake of Russia's involvement in Ukraine, where "little green men", information warfare, and support of rebel groups in Ukraine were just a few of the tactics employed by the Kremlin; a call for modernization symbolized the summit. The concept of cyber was enlarged to encompass the complexity of the dynamic of cyber defence and national defence. The Wales summit declaration appears to have been a paradigmatic shift for NATO and cyber security. Attacks were described as increasing in quantity and volatility. The cyber policy presented as a confirmation of the 2010 specifics on how to prevent, detect, recover, defend, and build resilience. The most prominent change in NATO's discourse of 2014, however, was the acknowledgement that cyber-attacks can trigger Article 5. The next section deals with the Article 5-problems of NATO in more detail. Moreover, a declared goal of integrating a cyber-component to NATO operation would also characterize a paradigm shift on how NATO carries out operations. This development originates from the need to improve and increase training, exercise, and education of personnel in the dimension of cyber. The time-period 2010-2014 adds another pillar of support to H3, as the concept of cyber saw a widening of associations of encompassing terms and concepts. Moreover, it supports the notion of H4, in which the security environment directly affected the degree of association of "cyber".

The cyber term saw a strengthening towards this direction in 2015 and 2016: 2015 was a ground-breaking year with regards to NATO's discourse on cyber security and cyber defence. There are three main facets of this: Firstly, "Cyber is now part of all crises and conflicts"[11] speaks to not only the prominence of cyber, but also the need to integrate a conscious cyber policy to all aspects of NATO. Secondly, the notion that a cyber-attack can trigger Article 5 has

[11] See literature list for link to Secretary General Stoltenberg's Keynote Speech in 2015

at this point in time become recurring. In effect, this could have decisive implications on how NATO prepares for, and responds to cyber-attacks. Lastly, for the first time in an official document, cyber and hybrid warfare are discussed as inextricably linked. With regards to the need to adapt to a new security environment, the concept of "cyber" has at this point in time reached such a level of complexity and prominence that NATO implicitly has to undergo some sort of re-structuring of the alliance's ways to deal with this reality. Speeches from 2016 reinforces the necessity of improving NATO's resilience to deal with both cyber and hybrid threats. Furthermore, the secretary general urges the need for an improvement with regards to NATO's cyber defence.

In sum, starting from 2007 in particular, the conceptualization of cyber has grown to embody a rich variety of associations. The genealogical approach provides an elucidation of this enrichening that supports both H3 and H4. This augmentation has serious implications for two reasons. Firstly, it reveals how NATO sees the cyber component of the security environment it operates in. Secondly, it means that NATO is urged to change how it responds to cyber security matters. The second point is discussed alongside other findings from the qualitative content analysis in detail below.

## CyCon 2016 and Article 5 – Imminent Change

An important aspect of the changing conceptualization of cyber is its leaning towards association with warfare and Article 5. The low-frequency, irregular mentions of Article 5 in the first content analysis in table 1 speaks to the complexity of the cyber issue. The qualitative content analysis shows that cyber and Article 5 were first mentioned together at the Wales summit in 2014, and then re-stated the year after in a keynote speech held by the secretary general. The lack of outwards projection about their (potential) constitutive relationship raises several questions. Was this a deliberate effort in order to avoid taking drastic action against the early developments of cyber-attacks against member states? Was the lack of mentions grounded in a generally shallow understanding of their interplay, and if so – a result of the slow developments of a big defensive alliance? Or perhaps the internal norms of NATO played a dictating role in setting the agenda for priorities and willingness to act? Additionally, if the latter question rings true, a thorough examination of how NATO sees its own identity could shed light on the phenomenon. The quantitative content analysis shows a consistent and

frequent reference to Russia - the traditional enemy[12]. It also shows consistent mentions of terrorism and proliferation of WMDs. These things (Yost 2010; Sowers 2009) could stem from NATO's involvement in Afghanistan since 2001 after the terrorist attack of 9/11, an invasion and occupation justified on grounds of the possession of weapons of mass destruction. If NATO saw these as the core associative concepts in relation to Article 5, then changing or adding to this course by acknowledging cyber-attacks to trigger the same consequences could have blurred the direction NATO was growing towards.

The 8th CyCon of June 2016 a conference organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), sheds further light on this topic. In practical terms, the NATO high officials attending and speaking at the conference is herein understood as an extension of the views and concerns of NATO itself. The opening speaker, Toomas Ilves[13], both president of Estonia and a board member of the advisory board of Center for Internet Security, highlighted several points that correlate with the content analyses of this paper. Firstly, Ilves accounts for the various ways in which a cyber-attack has the potential to hurt a country's critical infrastructure. Furthermore, a throwback to the decision not to invoke Article 5 at the time of the 2007 cyber-attacks acted as a transition into voicing expectations about cyber being named the 5th domain of warfare at the Warsaw Summit in July 2016. This would follow land, air, sea, and space, and have major implications for the structure and ways of operation within NATO. The Czech minister of defence Martin Stropnicky expanded on the inclusion of cyber as the 5th domain of warfare, arguing that this would have two main implications. Firstly, the recognition of cyber as a domain of warfare would increase budgets allocated to cyber security. Secondly, it would require mass-recruitment and training of experienced cyber specialists. Deputy Supreme Allied Commander of Transformation in Norfolk, Virginia, Manfred Nielson, expressed the necessary emphasis on the research and documentation carried out by the CCDCoE as a means to combat cyber threats. Additionally, Nielson urged the crowd to agree to recognizing cyber as a fifth domain of warfare, and pointed out that cyber cannot be limited by military perspectives. By the latter point, Nielson refers to the role of cyber in all aspects of organization, defence, surveillance, intelligence, and also offense.

In the following panel debate of CyCon 2016[14], the increasing dependence on IT in military operations was the subject of accentuation. Moreover, the recognition of the 5th dimension of warfare in Warsaw would both increase NATO's power in modern and future

[12] See table 1
[13] See https://youtu.be/j34jptiIxlQ?t=631 for Ilves' speech.
[14] See https://youtu.be/j34jptiIxlQ?t=7437 for the panel debate of day 1 of CyCon 2016.

warfare by implicitly stating the need for adding cyber capabilities to the alliance. Furthermore, Hans Folmer, commander of the Dutch Defence Cyber Commando identifies that the implementation of cyber as a dimension would lead to conceptual implications. Not only with cyber as an isolated component, but also the interplay with a potential NATO cyber command and the other commands for the four other dimensions. Major General and director of Cyber Intelligence and Information Integration in the UK, James Hockenhull extends the point of inter-organisational cooperation as a changing structure as a result of cyber-implementation. Not only would wielding these powers increase NATO's precision and usefulness, but it is also deemed a necessity to deal with the emerging hybrid approaches to warfare. Furthermore, Hockenhull strongly emphasized the need for NATO to develop a succinct and sufficient cyber doctrine. This could act as a step towards taking a leading role in developing norms in cyber space, and facilitate further cooperation both internally but also with other large organizations and governments. An interesting lesson learnt from the panel debate at CyCon was the disagreement about the need for developing offensive capabilities alongside the defensive ones. Finally, the topic of deterrence was linked to cyber. Deterrence, according to Hockenhull, hinges on the credibility of one's ability to strike back. The asymmetric nature of cyber, however, creates another problem: one must define the appropriateness of retaliation not onto property or human beings, but into the digital space. This is a problem NATO must deal with going forward.

