NATO's Militarisation of Cybersecurity

Master's Thesis
MSc Political Science: International Organisation

Universiteit Leiden

Leiden University
Faculty of Social and Behavioural Sciences
Institute of Political Science

Erwin Weurding BSc
Student Number: 1535447
Email: e.weurding@umail.leidenuniv.nl

Thesis seminar: **International Institutions and Security Governance**
Supervisor: Dr. N.J.G. van Willigen
Second reader: Dr. M.F. Meffert

9985 Words
11th June 2018

Abstract

NATO, a predominantly military organisation, is involved in a broad array of security topics. However, it considers cybersecurity to be one of its core tasks. In this study, it is researched how a military alliance became involved in the governance of a non-traditional security issue with a large civilian component.

In this study a model of militarisation, based on the Copenhagen School's securitisation theory, is proposed. This model states that militarisation is made possible due to functional differentiation by military security sector actors. Using this model, it is argued that NATO has militarised the issue of cybersecurity by specifically framing it as an issue of cyberwarfare and thereby as a means of hybrid warfare, a military existential threat. The findings from the qualitative case study show that this was made possible when the objective context surrounding cybersecurity changed after the 2007 Estonian cyberattacks.

Table of Contents

Introduction

With the rapid growth of the internet in the past decades, cybersecurity has become a much debated topic. This topic, which did not even exist in the Cold War era, has gained the attention of traditional security organisations in the post-Cold War world. One of these traditional security organisations, the North Atlantic Treaty Organization (NATO), describes "cyber defence" as a "core task of [its] collective defence" on its website (NATO, 2018, February 19).

Although NATO is a security organisation that concerns itself with a broad range of topics (Schlag, 2016, p. 161), it is still "first and foremost a … military alliance" (Mayer, 2008, p. 120). How is it possible then, that a predominantly military organisation describes a non-traditional security issue (NTSI) (Hameiri & Jones, 2015) with a large civilian component, namely cybersecurity, as one of its core tasks? Especially when considering that other NTSIs, for example; pandemics, global warming, pollution or money laundering (Hameiri & Jones, 2015) are not considered to be core tasks by NATO.

In this study a militarisation model, based on the securitisation theory of the Copenhagen School is used, in order to find an explanation for this puzzle. Building upon this model, it is argued that NATO has framed cybersecurity issues not as NTSIs, but as means of hybrid warfare, thereby facilitating militarisation. This model will also shed light on how militarisation occurs instead of "regular" securitisation.

This study is structured as follows. First, the literature on traditional and non-traditional security issues, Copenhagen School securitisation theory, and security governance is reviewed and the research question is formulated. Second, in the Theoretical Framework chapter, the model is explained leading to the hypothesis. Third, the methodology and operationalisation of the qualitative process-tracing case study is described. Thereafter, the findings of the case study are presented and analysed, indicating that they do fit the model,

although with a different precondition than initially expected. Finally, in the concluding chapter, the implications of the findings are discussed.

Literature Review

A clear definition of security issues is needed in order to understand non-traditional security issues. As this study uses a model based on the Copenhagen School of security studies, the concept of security will be defined accordingly.

According to the Copenhagen School, a security issue is something which poses an *existential threat* to a *referent object* (Buzan, Wæver & De Wilde, 1998, p. 21). A referent object in this context being; anything with a legitimate claim to survival (Buzan, Wæver & De Wilde, 1998, p. 36). Whilst an existential threat is something that threatens the very existence and thereby the survival of a referent object (Buzan, Wæver & De Wilde, 1998, pp. 20-21).

This rather broad concept of security includes both traditional and non-traditional security issues. A traditional security issue is an issue in which the referent object (usually) is a state and the existential threat is of a military nature (Buzan, Wæver & De Wilde, 1998, pp. 1-5). This leaves NTSIs, as somewhat of a "catch-all" concept for the remaining referent objects and existential threats. A large array of different topics have been described as examples of NTSIs, including: "transboundary pollution, epidemic diseases, transnational crime and terrorism" (Hameiri & Jones 2015, p. 1). In order to make this concept more manageable, in this study the conceptualisation of NTSIs by Hameiri & Jones (2015) is used. According to them, NTSIs must satisfy the following three criteria:

1. The threat is intensified by economic globalisation (Hameiri & Jones, 2015, p. 1)
2. The threat is of transboundary nature (Hameiri & Jones, 2015, p. 15)
3. The threat is potential (Hameiri & Jones, 2015, p. 22)

The *intensification due to economic globalisation* criterion implies that these threats are more threatening to a referent object because of globalisation. For example, the outbreak of an epidemic disease in South-East Asia, may threaten people all over the world due to airline travel to and from South-East Asia.

The *transboundary nature* of these threats implies that these threats transcend state borders. For example, international terrorist organisations may commit attacks outside of their own country of origin. While this can certainly apply to other (conventional) types of security threats as well, it is a specific requirement for an NTSI according to Hameiri & Jones' framework (2015).

Potentiality, in Hameiri & Jones' framework, implies that the existential threat thus far only exists in theory, as it has not (yet) actually occurred in practice. In other words, the existential threat is not yet a demonstrated threat. For example, in theory modern international piracy is able to cripple global maritime trade. In reality however, a complete disruption of global maritime trade due to piracy has not (yet) occurred.

Concerning NTSIs, the issue of cybersecurity is defined in this study as: "the protection of information and communication technologies from unauthorized access or attempted access" (Finnemore & Hollis, 2016, p. 431). A similar description of "cyber threats" is provided by Radu (2012); a description which notably echoes the criteria of Hameiri & Jones (2015).

The realm of cybersecurity includes civilian as well as military topics. In NATO's case it is important to understand the military side of cybersecurity, namely cyberwarfare, which is defined as:

> [A] state of conflict between two or more political actors characterized by the deliberate hostile and cost-inducing use of CNA [computer network attacks] against an

> adversary's critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes (Liff, 2012, pp. 405-408).

This definition leaves room for the three criteria as described by Hameiri & Jones (2015). As cyberspace does not end at state borders and by itself is a phenomenon of (economic) globalisation, cyberwarfare clearly conforms to the transboundary and globalisation criteria of NTSIs. Concerning the potentiality criterion, cyberwarfare was indeed a potential, non-demonstrated threat. Described as follows by Myriam Dunn Cavelty: "the defining characteristic of the cyber-threats is their unsubstantiated nature: none of the worst-case scenarios have materialized, not even in part" (2010, p. 187). However, various events in the past years have made this potentiality of cyberwarfare debatable. These events, and their implications, are discussed in the next chapter.