Both Ilves' speech and the panel debate illustrates an understanding of cyberspace and its implications to be of a more sophisticated nature than NATO's cyber policies indicate. This implies a changing culture within certain groups of NATO high officials that is ahead of the curve compared to what has been the dominant culture. This section challenges the strength of H3. While it is clear that the cyber dimension has gained importance, the transformation appears to be an ongoing process rather than a complete change in the *milieu*, and the expected subsequent reformulation of "cyber". The culture and norms that are found in NATO's *milieu* are examined in the next section.

## NATO's Strategic Culture and Norms

Katzenstein (1996) contends that the endurance of NATO as an organization after the end of the cold war can be explained, in part, by the perceived common threats towards the alliance itself (chapter 10, 1996). An acknowledgement of the non-state agencies in international politics

guides understanding of how cultures and norms develop both within these structures and by themselves, but additionally how the same cultures and norms are shaped by external pressures. As a certain culture develops and becomes embedded within an institution, it shapes both the decision-making process and identity of said institution (ibid.). This must be seen in a context where identity constitutes both self and other; NATO and Russia; NATO and terrorists; NATO and cyber criminals, and so forth. Moreover, norms serve "as collective understandings of appropriate behaviour (…)" (ibid.). By building on this, we can see that NATO's is consistent with regards to mentions of "Russia" in particular, but also "terrorism", and "proliferation of WMDs"[15]. The quantitative content analysis guides understanding of the norms guiding what constitutes appropriate behaviour. Correspondingly, the consistency in a lack of mentions of "cyber" and "Article 5" together before the 2014 Wales summit tells us one out of two things. The first alternative is that the outwards projection of threatening to retaliate to cyber-attacks in the same manner as attacks through other dimensions would trigger the collective defence clause which was deemed unwanted. Whichever components complete the sum of appropriate behaviour and thus identity of the institution adds together and maintains a more careful approach to the relationship between "Article 5" and "cyber". The other alternative is that internal norms and preferences (organizational culture) had decision-makers overestimating the importance of their own branches and tasks of the organization. This is not necessarily a conscious process, but the result is regardless a cognitive bias in which one's own work and its importance is judged at an artificially high level. This can result in the organization rejecting new developments for a longer time than what might be beneficial (Lantis 2002; Banchoff 1999). Consequently, the slow change in *milieu* in NATO is expected. As H3 asserts, significant change takes place in the wake of critical junctures. Therefore, the opposite must also ring true: if critical junctures are not perceived as *critical enough*, change is not an automated response. Moreover, it illuminates a disconnect between H3 and H4; while the enrichening association of "cyber" took place in the time period, it did not lead to the perception of a critical juncture by default.

This section contains that NATO's strategic culture and norms are the products of an embedded culture within the organization. This culture constitutes the *milieu* of NATO, and is constantly exposed to a varying degree of scrutiny – from internal and external pressures alike. With this in mind, the next section examines the change from 2002-2016 in which actors NATO has associated with cyberspace.

[15] See table 1.

## Who is the threat? Actors in Cyberspace

The content analysis shows a clear change in which actors NATO associate with "cyber". In the period 2002-2005, cyber is either mentioned as a vague concept, or in the same breath as terrorism. [16] The general focus on terrorism in the wake of 9/11 and the 2005 Madrid bombings is unsurprising. However, the link between cyber and terrorism does imply a mild connection between associations of cyber, and non-state actors performing illicit and dangerous acts towards members of the alliance. In 2006 this was expanded further by including the notion of crime networks, drug profits and nuclear proliferation alongside cyber space threats, as "new threats". In the wake of the 2007 Estonia attacks, the state re-enters the focal point of discourse: not only can states take actions to bolster their defenses against cyber-attacks, but cyber-attacks can shut down several key societal infrastructures such as power grids, government services, banks, and military facilities. In 2008, the unambiguous re-introduction of non-state actors as potential threats for NATO member states again took prominence. This follows an implicit understanding of a two-way channel that is cyber space that can affect both states and non-state actors, and the perpetrator could also be either of the two. In 2009[17] after both Estonia and Georgia had suffered severe cyber-attacks, signified a return to a state-centric approach to cyber security. The impact of attacks on economic and governmental infrastructure emphasized that both services and economic institutions in a country can be the victims of attacks. In 2010 the documents highlight a more in-depth examination of the potential effects of attacks, previously described as lethal towards,

"key infrastructure, economic institutions, and banks", the Bucharest meeting in 2010 offered specific effects, "A well-orchestrated cyber-attack can turn off the power in your house, your city, your country. It can shut down air traffic control. It can shut down banks. In short, a cyber-attack can bring a country down without a single soldier having to cross its borders."[18]

In the very same speech, NATO implicitly calls out Russia as the perpetrator by referring to the attacks as "coordinated". This marks a point in the understanding of cyber-warfare as a blurry arena in which states can coordinate attacks with non-state actors, making

[16] See Appendix A for the documents inferred from regarding this time-period; see Appendix B for the encoded output used in this analysis.
[17] Ibid.: time period 2006-2009
[18] Ibid.: 2010

the problem of attribution with regards to international law a difficult matter to pursue. The period from 2011-2014 is less focused around actors in cyber space[19] and more concerned with the ways research, development, and inter-organizational cooperation can better collective defense. Starting with the Wales summit in 2014, and onwards to Stoltenberg's speech in 2016[20], the statements change focus again, and discuss the need to enhance capabilities in order to maintain the alliance's goals of Euro-Atlantic as well as national security.

All things considered, Russia remains NATO's focus point when discussing threatening actors in a security context. However, a gradual but evident accept of a non-state actors as important players in cyberspace has taken place since 2002. From 2014 onwards, these appear together and are at times indistinguishable in NATO rhetoric. This links to the nature of the cyber-attacks in Estonia, Georgia, and Ukraine – where the cooperation between non-state actors and Russia serves as a lesson for NATO in understanding the inseparable nature of the two.

## Conclusion

The increasing prominence of cyber as a domain in international security makes the study of how key actors perceive its ensuing threats a topic of growing importance. This thesis has utilized a constructivist approach in order to meaningfully examine NATO's perception of the prominence and conceptualization of the cyber component in security. Furthermore, it has advanced this understanding by viewing NATO's resistance to change through a lens of strategic culture; the dominant cultures within NATO have remained weighty until the pressure exerted by external shocks forced a reaction from within. The focus on NATO's internal culture versus an ever changing security environment, propelled by the interconnectedness of technology and society, has proved useful in making sense of the impact of critical junctures on NATO perceptions, and ultimately a reformulation in understanding of what "cyber" is, and the threats it facilitates.

The research questions, *"how has NATO's perception of the prominence of cyber security changed from 2002-2016",* and*, "how has NATO's conceptualization of 'cyber' changed in the same timeframe?"* have been answered by analysing the results of quantitative and a qualitative content analyses. As strategic culture theory expects, these results emphasize

[19] Ibid.: 2011-2014
[20] Ibid.: 2014-2016

the catalysing impact of critical junctures as a pre-requisite for rapid and substantial change. Moreover, while the findings of the results are based solely off official NATO documents and thus only add to understanding of the case of NATO and cyber security, they also echo Eriksson and Giacomello (2006) and Klotz and Lynch (2007)'s ideational emphasis within the field of security studies in a digital age. In addition, the focus on shifting norms and identities within organizations could prove a fruitful focus when examining other actors and their perceptions of the security environment. While it does not equate to an ability to predict behaviour, it has identified an entry point for discovery; by analysing political communication in the context of emerging and transformative security threats, the way an organization projects its perception offers clues to when and how they are prepared to change.

Furthermore, this thesis has tested the claims of four hypotheses. Both H1 and H2 were rigorously proved true in the quantitative analysis. H1 was argued to correlate with existing scholarship on both societal developments and NATO's development. H1 was further tested by isolating summit declarations from 2002-2014 from NATO official speeches, which saw a drastic increase in prominence in the given timeframe. These findings are inextricably linked with H2, as the spikes in "cyber mentions" from 2007-2009 and in 2014 explain a large part of the change that constitutes H1. These findings find further support in that only "cyber" saw this boost in mentions. Graph 2 adds to this understanding by highlighting the two periods as critical junctures that altered NATO's cyber perception. An expansion of the body of documents would add strength to both H1 and H2's claims. H3 finds moderate support in the descriptive statistics in table 1. However, a qualitative analysis was necessary to adequately measure its accuracy. Through a genealogical examination of the qualitative data, several reformulations of "cyber" were identified. These speak both to its timing with regards to critical junctures as well as progressive reformulations of "cyber" over time. The results of examining H3 has serious implications. Essentially, by acknowledging cyber as a key domain in security, NATO must re-evaluate how it prepares for and responds to cyber security matters. Finally, H4 expounds a nuance to H3 through the disconnect between H3 and H4; an enrichening association of "cyber" did take place, however, it did not lead to the perception of a critical juncture by default. In other words, measures did not automatically follow what has been perceived as critical junctures.

The main implications of this research, is the reaffirmation of constructivism and strategic culture theory as an appropriate combination when researching security in the digital age. This thesis confirms that intra-organizational military cultures are resistant to change through the reproductive function of cultural domination and its ripple effects on how NATO's

shared beliefs and norms constitute a *milieu* that dictates the range of options available to deal with new challenges. Consequently, an increasing self-awareness towards this culture could help alter the strength and subsequent effects of dominant strategic cultures to increase NATO's adaptability towards new challenges. Moreover, the methods applied in examining NATO and cyber security are inexpensive and easily replicable. A similar script and theoretical framework could be applied to other organizations such as the European Union, which would allow for a comparative study of the two organizations. This type of research could foster a shared understanding of the respective organizations and their strategic culture, which in turn could improve the grounds for cooperation in the future.

# Bibliography


Arquilla, John and Ronfeldt, David (1993) *Cyberwar is Coming!* Chapter 2 in Athena's Camp: Preparing for Conflict in the Information Age, 1997. Rand Corporation

Berger, Thomas (1994) *Cultures of Antimilitarism*. John Hopkins University Press

Biava, Alessia, Drent, Margriet, and Herd, Graeme (2011) *Characterizing the European Union's Strategic Culture: An Analytical Framework*. Journal of Common Market Studies, 1-22

Castell, Manuel (2010) *The Information Age: Economy, Society, and Culture*. Blackwell Publishers, 2nd edition

Cyber Defence, NATO official webpage section. Last accessed from 12.7.16 from http://www.nato.int/cps/en/natohq/topics_78170.htm

CyCon 2016, "Cyber Power". Full conference available at CCDCoE's YouTube channel. Last accessed 12.7.16 from https://www.youtube.com/user/natoccdcoe

David J. Elkins and Richard E. B. Simeon (1979) *A Cause in Search of Its Effect, or What Does Political Culture Explain?*. Comparative Politics, 11 (2) 127-128.

Deibert, Ronald J (2013) *Black Code: Inside The Battle For Cyberspace.* Signal Publishing

Dunn Cavelty, Myriam (2008) *Cyber-Security and Threat Politics. US Efforts to secure the information age*. Routledge Publishing, London

Dutch National Cyber Security Centre (2014) *Cyber Security Assessment Netherlands-4* (CSAN-4). Published by the Dutch National Cyber Security Centre

Eom, Jung-Ho (2012) *Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare*. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec).

Eriksson, Johan and Giacomello, Giampiero (2007) *International Relations and Security in the Digital Age*. Routledge Publishing, New York

Eriksson, Johan and Giacomello, Giampiero (2006) *The Information Revolution, Security, and International Relations: (IR)relevant Theory?* International Political Science Review, 27 (3) 221-244

Farwell, James P and Rohozinsky, Rafal (2011) *Stuxnet and the Future of Cyber War*. Survival, 53 (1) 23-40

Fidler, David P, Pregent, Richard, and Vandurme, Alex (2013) *NATO, Cyber Defense, and International Law*. Articles by Maurer Faculty, Paper 1672

Geers, Kenneth (2015) *Cyber War in Perspective: Russian Aggression Against Ukraine*. NATO CCD COE Publications, Tallinn 2015

Giacomello, Giampiero and Eriksson, Johan (2014) *International Relations, Cybersecurity, and Content Analysis* in The Global Politics of Science and Technology-Vol. 2

Giles, Keir (2015) *Russia and Its Neighbours: Old Attitudes, New Capabilities*. Chapter 2 in *Cyber War in Perspective: Russian Aggression Against Ukraine*. NATO CCD COE Publications, Tallinn 2015

Grant, Greg (2008) *Hybrid Wars*. Last accessed 14.7.16 at http://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/

Granville, Johanna (2003) *Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions*. Australian Journal of Politics & History, 49 (1) 102-109

Gray, Colin S (2006) *Out of the Wilderness: Prime Time For Strategic Culture*. Report for Defense Threat Reduction Agency, Advanced Systems and Concepts Office. Last accessed 12.7.16 from http://www.nato.int/summit2009/topics_en/21-nato- eu_strategic_partnership.html

Herrington, Lewis and Aldrich, Richard (2013) *The Future of Cyber-Resilience in an Age of Global Complexity*. Politics, 33 (4) 299-310

Herzog, Stephen (2011) *Revisiting Estonian Cyber Attacks: Digital Threats and Multinational Responses*. Journal of Strategic Security, 2 (4) 49-60

Hollis, David (2011) *Cyberwar Case Study: Georgia 2008*. Small Wars Journal, 7 (1). Last accessed 12.7.16 from http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Holsti, Ole R (1969) *Content Analysis for the Social Sciences and Humanities*. Addison-Wesley, Reading

Homeland Security (2015) *Critical Infrastructure Sectors*. Last accessed 14.7.16 from https://www.dhs.gov/critical-infrastructure-sectors

Hudson, Valerie M (1997) *Culture and Foreign Policy*. Lynne Rienner Publications, Boulder, Colorado

Hughes, Rex (2010) *A Treaty For Cyberspace.* International Affairs, 86 (2) 523-541

Humbert, Mathias (2007) *Technology and Workforce: Comparison between the Information Revolution and the Industrial Revolution*. Last accessed 12.7.16 from https://infoscience.epfl.ch/record/146804/files/InformationSchool.pdf

Johnston, Alastair Iain (1995) *Thinking About Strategic Culture.* International Security, 19 (4) 32-64

Junio, Timothy J (2013) *How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate*. The Journal of Strategic Studies, 36 (1) 125-133

Katzenstein, Peter J (1996) *The Culture of National Security: Norms and Identity in World Politics.* Columbia University Press