Now that security issues have been defined, it is time to consider (international) security governance. One (crude)[1] way of differentiating the different modes governance is by dividing them according to the role played by the state (Peoples & Vaughan-Williams, 2015, p. 5).

One of the main theoretical approaches to the study of international politics, or its derivative, international security, are the rationalist theories. Both rationalist families, liberals and realists, consider states to be the primary actors in the domain of international politics

[1] Peoples & Vaughan-Williams (2015, p. 5), note that this division according to the role of the state does not apply in every single case, but is nonetheless useful in providing a general (crude) division.

(Abbott & Snidal, 1998, p. 6; Mearsheimer, 1994; 2014, p. 17). While liberals leave room for other institutions to act as actors in international politics (Abbott & Snidal, 1998; Keohane & Martin, 1995, p. 42; Ruggie, 1995), and thereby international security as well, most realists however, consider these institutions to be merely tools to be wielded by states (Karns & Mingst, 2010 p. 257; Mearsheimer, 1994). Nonetheless, both rationalist families agree that states are the primary actors in international politics.

While state primacy may be a common feature of the rationalist theories, this does not have to be the case for critical theories, such as (some forms of) constructivism, Marxism, or other strands of theories from different ontological and epistemological backgrounds (Peoples & Vaughan-Williams, 2015, p. 5). Nonetheless, most mainstream scholarly traditions do recognise (some form of) state involvement in security affairs.

The level of state involvement, however, can vary. Globalisation, for example, requires a mode of governance that transcends the traditional state-based one (Held 1997; Karns & Mingst, 2010, pp. 22-23). This has led various authors to argue that because of the globalised and transboundary nature of NTSIs, these issues require a different mode of governance (Bevir & Hall as cited in Hameiri & Jones, 2015, p. 15; IBM as cited in Radu, 2012, p. 147; Krahmann, 2005; Nance & Cottrell, 2014). Such a different mode of governance is found in a *global governance* based approach (Karns & Mingst, 2010, p. 21), involving many different types of actors, including international governmental organisations (IGOs), like NATO.

From the aforementioned non-rationalist epistemological and ontological traditions, the findings of social constructivism provide useful insights into the (global) governance of security issues. Social constructivists in the Wendtian tradition argue that the role played by an actor concerning an issue, is largely dependent on how the issue is socially constructed (Wendt, 1992). Without going into detail about all of the various branches of social

constructivism dealing with security issues, this section focusses on the theory of securitisation according to the Copenhagen School, on which this study's model is based. This version of securitisation theory, is usually described as a branch of social constructivism, although some authors have noticed similarities to (classical) realism as well (Williams, 2003).

Contrary to, for example, structural realists, Copenhagen School theorists argue that in order for a public issue to become part of the political process of security governance, *securitisation* has to occur. Securitisation, in this context, is increasing the degree of an issue's politicisation along the politicisation spectrum.

The first degree an issue can have on this spectrum is being *non-politicised*. This means that "the state does not deal with it and it is not in any other way made an issue of public debate and decision" (Buzan, Wæver & De Wilde, 1998, p. 23). The second degree an issue can take on the spectrum is being *politicised*. This means that "the issue is part of public policy, requiring government decision and resource allocations or, more rarely some other form of communal governance" (Buzan, Wæver & De Wilde, 1998, p. 23). The third degree of politicisation is *securitised*, this means that "the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of the political procedure" (Buzan, Wæver & De Wilde, 1998, pp. 23-24).

According to the Copenhagen School's theory, in order for an issue to become securitised it has to be defined as an existential threat to a referent object by a securitising actor:

> Threats and vulnerabilities can arise in many different areas, military and non-military, but to count as security issues they have to meet strictly defined criteria that distinguish them from the normal run of the merely political. They have to be staged as existential threats to a referent object by a securitizing actor who thereby generates

> endorsement of emergency measures beyond rules that would otherwise bind (Buzan, Wæver & De Wilde, 1998, p. 5).

A *securitising actor*, in the context of this theory, is an actor that is able to declare an issue an existential threat to a referent object (Buzan, Wæver & De Wilde, 1998, p. 36). Such a declaration is considered a *speech act* (Buzan, Wæver & De Wilde, 1998; Buzan & Hansen, 2009, pp. 33-34).

The act of declaring an issue an existential threat to a referent object can be considered a form of *framing* (Watson, 2012). While framing is a method researched in various strands of constructivism, Watson argues that securitisation is merely a more specific form of framing, which employs the single master-frame of security (2012, p. 288). It should be noted however, that while for some types of constructivism a frame can be entirely subjective, for securitisation theory, according to the Copenhagen School, the frame has to be based on contextual and objective facts as well (Buzan, Wæver & De Wilde, 1998, p. 33; Watson, 2012, p. 294).

Furthermore, it should be noted that securitisation is not the same as militarisation (Lobato & Kenkel, 2015, p. 38). While often these two processes are mentioned together and/or treated as the same thing, [2] they are not the same. As militarisation is a type of securitisation, but not a requirement for securitisation. Securitisation involves any "emergency measures and justifying actions outside the normal bounds of the political procedure" (Buzan, Wæver & De Wilde, 1998, pp. 23-24), while militarisation requires these measures to be of a military nature. For example, giving exceptional powers to the police force is a securitisation measure, but not a militarisation measure, as it does not involve the military. Whereas the deployment of troops to guard a famous tourist site, can be considered

[2] See for example: Ahmed (2011) and Graham (2012).

to be both a securitisation measure and a measure of militarisation. In other words, for securitisation, the issue has to be defined according to the security master-frame and can involve many different types of actors, whereas for militarisation the issue has to be defined within a narrower military frame and has to involve military actors.

The concept of *functional differentiation*, the idea that social relations are structured according to functional specialisations (Albert & Buzan, 2011, p. 416), can provide insights under which circumstances militarisation occurs instead of "regular" securitisation. The Copenhagen School initially identified five *security sectors* in which securitisation can occur: the political, economic, military, societal and environmental sectors [3] (Buzan, Wæver & De Wilde, 1998, pp. 7-8). This sectoral approach "allows for a broader empirical consideration of how different referent objects interact within different arenas of security" (Schlag, 2016, p. 166).

At first, these different sectors where mainly used as analytical tools, as all the security sectors are merely parts of the whole political complex (Albert & Buzan, 2011, p. 415). However, in later years, this analytical approach has shifted in favour of functional differentiation (Albert & Buzan, 2011), in which each of the security sectors forms an operational environment for its own actors (although overlap with other sectors is possible) (Albert & Buzan, 2011, p. 420). This implies that an economic issue would mostly be dealt with by economic security sector actors and a military issue by actors from the military security sector. In other words, a military security issue is, under functional differentiation, dealt with by actors from the military security sector of the political complex, leading to the issue to become militarised instead of merely securitised.