Klimburg, Alexander (2012) *National Cyber Security Framework Manual*. NATO CCD COE Publications, Tallinn

Klotz, Audie and Lynch, Cecelia (2007) *Strategies for Research in Constructivist International Relations*. M.E Sharpe Publications

Koval, Nikolay (2015) *Revolution Hacking*. Chapter 6 In Cyber War in Perspective: Russian Aggression Against Ukraine. CCD COE Publications, Tallinn

Lange-Ionatamishvili, Elina and Svetoka, Sanda (2015) Chapter 12 in *Cyber War in Perspective: Russian Aggression Against Ukraine*. NATO CCD COE Publications, Tallinn 2015

Lantis, Jeffrey (2003) *Strategic Culture and National Security Policy*. International Studies Review, 4 (3) 87-113

Lindsay, Jon R (2015) *The Impact of China on Cybersecurity: Fiction and Friction*. International Security, 3 (39) 7-47

MacNamara, Jim (2003) *Media Content Analysis: Its uses; benefits and best practice methodology*. Asia Pacific Public Relations Journal, 6 (1) 1-34

McGraw, Gary (2013) *Cyber War is Inevitable (Unless We Build Security In)*. The Journal of Strategic Studies, 36 (1) 109-119

NATO (2016) *NATO Defence Ministers Agree to enhance collective and deterrence*. Last accessed 14.7.16 from http://nato.int/cps/en/natohq/news_132356.htm?selectedLocale=en

NATO Wales Summit Declaration (2014). Last accessed 12.7.16 from http://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO (2009) *NATO's relations with the European Union*. Last accessed 14.7.16 from http://www.nato.int/summit2009/topics_en/21-nato-eu_strategic_partnership.html

Neuendorf, Kimberly A (2002) *The Content Analysis Guidebook*. SAGE Publications

Palmquist, M, Carley, K, and Dale, T (1997) *Applications of Computer Text Analysis: Analyzing Literary and Nonliterary Texts*. In Roberts "Text Analysis for the Social Sciences: Methods for Drawing Statistical Inferences from Texts and Transcripts", Mahwah, New Jersey, 171-189

Rid, Thomas and Buchanan, Ben (2015) *Attributing Cyber Attacks*. The Journal of Strategic Studies, 38 (1-2) 4-37

Rid, Thomas (2012) *Cyberwar Will Not Take Place*. Journal of Strategic Studies, 35 (1) 5-32

Roscini, Marco (2014) *Cyber Operations and the Use of Force in International Law*. Oxford University Press, United Kingdom

Schmitt, Michael N (2013) *Tallinn Manual On The International Law Applicable to Cyber Warfare*. Cambridge University Press

Sigholm, Johan *(2013) Non-State Actors in Cyberspace Operations*. Journal of Military Studies, 4 (1)

Singer, Peter and Friedman, Allan (2014) *Cybersecurity and Cyberwar*. Oxford University Press

Sowers, Alexandra K (2009) *Changes in Branding Strategy: A Discourse Analysis of NATO Publications and Speech Regarding its Russian Relationship and the NATO-Russia Council*. Thesis, Georgia State University

Stone, John (2013) *Cyber War Will Take Place!* Journal of Strategic Studies, 36 (1) 101-108

The North Atlantic Treaty (1949) April 4th, 1949 in Washington DC. Last accessed 14.7.16 from http://www.nato.int/cps/en/natolive/official_texts_17120.htm

Banchoff, Thomas (1999) *The German Problem Transformed: Institutions, Politics, and Foreign Policy, 1945-1995*. The University of Michigan Press, Ann Arbor.

Wirtz, James J (2015) *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*. Chapter 3 In Cyber War in Perspective: Russian Aggression Against Ukraine. CCD COE Publications, Tallinn

Yost, David (2010) *NATO's evolving purposes and the next Strategic Concept*. International Affairs, 86 (2) 489-522

## Body of Documents

This subsection is an overview of the documents used in the content analyses, with links to where to find them online. All links were confirmed functioning as of July 13th 2016.

NATO, Summit Declaration Prague 2002
http://www.nato.int/docu/pr/2002/p02-127e.htm

NATO, Speech at SecGen Warsaw "Building Security in an Uncertain World". February 14th 2002
http://nato.int/docu/speech/2002/s020214a.htm

NATO, Speech "Farewell to SACEUR". January 15th 2003
http://www.nato.int/cps/en/natohq/opinions_20406.htm?selectedLocale=en
NATO, Summit Declaration Istanbul 2004
http://www.nato.int/docu/pr/2004/p04-096e.htm

NATO, Keynote Speech at SecGen Norfolk USA. April 5th 2004
http://www.nato.int/docu/speech/2004/s040405a.htm

NATO, Speech and conference Brussels. June 9th 2005
http://www.nato.int/docu/speech/2005/s050609e.htm

NATO, Summit Declaration Riga 2006
http://www.nato.int/docu/pr/2006/p06-150e.htm

NATO, Keynote Speech at Riga Conference. November 28th 2006
http://www.nato.int/docu/speech/2006/s061128a.htm

NATO, Speech "Today's NATO, and why it matters". London, September 5th 2007
http://www.nato.int/docu/speech/2007/s070905b.html

NATO, Summit Declaration Bucharest 2008
http://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO, Speech "NATO: The Next Decade". Brussels June 3rd 2008.
http://nato.int/docu/speech/2008/s080603a.html

NATO, Speech "Emerging Security Risks" London. October 1st 2009
http://www.nato.int/cps/en/natolive/opinions_57785.htm

NATO, Summit Declaration Lisbon 2010
http://www.nato.int/cps/en/natolive/official_texts_68828.htm

NATO, Speech "Meeting Future Challenges Together". Bucharest May 7th 2010
http://www.nato.int/cps/en/natohq/opinions_63307.htm

NATO, Keynote Speech "Building security in an age of austerity". Munich February 4th 2011
http://www.nato.int/cps/en/natolive/opinions_70400.htm

NATO, Summit Declaration Chicago 2012
http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO, Speech "NATO in the New Global Security Era". Amman June 21st 2012
http://www.nato.int/cps/en/natohq/opinions_88536.htm?selectedLocale=en

NATO, Speech "Switzerland and NATO: Partners in Security". Zurich November 22nd 2012

http://www.nato.int/cps/en/natolive/opinions_91490.htm

NATO, Summit Declaration Wales 2014
http://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO, Keynote Speech at NATO Transformation Seminar. March 25th 2015
http://www.nato.int/cps/en/natohq/opinions_118435.htm

NATO, Speech "Projecting Stability: Charting NATO's Future". Washington April 6th 2016
http://www.nato.int/cps/en/natohq/opinions_129758.htm?selectedLocale=en

# Appendix A

Below is the script required to run the analysis in R 3.1.1 Every line starting with a # is a comment line, which explains the function of the commands below it.