[3] Later Copenhagen School scholars have identified more or different security sectors. See for example: Lausten & Wæver (2000) and Lobato & Kenkel (2015).

In this chapter, cybersecurity has been defined as an NTSI. An issue which could be argued to fit into multiple security sectors: the economic sector, the military sector, the political sector or even the societal sector. It is therefore interesting to research why a military alliance and thereby a military security sector-based actor, is involved in the governance of this NTSI, which can be argued to span multiple security sectors of the political complex. As the findings from such a study have implications for how functional differentiation can impact securitisation framing and lead to militarisation instead. This leads to the following research question:

What explains the increased involvement of NATO, a military alliance, in the governance of cybersecurity, a non-traditional security issue?

Theoretical Framework

According to the Copenhagen School, an issue has to be framed as an existential threat to a referent object by a securitising actor in order for it to be securitised. For it to be militarised, the issue has to be framed within a narrower military frame, in order for the issue to "fit" into the military security sector of the political complex. In this chapter this study's theoretical framework is laid out, as to how this process occurred regarding NATO and cybersecurity.

The Changed Objective Context

Framing, according the Copenhagen School, cannot occur regardless of the external objective context (Buzan, Wæver & De Wilde, 1998, p. 33; Watson, 2012, p. 294). This implies that in order for cybersecurity to be reframed, the context in which it exists has to change.

In the previous chapter, cybersecurity has been identified as an NTSI, an NTSI that includes civilian as well as military topics. It is therefore possible that not all topics of

cybersecurity conform to Hameiri & Jones' criteria (2015). The topic of cyberwarfare for instance, can be considered a transboundary threat that is intensified by globalisation, but is no longer a potential threat.

It can be argued that the potentiality of cyberwarfare changed after the cyberattacks on Estonia in 2007. Some authors have even identified these attacks as the catalyst for NATO involvement in cybersecurity governance (Choucri, Madnick & Ferwerda, 2014, p. 110; Fidler, Pregent & Vandurme, 2016, p. 3). However, the nature of these attacks as instances of cyberwarfare, is open to debate. The attacks have, for example, been labelled by the Estonian government as instances of "cyber terrorism" (as cited in Colarik & Janczewsski, 2012, p.34), making their status as acts of cyberwarfare ambiguous. The fact that the Estonian government has described the attacks as acts of cyber terrorism, instead of cyberwarfare, could be considered an example of securitisation without militarisation, as cyber terrorism could be considered a criminal affair and therefore a police issue. While terrorist acts have been treated as military affairs in the past, most notably in the "War on Terror" response to the September 11 attacks in 2001, acts of terrorism are not always responded to by the military. Thus, while the Estonian cyberattacks may present a case of demonstrated cyberwarfare, their ambiguous military nature makes this argument uncertain.

A less ambiguous case of demonstrated cyberwarfare is found in 2010, when the Stuxnet worm, the world's first demonstrated cyberweapon (Langer, 2011), crippled the Iranian nuclear programme. This meant that the threat of a cyberattack damaging vital (military) infrastructure was no longer a potential threat, but has become a real one (Langer, 2011, p 49; Lindsay, 2013). Furthermore, Stuxnet has been described as a "military-grade" weapon (Clayton as cited in Lindsay, 2013). This makes the Stuxnet event a less ambiguous case of cyberwarfare as it is less dependent on an intersubjective interpretation of the events.

Other instances of cyberwarfare after 2010 are, for example, the cyberattacks on the Ukranian electric power grid in December 2015 (Connell & Vogler, 2017, p. 20).

It can therefore be argued that cyberwarfare has become a demonstrated issue, which no longer fits the potentiality criterion of Hameiri & Jones (2015) and thus can no longer fully be considered an NTSI. This changed status of cyberwarfare, from a potential issue to a demonstrated issue, can be argued to have changed the context of cybersecurity. Thereby creating an opportunity for securitising/militarising actors[4] to reframe cybersecurity as an existential threat, or a military existential threat in particular, as will be described in the next section.

The Existential Threat

In the classic Clausewitzian conception, "the use of force provides a military outcome which sets conditions for a political solution" (Simpson, 2012, p. 67). The enemy in this conception is merely an obstacle to achieving a political goal which must be overcome (Simpson, 2012, p. 233).This implies that the balance of power must be tipped in such a way, in favour of the "victor", that a political solution is made possible. Upsetting the balance of power may, according to structural realists, lead to unstable conditions threatening state survival (Mearsheimer, 2014). Warfare, thus may threaten state survival and thereby poses an existential threat. However, this does not have to be limited to conventional forms of warfare.

Building upon the Clausewitzian tradition, General Sir Rupert Smith defined the utility of force in war by the four functions of force: destruction, coercion and deterrence, containment, and amelioration (Smith, 2005, pp. 320-321). Liff's definition of cyberwarfare (2012, pp. 405-408), used throughout this study, echoes these four functions of force. In

[4] In this study, the term *militarising actor* is used instead of *securitising actor* in cases were militarisation instead of "regular" securitisation is concerned.

practice these four functions are demonstrated by the aforementioned Stuxnet worm (Lindsay, 2013), the world's first cyberweapon (Langer, 2011).

It could however be argued that the damaging effects of using a cyberweapon, at least in the present situation, could be limited. The existential threat, posed by the use of cyberwarfare tactics, could therefore be limited as well. However, it is possible to combine conventional ways of warfare with non-conventional ways of warfare, such as cyberwarfare, thereby these non-conventional ways of warfare become a part of the previously mentioned existential threat of war.

This type of warfare, described by Lieutenant Colonel Hoffman as an "operational fusion of conventional and irregular capabilities", is called *hybrid warfare* (Hoffman, 2009, p. 36). The increased threat posed by hybrid warfare vis-á-vis conventional warfare, is notably described in the 2005 U.S. National Defense Strategy: "the most dangerous circumstances arise when we face a complex of challenges … the most capable opponents may seek to combine truly disruptive capacity with traditional, irregular, or catastrophic forms of warfare" (Department of Defense, 2005, p. 2; Hoffman, 2009, pp. 34-35). The Stuxnet event proves the utility of cyberwarfare tactics for war by demonstrating Smith's four functions of force (2005, pp. 320-321) in practice; and thereby its suitability for integration of this irregular form warfare into hybrid warfare.

Thus, cyberwarfare may not necessarily pose an existential threat on its own. War however, definitely poses an existential threat, due its ability to upset the balance of power. When conventional warfare is combined with other irregular forms of warfare, it contributes to the threat. Therefore, although cyberwarfare may pose an existential threat in some cases; a form of hybrid warfare, which includes cyberwarfare tactics, certainly poses an existential threat.