## R-Script

```
# Text Mining - NATO and Cyber

# Before running the code, put all documents in one folder, entitled "sources"

library(tm)
library(stringr)
library(dplyr)

#---------- Analysis 1 ----------#
# List the 8 keywords of interest[21]
term <- c("cyber",
        "new threats",
        "regional stability|regional security|regional defense|regional defence",
        "terrorism",
        "proliferation", # of weapon/s of mass destruction
        "biological weapon|nuclear weapon|chemical weapon|weapon of mass
destruction|weapons of mass destruction",
```

[21] Note: Analyses were done with additional words such as "internet", "computer", "digital", without a difference in output. The script is therefore kept as simple as possible.

```
        "russia",
        "article 5")

# Create a vector of PDF file names
files <- list.files(path = "sources", pattern = "pdf$")

# create function to read in PDF files
Rpdf <- readPDF(control = list(text = "-layout"))

# Convert the PDF files to text and store them in corpus
corpus <- Corpus(URISource(paste0("sources/", files)),
                 readerControl = list(reader = Rpdf))

# Clean the corpus for better matching of search terms
clean <- function (corpus) {
   # convert words to lower case
   cleaned  <- tm_map(corpus, content_transformer(tolower))

   # remove white spaces
   cleaned <- tm_map(cleaned, stripWhitespace)

   # remove punctuation
   cleaned <- tm_map(cleaned, removePunctuation)

   return (cleaned)
}

cleaned.corpus <- clean(corpus)

# Initialize frequency table
df <- data.frame(matrix(NA, ncol=9),
            row.names = NULL,
            stringsAsFactors = FALSE)

# Rename columns of frequency table
name <- c("cyber",
        "new.threats",
        "regional.stability.security.defence",
        "terrorism",
        "proliferation", # of weapon/s of mass destruction
        "biological.nuclear.chemical.weapon",
        "russia",
        "article5")
colnames(df) <- c("file", name)

# Iterate through each filename and search term to record frequency
for (i in 1:length(files)) {
   df[i,1] <- files[i]
   for (j in 1:length(term)) {
      df[i,j+1] <- sum(str_count(cleaned.corpus[[i]]$content, term[j]))
```

```
    }
}
write.csv(df, "Prominence.csv", row.names = FALSE)


#---------- Analysis 2 ----------#
# Initialize data frame
par <- data.frame(matrix(ncol=3),
                  row.names = NULL,
                  stringsAsFactors = FALSE)

# Rename columns of data frame
par.name <- c("paragraph",
          "file",
          "line.no")
colnames(par) <- par.name

# Iterate through each filename and record paragraphs with "cyber"
for (i in 1:length(files)) {
    add.para <- cleaned.corpus[[i]]$content[grepl("cyber", cleaned.corpus[[i]]$content)]
    add.line <- grep("cyber", cleaned.corpus[[i]]$content)
    add.file <- rep(files[i], length(add.para))

    add.par <- cbind(add.para, add.file, add.line)
    colnames(add.par) <- par.name
    par <- rbind(par, add.par)
}
write.csv(na.omit(par), "Paragraphs.csv", row.names = FALSE)
```

# Appendix B

Appendix B contains the coding scheme and full output of the qualitative conceptualization analysis of the content.

## Coding Scheme

[1] Blunt or vague statement

**[2] Associations with cyber and other concepts**

[3] Statement indicating complexity of cyber

2002:

- Cyber-attacks [1]
- Cyber **warfare** [2]
- Borderless threats [3]

The initial awareness of cyber as a concept, combines attacks and warfare with the idea of borderless threats.

2003:

- Cyber-attack [1]

2004:

- Cyber security [1]

2005:

- Cyber space [1]

2006:

- Cyber-attack [1]
- Protecting Information and Communications Technology (ICT) [2]

This year saw a minor shift, as the focus turned to protecting ICTs from cyber-attacks.

2007:

- Cyber-attack [1]
- IT **Infrastructure** [2]
- Cyber defence [1]
- **Power grids, banking systems, government services** [2]
- Economic impact of attacks on critical infrastructure [2]

In 2007 a connection between IT infrastructure and specifics like power grids, banking systems, and government services were made. This follows the context of the 2007 cyber-attacks on Estonia. Furthermore, it displays NATO realizing the potential effects on the economy by cyber-attacks.

2008:

- Non-state actors and globalization affecting security [3]
- Cyber-attack [1]
- Operational requirements (…) **cyber defence and energy security** [2] [3]
- Cyber defence policy [1]
- CCDCoE [1]
- Cyber defence [1]
- **Protecting ICTs** [2]
- Countering cyber-attacks [1]
- Developing capabilities of cyber defence [1]

2008 was a big year for NATO and cyber security. The previous years' attacks on Estonia, and 2008's cyber-attacks on Georgia made for a more complex understanding of the cyber component in warfare. Firstly, the complexity of non-state actors in a globalized world is described as an increasing threat to security. Secondly, cyber defence and energy security are linked, and the need to protect NATO's ICTs emphasized. A growing need to invest and develop in cyber defence, both through the CCDCoE, as well as within member states appears in the discourse.

2009:

- Cyber security [1]
- Governments and private companies **both launch attacks** [2] [3]
- Private companies suffer **lost revenue, data, and services** [2]
- Cooperation between public and private sectors necessary [1]
- Cyber defence improvements [1]
- Difference between piracy and cyber security [1]
- Costs for both industry and governments of cyber-attacks [1]
- Cyber defence [1]
- Attacks of industry and government websites daily [1]

In 2009, the actors involved when discussing cyber security see an expansion that now includes both governments and private companies. From a defensive point of view, the attacks allegedly performed by Russia in the previous two years had to depend on a coordination between non-state and state actors to be effective. Moreover, this showed promise to have severe impact on private companies' revenue, data retainment, and ability to perform services. Exemplified by the temporary shut-down of governmental web services in Tallinn, or to interfere with communications systems in Georgia in coordination with the invasion. Additionally, NATO

texts from 2009 explicitly emphasizes the difference between cyber piracy, and cyber security – all though they are inextricably linked.

2010:

- Agreement to enhance cyber defence capabilities [1]
- Transnational-challenges in 2010; **proliferation, terrorism, maritime, cyber, and energy security** [1] [2] [3]
- Cyber threats increasingly sophisticated [1]
- Cyber-attacks [1]
- Detecting, assessing, preventing, defending, and recovery of cyber-attacks on critical systems [1] [2] [3]
- Centralized cyber protection (NCIRC) [1]
- Assisting and developing allies' capabilities [1]
- Cooperation with United Nations and European Union [1]
- Cyber defence policy development to be ready in 2011 [1]
- Cyber defence [1]
- Cyber-attacks on power grids, houses, cities [3]
- Air traffic controls, shutting down banking services [2] [3]
- Coordinated attacks to cripple key infrastructure [1] [2]
- Cyber warfare recognized at permanent aspect of low-level warfare [1]
- Missile defence, energy security, and cyber defence as NATO's new dimensions [1]
- Cyber cannot be put on the back-burner, must have priority [1]

2010 saw a great increase in projecting understanding about cyberspace, warfare, and security. The complexity of cyber is accentuated by connecting trans-national challenges of proliferation, terrorism, maritime, cyber, and energy security. Furthermore, the importance of breaking down understanding of cyber defence as a mechanism to both detect, assess, prevent, defend, and recover from cyber-attacks to critical infrastructures. An acknowledgement of an increasing sophistication in the style of attacks, and the urging need to cooperate both within the alliance, as well as with both the European Union and the United Nations takes prominence. Additionally, the concept of defending critical infrastructure develops into accounting for power grids, houses, cities, air traffic controls, banking services etc., and the urgent need of establishing better practices in public-private cooperation in cyber security.