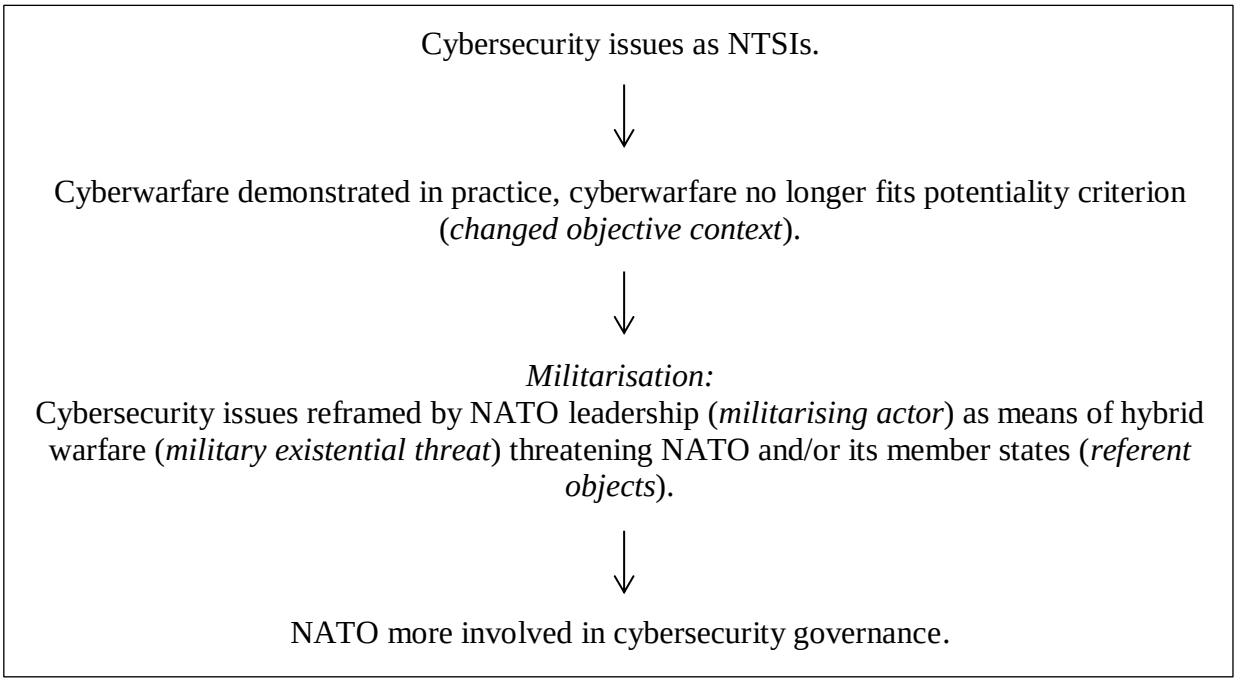
The Reframing of Cybersecurity Issues

An issue cannot simply be (re)framed as a security issue, without the frame being based on objective external contexts (Buzan, Wæver & De Wilde, 1998, p. 33; Watson, 2012, p. 294). As is described in the first section of this chapter, the context of cybersecurity has changed due to cyberwarfare no longer being a potential issue, but a demonstrated one. This changed context of cybersecurity provided a prerequisite for its securitisation. However, while an issue may be securitised, this does not have to imply that the issue is militarised as well. The previous section described how cybersecurity issues can be considered existential threats by means of hybrid warfare. If cybersecurity issues were therefore to be framed as means of hybrid warfare, they become not only existential threats, but military existential threats as well. This facilitates the involvement of the military security sector of the political complex, thus making it a case of militarisation instead of "regular" securitisation. Therefore, it would make sense that NATO, as an actor part of the military security sector of the political complex, would become (increasingly) involved in cybersecurity governance as well.

In order for an issue to become securitised, the Copenhagen School's theory states that an issue would have to be defined as an existential threat to a referent object by a securitising actor. In the case of this study, a case of militarisation instead of "regular" securitisation, this implies that the NATO leadership (the militarising actor), must describe cybersecurity issues as means of hybrid warfare, a military existential threat, to the alliance and/or its member states (the referent objects). This theory is schematically described in Figure 1 and leads to the following hypothesis:

H1: The militarisation of cybersecurity issues facilitated NATO's involvement in cybersecurity governance.

Figure 1. *Schematic summary of the model.*



This theory is relevant because of its implications for the Copenhagen School's version of securitisation theory. The assumption that the involvement of a military actor led to the use of a military frame and thereby militarisation, speaks in favour of functional differentiation of the different security sectors of the political complex, instead of the sectors merely being analytical tools (Albert & Buzan, 2011). Furthermore, the use of framing also speaks in favour of considering the Copenhagen School's theory to be a form of framing theory, but one based on objective facts as well (Watson, 2012). The theory also sheds light on the requirement of a changed objective context for (re)framing. As well as on the effects of a shift from a potential to a demonstrated threat as such a prerequisite condition.

Methodology

Operationalisation

A qualitative single case study by means of process-tracing was conducted. As explained in the previous chapter, in this study it is theorised that the NATO leadership (militarising actor)

has militarised cybersecurity issues by reframing them as means of hybrid warfare, a military existential threat, to NATO and/or its member states (the referent objects), thus increasing NATO involvement in cybersecurity governance.

In order to test this theory, the case was examined for its dependent (DV) and independent variables (IV):

DV: NATO's involvement in cybersecurity governance.

IV: NATO's framing of cybersecurity issues.

Furthermore, according to the Copenhagen School, reframing can only happen in an objectively changed context. Therefore the changed objective context of cybersecurity serves as the condition variable (CV). In the previous chapter it was argued that the Stuxnet demonstration was expected to have provided such a changed context.

CV: Changed objective context of cybersecurity issues.

As the model deals with intersubjective concepts like framing, which can be difficult to quantify, a qualitative approach was used. Concerning the DV, this implies that the primary sources were qualitatively assessed for mentions of NATO involvement in cybersecurity governance. In order to qualitatively assess this involvement, the variable is based on the concept of "policy" according to Versluis, Van Keulen & Stephenson (2011, p. 11). Namely, as *a deliberate statement of NATO action or in-action in the field of cybersecurity*. In order to measure such a deliberate policy statement, this study employed the indicators by Fidler, Pregent & Vandurme, who define NATO cyber defence policy statements as: establishing or

encouraging "the creation of, mechanisms to implement … the strategy of improving cyber defense within the Alliance and in NATO members" (2016, p. 6).

Concerning the IV, the qualitative nature of the analysis left room for assessment of NATO's frame of cybersecurity; whether NATO defines it as an NTSI, a means of hybrid warfare (thus a military existential threat), or as something else entirely. Concerning this variable; explicit mentions of hybrid warfare in conjunction with cybersecurity issues, as well as implicit mentions which fit Hofmann's definition (2009, p. 36), served as indicators. The same applies to explicit mentions of NTSIs and for implicit mentions fitting the criteria of Hameiri & Jones (2015). As previously stated, the concept of cyberwarfare in this study is defined according to the definition of Liff (2012, pp. 405-408).

Case Selection

As this study uses a process-tracing analysis, it is important to identify the timeframe for the analysis. NATO's (initially limited) formal involvement in cybersecurity governance began in 2002 (Burton, 2015, p. 305). The year 2002 therefore served as the starting point of the analysis' timeframe.

As argued in the previous chapter, before the Stuxnet demonstration, cyberweapons were not an actual demonstrated phenomenon, but merely a potential one. When this changed, the objective context of cybersecurity issues is expected to have changed with it. Therefore, the CV divided NATO history in a pre-2010 period, in which cyberweapons were only a theoretical threat, and a post-2010 period, in which cyberweapons have been demonstrated to be an actual existing threat. The difference between these two periods served as the focus of the analysis.

The Estonian cyberattacks, however, were described in the previous chapter as being considered by some authors (Choucri, Madnick & Ferwerda, 2014, p. 110; Fidler, Pregent &

Vandurme, 2016, p. 3), to be the actual catalyst for NATO involvement in cybersecurity governance. Therefore, this option was also taken into consideration for the analysis.

In order to mitigate the interference by other (geo)political variables influencing NATO involvement, the timeframe of the analysis was limited to 2014. This is because the 2014 Ukrainian/Crimean crisis ushered in a new era in NATO history (Kroenig, 2015), which imposes the risk of other and new dynamics and variables influencing the case. Therefore, for the sake of internal validity, the case was limited to the period 2002-2014.

Data Selection

This study relies mostly on primary source data published by NATO itself. These primary sources were drawn from the "Official texts" section of the NATO e-Library and NATO's "Speeches & transcripts" database. The official texts provide insights into NATO policies and reasoning concerning cybersecurity governance. They include: official statements, declarations, communiqués by the North Atlantic Council (NAC), ministerial meetings and summits, as well as various (committee) proposals, programmes and action plans. The analysis specifically focussed on the 41 documents dealing with "cyber". Not only do these sources provide first-hand information about NATO policies concerning cybersecurity, they can also be seen as statements by the militarising actor (NATO leadership) and therefore provide insights in any potential speech acts by the militarising actor.

Other statements by (potential) NATO militarising actors are drawn from NATO's "Speeches & transcripts" database. This database includes transcripts of speeches or press conferences by high level NATO officials. A search query, covering the 2002-2014 period, provided 271 transcripts dealing with "cyber". These are the transcripts that were analysed in this study.

The findings from the document analysis were intended to be triangulated with findings from semi-structured interviews, planned to be conducted as part of this study, in order to increase its internal validity. This type of interview is useful to direct the interviewee to the topics of NATO, cyberwarfare, cybersecurity, hybrid warfare and Stuxnet, while maintaining the possibility to expand upon a certain topic and thereby allowing the researcher to gain more insight into the variables involved (Bryman, 2012, pp. 469-471). The interviews were proposed to be conducted at the NATO Communications and Information Agency's (NCI) Directorate of Infrastructure Services, which is the directorate in charge of cybersecurity, as well as with IT professionals at the NCI Agency in general. Other requests for (online) interviews were send to NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and to a cyber defence policy expert at the Emerging Security Challenges division of the NATO Headquarters. Furthermore, in order to gain an understanding of member state input concerning these issues, interviews were requested to be conducted at the Directorate-General of Political Affairs (DGPZ) and at the "Cyber Cluster" of the Directorate of Security Policy (DVB), both at the Dutch Ministry of Foreign Affairs.

Unfortunately, due to lack of response to interview requests or due to denial of interview requests, the intended interviews have not taken place. The implications this has for this study's results are discussed in the Conclusion chapter.

When needed for clarification, to provide additional data, or to further increase internal validity by triangulation, the findings in this study are complemented by findings from secondary (peer-reviewed) sources.

Data Analysis

In this chapter, the findings of the process-tracing analysis are discussed in two sections. The first section of the analysis addresses the findings concerning the IV and the militarisation

process. The second section addresses de findings concerning the DV and the CV. As no interviews have been conducted, all findings are based upon the analysis of primary source documents. Any remaining data or clarifications from secondary sources are discussed when deemed necessary. A tabular summary of the findings is provided in the annex.

Militarisation and the Independent Variable

The earliest mentions related to cybersecurity in official NATO publications are found in the period 2002-2006. What is interesting about these mentions is their framing in militaristic terms such as "defend against cyber attacks" (NATO, 2002, p. 3). Such a frame is unsurprising, as NATO was targeted by cyberattacks as part of the Kosovo War in 1999 (Burton, 2015, p. 305). However, while referent objects are clearly mentioned in the documents from this period, for example: "information systems of critical importance" (NATO, 2006, p. 4), no real existential threat to the alliance and/or its member states is mentioned. It is therefore safe to conclude that cybersecurity was not a securitised or militarised issue in the period before 2006, at least not according to Copenhagen School criteria, which require the framing of an issue as an existential threat.

This situation changed drastically after the 2007 Estonian cyberattacks: "In light of recent cyber attacks on one Ally's electronic infrastructure, urgent work is needed to enhance the ability to protect information systems of critical importance to the Alliance against cyber attacks" (NATO, 2007, p. 4). Judging from this quote, the Estonian cyberattacks seemed to have provided a changed objective contextual situation, such as required for securitisation or militarisation to occur according to the Copenhagen School. The importance of this changed contextual situation is illustrated by the various references to the Estonian cyberattacks by the NATO leadership throughout the years, for example: De Hoop Scheffer (2007, September 5;

2008, March 15), Rasmussen (2009, October 22; 2013, September 19) and NATO (2012f, p. 10).

However, for securitisation or militarisation to occur a changed contextual situation is not enough. The issue of cybersecurity would have to be framed as an existential threat to the alliance and/or its member states. Such framing has happened repeatedly, for example when Secretary-General Jaap de Hoop Scheffer warned that cyberattacks can bring down a country (De Hoop Scheffer, 2007, December 13), or when cyberattacks were described by Secretary-General Anders Fogh Rasmussen as "threats to the security of our nations" (Rasmussen, 2010, 22 April). Furthermore, the 2010 NATO Strategic Concept lists cyberattacks as threats to "national and Euro-Atlantic prosperity, security and stability" (NATO, 2010a). Thus, it can be concluded that NATO frames cybersecurity issues as existential threats.