2011:

- Cyber defence [1]
- Shared research and development between NATO members necessary to overcome challenges [1]
- Protecting critical infrastructure a shared and important goal [2]
- Developing closer links with the private sector to bolster cyber security [1] [2]
- Public-private partnerships [1]

In 2011, the points from the previous two years were firmly re-stated. The need for (shared) research and development, with the purpose of protecting critical infrastructure both in the private and public sectors.

2012:

- A large increase in number and sophistication of attacks [1]
- Cyber defence capabilities [1]
- **Defence measures of infrastructure** [2]
- Cooperation and collaboration central in tackling issues [1]
- Lean on the expertise of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) [1]
- Cyber-**crime** is rampant [1] [2]
- New, borderless threats face member nations [1]
- **Terrorism, piracy, cyber-crime** [2]
- A rapidly evolving security environment [1]

2012 solidified the discourse of protecting critical infrastructure as a core responsibility of NATO's defence alliance. This, again, is to be done through collaboration and cooperation both internally and externally. In a context where cyber-crime is rampant, and also linked with both terrorism and piracy, these new borderless threats face member nations in a rapidly evolving security environment.

2013:

- Cyber-crime with large economic costs [1]

A simple re-stating of the economic costs that follow cyber-crime.

2014:

- Modernizing NATO's forces [1]
- **Cyber defence and national defence** [1] [2]

- Cyber-attacks likely to be more common, sophisticated, and potentially more damaging in the future [1] [3]
- **Cyber policy is centered around prevention, detection, resilience, recovery, and defence** [1] [2] [3]
- Defend NATO's own ICT is a fundamental responsibility [1]
- **Cyber-attacks could trigger article 5** [1] [2] [3]
- Enhance **national networks that NATO relies on for core tasks of cooperation and defence** [1] [2]
- Integrate **cyber component to NATO operations** [1] [2] [3]
- Cooperation with European Union and United Nations [1]
- Must improve and **increase training, exercise, and education of cyber** [1] [2]

The Wales summit declaration could prove to be a paradigm shift for NATO and cyber security. Not only are attacks portrayed as increasing in number and volatility, but the cyber policy is laid out as a confirmation of the 2010 specifics on how to prevent, detect, recover, defend, and build resilience. The most prominent change in NATO's discourse of 2014, was the acknowledgement that cyber-attacks could trigger article 5. Furthermore, the idea of integrating a cyber-component to NATO operation would also characterize as a paradigm shift of how NATO conducts its operations. This development is grounded in the need to improve and increase training, exercise, and education of personnel in the dimension of cyber.

2015:

- Must develop response to cyber aggression [1]
- **Cyber is now part of all crises and conflicts** [1] [2] [3]
- **Cyber can trigger article 5** [1] [2] [3]
- Must improve cyber resilience [1]
- Cyber as a complex and fast-moving issue [1] [3]
- Cyber security requires a comprehensive approach [1]
- **Cyber and hybrid warfare is inextricably linked** [1] [2] [3]
- NATO must develop concrete cyber strategies [1]
- **NATO must adapt to the new security environment** [1] [2]

2015 was a ground-breaking year with regards to NATO's discourse on cyber. There are three main facets of this: Firstly, "Cyber is now part of all crises and conflicts" speaks to not only the prominence of cyber, but also the need to integrate a conscious cyber policy to all aspects of NATO. Secondly, the notion that a cyber-attack can trigger article 5 has at this point become

recurring. In effect, this could have gross implications of how NATO prepares for, and responds to cyber-attacks. Lastly, for the first time in an official document, cyber and hybrid warfare are discussed as inextricably linked. With regards to the need to adapt to a new security environment, the concept of cyber has at this point in time reached a level of complexity and criticalness that NATO implicitly has to undergo some sort of re-structuring of the alliance's ways to deal with this reality.

2016:

- NATO is looking to **improve its resilience versus cyber and hybrid threats** [1] [2] [3]
- Cyber defence is in need of improvement [1].

The latest official statements resubmits the necessity of improving NATO's resilience to deal with both cyber and hybrid threats. Furthermore, the secretary general urges the need for an improvement with regards to NATO's cyber defence.

## Conceptualization over time: Output

| Paragraph | Title | Year |
|---|---|---|
| Strengthen our capabilities to defend against **cyber attacks**. | NATO Summit Declaration, Prague | 2002 |
| The real threats to our security, from regional instability to the proliferation of ballistic missile technology and nuclear, biological and chemical agents, to terrorism, to **cyber-warfare**, to organised crime, do not recognise borders, and are faced by NATO Allies and Russia alike. Isolating or ignoring Russia would only hobble our response to those dangers. If we can develop common approaches to these challenges, if we can find a way to fulfil the Founding Act's vision of joint action against these threats, we will all benefit. Close practical and pragmatic | NATO Speech, SecGen, Warsaw | 2002 |

| | | |
|---|---|---|
| cooperation between NATO and Russia could be as important a transformation for its good in the strategic environment as the events of September 11 were for evil. | | |
| Since the terrorist attacks of September 11, 2001, you have demonstrated critical leadership in helping NATO and Allied militaries transform to meet the needs of the modern security environment. By playing pivotal roles in defining a ground-breaking military concept for the defence against terrorism, to focusing SHAPE on the threats from weapons of mass destruction or **cyber attack,** your tenure has indeed helped retool the Alliance for the future. | NATO speech, North Atlantic Council | 2003 |
| Our scientists have pooled their efforts in areas such as explosives detection, the secure decommissioning of nuclear submarines, **cyber-security**, and the psychological and social causes, effects and responses to terrorism. We have tested and enhanced our capabilities to manage the consequences of terrorist attacks, with the large scale exercise that Russia hosted in Noginsk in 2002, and another planned in Kaliningrad this coming June. | NATO keynote Address, NATO Russia Council, Norfolk | 2004 |
| There are also some areas of NATO-Russia cooperation which do not get the headlines regularly. Let me mention to you the first meeting of the NATO-Russia Council Science Committee to be held in St. Petersburg in a few weeks; where scientists from NATO countries and Russia will debate cooperation in such | NATO News Conference, NATO-Russia Council, Brussels | 2005 |

| | | |
|---|---|---|
| areas as explosive detection and the psychological and sociological consequences of terrorism and **cyber security**. | | |
| First and foremost, it is not enough to agree on our analysis of this new 21st century world. We all know that it is a world of globalised threats that require a globalised response. We know that we have to anticipate threats emerging from anywhere: events in the world's poorest and most under-developed societies can threaten the security of the world's wealthiest. We know that we have to confront not single, easily identifiable threats but flows: that is to say terrorism allied to drug profits or **cyber space** ; or small arms allied to militias and to illicit diamond trading; or organised crime networks allied to nuclear proliferation. The new conventional wisdom is that we need to operate without self-imposed geographical restrictions; that we need armed forces able to create and maintain stability as much as to win wars; and that we will not succeed unless we have an integrated approach where military, diplomatic and economic means combine to produce maximum effect | NATO Keynote Speech, Riga | 2006 |
| Work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against **cyber attack.** | Riga Summit Declaration | 2006 |

| | | |
|---|---|---|
| The range of threats has also expanded, from classic military challenges to new ones. Peter mentioned **cyber-attacks**. He was right to. Estonia put up a stout and skilled defence of its IT infrastructure, and weathered the storm. I'm not sure every NATO country could defend itself so well. | NATO Speech, London | 2007 |
| **Cyber attacks** can take out a power grid, a banking system, and government services. While the attacks take place in **cyber-space**, the effects are very real. And while they are not military in the traditional sense, they have a clear security dimension, along with -- and linked to -- their economic impact | NATO Speech, London | 2007 |
| I also mentioned **cyber defence**. In 2004, NATO set up a centre focused precisely on cyber defence. When Estonia was hit by **cyber attacks**, that NATO centre sent personnel to help. As the military has had years of learning how to protect IT infrastructure, and because there is clearly an advantage to sharing best practices, I believe you will see more of a role for NATO in this area as well. | NATO Speech, London | 2007 |
| Second, the growing power of non-state actors. Globalisation brings incredible opportunities, yet it also has its dark spots. One is that it empowers fanatical individuals, by giving them access to enormously destructive means. I am not thinking of a nuclear "9/11", but a terrorist attack with a radiological weapon certainly can no longer be considered "science fiction". And last year's **cyber attack** against Estonia demonstrated that an attack | NATO Speech, Brussels | 2008 |

| | | |
|---|---|---|
| against another country does not necessarily have to entail the use of military force. For non-state actors in particular, there are other options available | | |
| Second, in addition to making sure that we can meet operational requirements, we also need to move forward on missile defence, cyber defence, and energy security. Regarding missile defence, our recent Bucharest Summit has provided us with a clear roadmap for the future. We agreed that the proliferation of missiles is a growing threat and that the US defence system should be an integral part of any future NATO?wide architecture. Based on this, we are now examining options for a comprehensive missile defence architecture, to be reviewed at our next Summit in 2009. Regarding cyber defence, we not only have a **Cyber Policy** in place now, but we have also created a Centre of Excellence, fittingly located in Estonia's capital, Tallinn. | NATO Speech, Brussels | 2008 |
| NATO remains committed to strengthening key Alliance information systems against **cyber attacks**. We have recently adopted a Policy on **Cyber Defence**, and are developing the structures and authorities to carry it out. Our Policy on **Cyber Defence** emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a **cyber attack**. We look forward to continuing | Bucharest Summit Declaration | 2008 |

| | | |
|---|---|---|
| the development of NATO's **cyber defence** capabilities and strengthening the linkages between NATO and national authorities | | |
| **Cyber security** – our second topic today – is another case in point. Government and private companies launch **cyber-attacks**. Governments and industry suffer the consequences, in terms of lost revenue, lost data and lost services. And it will take cooperation between the public and private sectors to build real defences. | NATO Speech, London | 2009 |
| We also want to do better at **cyber defence**. NATO's **Cyber Defence Centre** is a good step in the right direction. But the sustained, directed **cyber attacks** Estonia suffered a couple of years ago shows that the problem is much bigger than that. On both subjects, I'm very much looking forward to the discussions today. But there is a fundamental difference between, one the one hand, piracy and **cybersecurity**, and climate change on the other. In the first two cases, the threat is very clear. We know what a pirate looks like – and no, I'm not thinking of someone with an eye patch and parrot on his shoulder. I'm thinking of someone well armed and ruthless. The kidnapping and ransom is taking place now. The costs to industry and Governments are easily calculated. And while implementing them might be difficult, we have a pretty good idea of what the right solutions might be. | NATO Speech, London | 2009 |

| | | |
|---|---|---|
| The same is true of **cyber defence**. Attacks on industry and government websites and information systems are already a daily occurrence. Again, the costs are pretty easy to calculate. And while we are certainly able to do better, we have a general idea of the steps we should take. The challenge is figuring out how to do it. | NATO Speech, London | 2009 |
| Agreed to enhance our **cyber defence** capabilities; agreed | Lisbon Summit Declaration | 2010 |
| Partnerships enhance Euro-Atlantic and wider international security and stability; can provide frameworks for political dialogue and regional cooperation in the field of security and defence; contribute to strengthening our common values; and are issued by the Heads of State and Government participating in the meeting of the North Atlantic Council essential to the success of many of our operations and missions. They enable us to share expertise; support broader reform; promote transparency, accountability and integrity in the defence sector; train and assist our partners in developing their own capabilities; and prepare interested nations for membership in NATO. They are also important in addressing emerging, and continuing, trans-national challenges such as proliferation, terrorism, maritime-, **cyber- and energy security**. | Lisbon Summit Declaration | 2010 |
| **Cyber threats** are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to | Lisbon Summit Declaration | 2010 |

| | | |
|---|---|---|
| cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conficts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a **cyber attack** against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO's defence planning processes in order to promote the development of Allies' **cyber defence capabilities**, to assist individual Allies upon request, and to optimise information sharing, collaboration and interoperability. To address the security risks emanating from **cyberspace**, we will work closely with other actors, such as the UN and the EU, as agreed. We have tasked the Council to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth **cyber defence policy** by June 2011 and to prepare an action plan for its implementation. | | |
| Face current, evolving and emerging challenges – including through expanding the current theatre missile defence programme, and defending against **cyber attacks**. | Lisbon Summit Declaration | 2010 |
| So let us look beyond Afghanistan. Let us look at some of the other security challenges that we will have to confront – challenges where | NATO Speech, Bucharest | 2010 |

| | | |
|---|---|---|
| acting now is paramount: coping with proliferation, energy security, and **cyber defence**. | | |
| My third example is **cyber defence**. Nowhere is the need to act today rather than tomorrow more evident than in this area. A well orchestrated **cyber attack** can turn off the power in your house, your city, your country. It can shut down air traffic control. It can shut down banks. In short, a **cyber attack** can bring a country down without a single soldier having to cross its borders. This is not science fiction. It is the real world. Three years ago, our Ally Estonia suffered **a coordinated cyber attack** that temporarily crippled key governmental, financial and media services. Several other NATO and partner nations have experienced similar attacks, although without suffering the same degree of disruption. So it is no exaggeration to state that **cyber attacks** have become a new form of permanent, low-level warfare. Our NATO Headquarters, for example, suffers over 100 attacks per day. | NATO Speech, Bucharest | 2010 |
| Above all, we set up the NATO Centre of Excellence on **cyber defence** in Estonia. So we now have a focal point for developing practical action programmes and for sharing lessons learned and best practice – both among Allies and with partners. | NATO speech, Bucharest | 2010 |

| | | |
|---|---|---|
| Missile defence, energy security and **cyber defence** are new dimensions for NATO. And | NATO Speech, Bucharest | 2010 |

| | | |
|---|---|---|
| we have to address them while other pressing tasks – notably our Afghanistan mission – call for our political attention and our financial resources. This will inevitably raise questions about the proper balance between the various tasks of NATO. | | |
| I am not going to prejudge the new Strategic Concept. But I'll make one point very clear: We cannot afford to put missile defence, energy security or **cyber defence** on the back burner. Because new challenges don't wait until we feel ready to meet them. It is our job – indeed, our duty – to prepare ourselves. We need to look ahead. To prevent unwelcome developments, or to mitigate their consequences | NATO Speech, Bucharest | 2010 |
| But pooling is not enough, if we don't put our money where the real priorities are. At the NATO Summit in Lisbon last November, we identified several of these priorities, including **cyber defence**, and the fight against terrorism and piracy. We also agreed on ten critical capabilities for our forces – such as helicopter transport, medical support, and countering road-side bombs. | NATO Speech, Munich | 2011 |
| So even big European nations have difficulty in keeping the edge, for example on drone technology. At a time when challenges are global, 80 per cent of European Research and Development continues to be spent on national programmes. We need to do better. If nations devote a greater share of their Research and development spending to multinational | NATO Speech, Munich | 2011 |