In order for securitisation to occur, a call for extraordinary measures is required to deal with this existential threat. Furthermore, in order for the issue to be militarised, it is critical that the issues are presented as military issues requiring the involvement of actors from the military security sector. The primary source documents show that both these requirements have actually occurred. For example, one of these extraordinary measures, set forth in NATO's Policy on Cyber Defence, is the provision of a counter attack capability (NATO, 2008, p. 11). Another example is found in the recommendation that cyberattacks should be able to trigger Article 5 of the North Atlantic Treaty[5] if so determined by the NAC (NATO, 2010c, p. 12). This scenario, of cyberattacks triggering Article 5, was later described as a possible real scenario by Secretary-General Rasmussen (as cited in NATO, 2010, October 11).

Most NATO primary source documents show a distinctive military frame concerning cybersecurity topics. Such a frame favours the involvement of the military security sector and

[5] Article 5 is the article with the most far reaching implications of NATO's founding treaty. It describes NATO's collective defence by prescribing that an attack against one ally should be considered an attack against all allies (NATO, 1949).

thereby benefits militarisation instead of "regular" securitisation. For example, when discussing the challenges faced by NATO, cyberattacks are often mentioned in conjunction with distinctively military issues such as ballistic missile attacks, see for example: Albright (2014, May 17), Rasmussen (2011, February 9; 2014, February 26) and Vershbow (2013, June 24). There is also the description of cybersecurity issues themselves, NATO usually employs a distinctive military language when discussing these issues. For example, cyberspace has been described as a "peacetime battleground" (De Hoop Scheffer, 2009, October 9) and cyberattacks are described as instances of information and electronic warfare (De Hoop Scheffer, 2008, March 15), which are recommended to be dealt with according to the military "rules of engagement" (NATO, 2010c, p. 23). A recommendation that was further expanded upon when NATO tried to integrate cyberwarfare into the international legal framework concerning war, by publishing the Tallinn Manual on the International Law Applicable to Cyberwarfare in 2013 (Lobato & Kenkel, 2015, p. 25; Nocetti, 2015, p. 127).

Furthermore, as described in the Theoretical Framework chapter, NATO is theorised to have framed cybersecurity issues as instances of hybrid warfare. While no direct explicit references to hybrid warfare are found in the primary source documents, many implicit references conforming to Hofmann's definition of an "operational fusion of conventional and irregular capabilities" (Hofmann, 2009, p. 36) are found in the primary sources. For example: when responding to a question about cyber warfare, Secretary-General Rasmussen answers by connecting "cyber security" and "asymmetric warfare" (Rasmussen, 2012, July 4). Furthermore, NATO describes cyberattacks as a military type of unconventional threat (NATO, 2010c, pp. 4-5) and states that modern conflicts include a distinctive "cyber dimension" (NATO, 2010b, pp. 10-11). NATO also specifically recommends integration of "cyber defence capacities" into NATO's conventional forces (NATO, 2012c, pp. 3-4),

evidencing Hofmann's "operational fusion of conventional and irregular capabilities" (2009, p. 36).

Concerning the IV, based on these findings, it can be concluded that NATO has indeed militarised cybersecurity issues by framing them as possible instances of hybrid warfare, and by describing them as military existential threats to the alliance and/or its member states.

The Dependent and Condition Variables

When it comes to the DV, NATO's involvement in cybersecurity governance, plenty of evidence for increased involvement is found in the primary source documents. This increase of involvement, did indeed as expected, occur after a changed contextual situation (CV). However, contrary to what was expected and described in the Theoretical Framework and Methodology chapters, this changed contextual situation did not occur after the Stuxnet demonstration. In fact, no reference to Stuxnet or evidence of increased NATO involvement after the Stuxnet event has been found in the primary source documents. Instead it were the 2007 Estonian cyberattacks that can be considered to have provided the changed contextual situation. The implications this has for the CV and for the model in general, are further discussed in the next chapter.

In the period before 2007, NATO's involvement in cybersecurity governance was very limited (Fidler, Pregent & Vandurme, 2016, p. 5). Apart from limited actions, such as organising a workshop on cybersecurity in 2003 (NATO, 2004, p. 6), very few concrete actions, recommendations or policy statements are found in the primary sources.

After the 2007 cyberattacks this changed rapidly. The Defence Ministers session of the NAC noted that: "In light of recent cyber attacks on one Ally's electronic infrastructure, urgent work is needed to enhance the ability to protect information systems of critical importance to the Alliance against cyber attacks" (NATO, 2007, p. 4). This "urgent work"

involved the adoption of the Policy on Cyber Defence, which led to the creation of a NATO Cyber Defence Management Authority (CDMA), improvement of the Computer Incident Response Capability (NCRIC) and the activation of the CCDCOE (NATO, 2009, p. 11) and even included a counter attack capability (NATO, 2008, 11). It is interesting to note that the activation of the CCDCOE has been specifically described by some authors as a reaction to the 2007 Estonian events (Choucri, Madnick & Ferwerda, 2014, p. 110). Furthermore, expansion of cybersecurity cooperation between NATO and partner states was announced (NATO, 2009, p. 11), for example with: Ukraine (NATO10, 2008, p. 3), Georgia (NATO, 2011, p. 1), Russia (NATO, 2012e, p. 2), New Zealand (NATO, 2012d, p. 1), Australia (NATO, 2012a, p. 1) and Japan (NATO, 2013a, p. 3). The adoption of the Policy on Cyber Defence was further accelerated after the Strasbourg/Kehl summit in 2009 in order to "achieve full readiness" (NATO, 2009, p. 11).

Beyond the Policy on Cyber Defence, NATO also worked on integrating cyber defence into its new Strategic Concept. This Strategic Concept was for a large part based on expert recommendations listed in the "NATO 2020" report (NATO, 2010c). Apart from the aforementioned recommendation to redefine cyber threats as potential Article 5 triggers, a list of practical recommendations enhancing cyber defence capabilities, such as the creation of early warning systems and the formation of expert teams, is provided (NATO, 2010c, pp. 30-32). What stands out is the recommendation to expand NATO's "definition of mission" to include "cyber security" (NATO, 2010c, p. 22). These recommendations were largely adopted at the Lisbon summit as part of the new Strategic Concept (NATO, 2010a). During this summit, the promise was added to accelerate the NCRIC to "Full Operational Capability" by 2012 and to create an updated Policy on Cyber Defence and accompanying action plan by June 2011 (NATO, 2010b, pp. 10-11). The announced action plan was launched in October 2011 (NATO, 2013b, p. 19).