| | | |
|---|---|---|
| projects, that will make a difference. For example, smaller nations who can't necessarily develop their own responses to **cyber threats** could join together. NATO can help and advise them on how to protect their critical information infrastructures. | | |
| To prepare for the future, let us also build closer links with the private sector – and I am pleased to see several representatives from industry at our meeting today. In the past, military Research and Development put defence at the cutting edge of technology, with the civilian sector eventually taking advantage of those innovations. Now, in many areas, the situation has reversed. Industry has a wealth of expertise, including on **cyber defence**, fuel cell energy and light logistics. We must find better ways through public-private partnerships to explore the military potential of emerging technologies, and to involve industry sooner and more closely. | NATO Speech, Munich | 2011 |
| **Cyber attacks** continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the **cyber defence** commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a **Cyber Defence Concept**, Policy, and Action Plan, which are now being implemented. Building on NATO's existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, | Chicago Summit Declaration | 2012 |

| | | |
|---|---|---|
| will be in place by the end of 2012. We have committed to provide the resources and complete the necessary reforms to bring all NATO bodies under centralised cyber protection, to ensure that enhanced **cyber defence capabilities** protect our collective investment in NATO. We will further integrate **cyber defence measures** into Alliance structures and procedures and, as individual nations, we remain committed to identifying and **delivering national cyber defence capabilities** that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from **cyber attacks.** To address the **cyber security threats** and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation. We will also take full advantage of the expertise offered by the **Cooperative Cyber Defence Centre of Excellence in Estonia** | | |
| Over the past few decades, NATO has adapted to the new, global security challenges of the 21st century – terrorism, failing states, proliferation and **cyber crime**. The Alliance has turned into a very flexible security instrument -- an instrument at the service of | NATO Speech, Jordan | 2012 |

| | | |
|---|---|---|
| our own 28 member nations, but also, and increasingly, at the service of the wider international community as well. | | |
| Risks and threats like terrorism, proliferation, piracy and **cyber crime** know no borders – and they tend to reinforce each other too. To meet these challenges and to defeat them will require a new level of international consultation and cooperation. | NATO Speech, Jordan | 2012 |

| | | |
|---|---|---|
| Threats like terrorism, the proliferation of weapons of mass destruction, and **cyber warfare** know no borders. Instability halfway around the world can have a direct impact on our security at home. Today, territorial defence and security demand a global perspective. | NATO Speech, Zurich | 2012 |
| Recently, Switzerland has expressed an interest in broadening its political dialogue and practical cooperation with NATO to include issues **such as cyber-security** and countering proliferation. We welcome this interest. And look forward to working more closely with you on these issues in the future. They are a further demonstration of your country's understanding of our evolving security environment, and the merits of your partnership with NATO. | NATO Speech, Zurich | 2012 |
| Europol, the European Union's law-enforcement agency, puts the annual value of corporations' losses from **criminal cyber activity** at one trillion US dollars. | NATO Speech, Dubrovnik | 2013 |

| | | |
|---|---|---|
| NATO needs, now more than ever, modern, robust, and capable forces at high readiness, in the air, on land and at sea, in order to meet current and future challenges. We are committed to further enhancing our capabilities. To this end, today we have agreed a Defence Planning Package with a number of priorities, such as enhancing and reinforcing training and exercises; command and control, including for demanding air operations; intelligence, surveillance, and reconnaissance; NATO's ballistic missile defence capability, in accordance with the decisions taken at the 2010 Lisbon and 2012 Chicago Summits, including the voluntary nature of national contributions; **cyber defence**; as well as improving the robustness and readiness of our land forces for both collective defence and crisis response. Fulfilment of these priorities will increase the Alliance's collective capabilities and better prepare NATO to address current and future threats and challenges. We have agreed this Package in order to inform our defence investments and to improve the capabilities that Allies have in national inventories. In this context, NATO joint air power capabilities require longer-term consideration | Wales Summit Declaration | 2014 |
| As the Alliance looks to the future, **cyber threats and attacks** will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, **we have endorsed an Enhanced Cyber Defence** | Wales Summit Declaration | 2014 |

| | | |
|---|---|---|
| **Policy**, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. **Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity**, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence**. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis** | | |
| We are committed to developing further our national cyber defence capabilities, and we will **enhance the cyber security of national networks upon which NATO depends for its core tasks**, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the **cyber defence** | Wales Summit Declaration | 2014 |

| | | |
|---|---|---|
| **capabilities of the Alliance**. We will continue to **integrate cyber defence** into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing **cyber threats and risks**. We will therefore continue to engage actively on **cyber issues** with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. **We will improve the level of NATO's cyber defence education, training, and exercise activities**. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO CIS School and other NATO training and education bodies | | |
| In a crisis, the first responder will be the nation that is targeted. But NATO must be there to support any national efforts. This is a matter of planning and of political will; and making sure that we complement and reinforce each other. We need to be able to deal with complex evolving hybrid situations, **including cyber-aggression** | NATO Keynote Speech, Washington | 2015 |

| | | |
|---|---|---|
| **Cyber** is now a central part of virtually all crises and conflicts. NATO has made it clear that **cyber-attacks can potentially trigger an Article 5 response**. We need to detect and counter **cyber-attacks early; improve our resilience**; and be able to recover quickly. A more active cyber policy should be a focus as we plan for Warsaw. **Cyber defence** is just one of the capabilities we need in order to deal with the changed security environment... which brings me to my second point: how do we keep our edge? | NATO Keynote Speech, Washington | 2015 |

| | | |
|---|---|---|
| But once it's done, it sends a very power signal: 28 Allies acting as one. The issues we are facing are complex and fast-moving. **Cyber-attacks happen in seconds**. Missiles reach their targets in minutes. Little green men can move within hours. So we must also be able to move fast. | NATO Keynote Speech, Washington | 2015 |
| But then, as I underlined, we have to have a comprehensive approach and to increase the resilience of our societies. **Cyber is extremely important as part of the strategy which we are developing against hybrid warfare**; but also working with partners, for instance the European Union to improve governance; to increase the general resilience of countries; and therefore, also, reduce the vulnerability towards hybrid warfare. | NATO Keynote Speech, Washington | 2015 |
| I foresee that by Warsaw we have both implemented on the measures which we have already agreed on. But in addition we should | NATO Keynote Speech, Washington | 2015 |

| | | |
|---|---|---|
| have developed more concrete strategies and plans when it comes to, for instance, as I mentioned, **cyber, decision-making** and, of course, some of the elements which is now on the drawing board like a sea component and the naval component and the air component of the Spearhead Force. So there are many elements, some are quite clear already; some we have to develop. But the thing is that we are just in the beginning of a big transformation, a big adaptation of NATO facing a new security environment. | | |
| We will enhance our resilience against **hybrid warfare and cyber threats**. And make sure that the nuclear component of our deterrence posture remains credible and effective. | NATO Speech, Washington | 2016 |
| We are also exploring what more we can do in areas such as counter-terrorism, energy and maritime security, and **cyber defence.** My aim is to bring forward our cooperation with the GCC at the Warsaw Summit in July. | NATO Speech, Washington | 2016 |