At the Chicago summit in May 2012, the Lisbon reforms were described as being implemented or on track to be implemented (NATO, 2012b, p. 12; NATO, 2012g, p. 2). During this summit, the Deterrence and Defence Posture Review was also adopted, which called for further development of cyber defence capabilities and their integration into "Allied structures and procedures" (NATO, 2012c, p. 4). Further investments include a €58 million contract with "a consortium of private companies to significantly upgrade its [NATO's] unique operational cyber defence capability" (NATO, 2013b, p. 19) and a project to centralise protection of NATO networks by autumn 2013 (NATO, 2013b, p. 19). In order to further improve its cyber defence capability, NATO established a "cyber threat assessment cell" and annually holds an exercise called Cyber Coalition (NATO, 2013b, p. 20). Continuing this process, NATO's Strategic Allied Commander of Transformation, General Paloméros, announced a focus on "cyber" in NATO's transformation in order to "adapt itself to the environment" (Paloméros, 2014, January 23).

Judging from these findings and concerning the DV, it can be safely concluded that NATO's involvement in cybersecurity governance increased significantly after 2007. As deliberate (policy) statements of NATO action or inaction in the field of cybersecurity were continuously made after 2007. Concerning de CV, a changed objective context was also identified from these sources. However, this changed context was not provided by the 2010 Stuxnet event as expected, but instead by the 2007 Estonian cyberattacks.

Conclusion

Discussion of Results

Albeit some limitations, which will be addressed in the next section, the results provide a relatively clear picture concerning the DV, IV and the CV. These variables are based on a Copenhagen School style model of militarisation applied to the NATO cybersecurity case.

Securitisation, according to this school, occurs when a securitising actor describes something as an existential threat to a referent object, by means of a speech act. In order for militarisation to occur, the actors involved would have to be from the military security sector. Their involvement can be triggered by defining the existential threat as a military threat. This military existential threat was expected to be found in the defining of cybersecurity issues as means of hybrid warfare. The results of the analysis show that NATO has indeed employed such a frame. Therefore, it can be concluded that concerning the IV, NATO has indeed framed cybersecurity issues as means of hybrid warfare.

According to the Copenhagen school, securitisation and militarisation require exceptional (political) measures. This was also included in the model of this study, in the form of an expected increased involvement of NATO in the governance of cybersecurity issues. This could be considered exceptional because NATO is mostly a military organisation and cybersecurity issues have a clear civilian component as well. Therefore, they do not warrant the involvement of military IGOs per se. The findings concerning the DV however, speak in favour of this study's expectations. NATO has become increasingly involved in cybersecurity governance and has integrated cybersecurity into its structure in such a way that it can be considered a core task of the alliance.

Contrary to some more "radical" branches of social constructivism, the Copenhagen School does require an objectively changed contextual situation in order for securitisation or militarisation to occur. This prerequisite condition, defined in this study as the CV, was expected to have been fulfilled by the demonstration of a cyberweapon in the form of the Stuxnet worm.

The data, however, show a different event which provided the changed objective context, in the form of the 2007 Estonian cyberattacks. Fortunately, this does not compromise the suitability of the model in providing an explanation for NATO's increased involvement in

cybersecurity governance, as there is still a changed objective context, albeit not the one initially expected in this study. What this alternative context shows, is that even ambiguous cases, such as the Estonian cyberattacks can serve as the required changed objective context. The degree as to how "ambiguous" objective contexts can serve as this prerequisite for securitisation or militarisation is an avenue that requires further research.

All of these findings speak in favour of a Copenhagen School style militarisation process concerning cybersecurity issues, leading to increased NATO involvement in cybersecurity governance. Thus, the findings do fit this study's hypothesis.

Limitations

In order to make this study's research manageable and feasible, this study has used a black box approach when it comes to NATO. In reality NATO is not a single monolithic organisation, but is made up of various different member states and involves an array of different types of actors and organisational structures and procedures, all of which may have influenced NATO's decision and policy making process. This black box approach extended to the NATO leadership which was treated as a single militarising actor, whereas in reality there may or may not be differences of views and opinions within the NATO leadership. However, in the future it can be interesting to investigate how an organisation's internal structures influence the frames it uses. Is the military frame a logical outcome option for a military organisation, or is it, for example, a product of internal politicking? This question therefore provides another possible avenue for further research.

Another limitation is found in the timeframe of the study itself. While the post-2014 period was deliberately avoided, in order to mitigate the influence of other geo-political variables influencing NATO politics, other variables may still have interfered during the selected timeframe. For example, as internet usage has rapidly expanded worldwide in the

past decades, it is not unthinkable that the growth of the internet and computer usage have helped to make cybersecurity a NATO priority as well. Unfortunately, as the growth of the internet coincided with the rise of cybersecurity it was not possible to mitigate this variable as well.

The final limitation of this study is found in its lack of triangulation. Because the intended interviews could not be conducted, the analysis had to be based solely on document analysis. Unfortunately, this has compromised the validity of the findings to some degree. However, due to the strong and clear results of the document analysis, combined with the secondary academic sources, it is still possible to draw conclusions from the findings.

Implications

The research question stated: *What explains the increased involvement of NATO, a military alliance, in the governance of cybersecurity, a non-traditional security issue?* This study found that it was, conform the hypothesis, the militarisation of cybersecurity issues that facilitated NATO's increased involvement.

This has implications for other NTSIs as well, such as global terrorism. As the cybersecurity case shows, the military aspect of such an issue can be used to frame them as military issues, thereby making them the concern of military security sector actors. This implication speaks in favour of functional differentiation, such as described by some Copenhagen School theorists (Albert & Buzan, 2011). As the specific frame employed by NATO was one of hybrid warfare, for future research it could be interesting to investigate what other frames a militarising actor can employ in order to militarise an NTSI.

Concerning the three criteria of an NTSI by Hameiri & Jones (2015), the findings show little to no effect on NATO involvement because of a change in potentiality-status by demonstration of a threat. In this case the demonstration of cyberwarfare by Stuxnet. Whether

this lack of findings was due to a wrongful focus on Stuxnet, or because of bias due the sole reliance on primary source documents published by NATO, is not clear.

Finally, the findings concerning the changed objective context speak in favour of its requirement as a prerequisite condition for securitisation or militarisation to occur, just as the Copenhagen School's model of securitisation suggests.

Bibliography

Abbott, K.W. & Snidal, D. (1998). Why States Act through Formal International Organizations. *Journal of Conflict Resolution, 42*(1), 3-32.

Ahmed, N.M. (2011). The International Relations of Crisis and the Crisis of International Relations: From the Securitisation of Scarcity to Militarisation of Society. *Global Change, Peace & Security, 23*(3), 335-355.

Albert, M. & Buzan, B. (2011). Securitization, Sectors and Functional Differentiation. *Security Dialogue, 42*(4-5), 413-425.

Albright, M.K. (2010, May 17). *Remarks: Of Madeleine K. Albright at the Meeting of the North Atlantic Council with the Group of Experts on NATO's New Strategic Concept* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_63678.htm?selectedLocale=en

Bryman, A. (2012). *Social Research Methods.* Oxford: Oxford University Press.

Burton, J. (2015). NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation. *Defence Studies, 15*(4), 297-319.

Buzan, B., Wæver, O. & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Buzan, B. & Hansen, L. (2009). *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Department of Defense. (2005). *The National Defense Strategy of The United States of America.* Retrieved from: archive.defense.gov/news/Mar2005/d20050318nds1.pdf

Dunn Cavelty, M. (2010). Cyber-threats. In M. Dunn Cavelty & V. Mauer (eds.), *The Routledge Handbook of Security Studies* (pp. 180-189). London: Routledge.

Choucri, N., Madnick, S. & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development, 20*(2), 96-121.

Colarik, A. & Janczewski, L. (2012). Establishing Cyber Warfare Doctrine. *Journal of Strategic Security, 5*(1), 31-48.

Connell, M. & Vogler, S. (2017). *Russia's Approach to Cyber Warfare.* Arlington: Center for Naval Analyses.

Fidler, D.P., Pregent, R. & Vandurme, A. (2016). NATO, Cyber Defense, and International Law, *Journal of International and Comparative Law, 4*(1), 1-25.

Finnemore, M. & Hollis, D.B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law, 110*(3), 425-479.

Graham, S. (2012). When Life Itself is War: On the Urbanization of Military and Security Doctrine. *International Journal of Urban and Regional Research, 36*(1), 136-155.

Hameiri, S. & Jones, L. (2015). *Governing Borderless Threats: Non-Traditional Security and the Politics of State Transformation.* Cambridge: Cambridge University Press.

Held D. (1997). Democracy and Globalization. *Global Governance, 3*(3), 251-267.

Hoffman, F.G. (2009). *Hybrid Warfare and Challenges*. Washington D.C.: National Defense University.

Hoop Scheffer, J.G. de. (2007, September 5). *Today's NATO, and Why It Matters: Speech by NATO Secretary General Jaap de Hoop Scheffer Lloyd's City Dinner* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_8471.htm?selectedLocale=en

Hoop Scheffer, J.G. de. (2007, October 9). *Speech: By NATO Secretary General, Jaap de Hoop Scheffer at the NATO Parliamentary Assembly's Annual Session, Reykjavik, Iceland* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_8511.htm?selectedLocale=en

Hoop Scheffer, J.G. de. (2007, December 13). *Meeting the Security Challenges of Globalisation: by the NATO Secretary General, Jaap de Hoop Scheffer* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_9636.htm?selectedLocale=en

Hoop Scheffer, J.G. de. (2008, March 15). *Beyond the Bucharest Summit: Speech by NATO Secretary General, Jaap de Hoop Scheffer, at the Brussels Forum of the George Marshall Fund (GMF)* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_7566.htm?selectedLocale=en

Karns. M.P. & Mingst, K.A. (2010). *International Organizations: The Politics and Processes of Global Governance.* Boulder: Lynne Rienner.

Keohane, R.O. & Martin, L.L. (1995). The Promise of Institutionalist Theory. *International Security, 20*(1), 39-51.

Krahmann, E. (2005). Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security. *Cambridge Review of International Affairs. 18*(1), 15-30.

Kroenig, M. (2015). Facing Reality: Getting NATO Ready for a New Cold War. *Survival, 57*(1), 49-70l.

Langer, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy, 9*(3), 49-51.

Lausten, C. & Wæver, O. (2000). In Defence of Religion: Sacred Referent Objects for Securitization. *Millenium, 29*(3). 705-739.

Liff, A.P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities as Interstate War. *Journal of Strategic Studies, 35*(3), 401-428.

Lobato, L.C. & Kenkel, K.M. (2015). Discourses of Cyberspace Securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional, 58*(2), 23-43.

Lindsay, J.R. (2013). Stuxnet and the Limits of Cyber Warfare, *Security Studies, 22*(3), 365-404.

Mayer, P. (2008). Civil Society Participation in International Security Organizations: The Cases of NATO and the OSCE. In J. Steffek, C. Kissling & P. Nanz (eds.), *Civil Society Participation in European and Global Governance: A Cure for the Democratic Deficit?* (pp. 116-139). New York: Palgrave Macmillan.

Mearsheimer, J.J. (1994). The False Promise of International Institutions. *International Security, 19*(3), 5-49.

Mearsheimer, J.J. (2014). *The Tragedy of Great Power Politics.* New York: W.W. Norton.

Nance, M.T. & Cottrell, M.P. (2014). A Turn Toward Experimentalism? Rethinking Security and Governance in the Twenty-First Century. *Review of International Studies, 40*(2), 277-301.

NATO. (1949). *The North Atlantic Treaty.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_17120.htm

NATO. (2002). *Prague Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Prague, Czech Republic.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_19552.htm?selectedLocale=en

NATO. (2004). *Action Plan 2004-2005: Of the Euro-Atlantic Partnership Council (EAPC).* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_21029.htm?selectedLocale=en

NATO. (2006). *Comprehensive Political Guidance: Endorsed by NATO Heads of State and Government on 29 November 2006*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_56425.htm?selectedLocale=en

NATO. (2007). *Final Communiqué: Meeting of the North Atlantic Council in Defence Ministers Session.* Retrieved from: https://www.nato.int/cps/en/natohq/news_47011.htm?selectedLocale=en

NATO. (2008). *Bucharest Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Bucharest on 3 April 2008*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_8443.htm?selectedLocale=en

NATO. (2009). *Strasbourg / Kehl Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Strasbourg / Kehl.* Retrieved from: https://www.nato.int/cps/en/natohq/news_52837.htm?selectedLocale=en

NATO. (2010a). *Active Engagement, Modern Defence: Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120203_strategic-concept-2010-eng.pdf

NATO. (2010b). *Lisbon Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Lisbon.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_68828.htm?selectedLocale=e

NATO. (2010c). *NATO 2020: Assured Security; Dynamic Engagement: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_63654.htm?selectedLocale=en

NATO. (2010, October 11). *Monthly Press Briefing: By NATO Secretary General Anders Fogh Rasmussen* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_66734.htm?selectedLocale=en

NATO. (2011). *Joint Statement: At the Meeting of the NATO-Georgia Commission at the Level of Foreign Ministers in Berlin, Germany*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_72697.htm?selectedLocale=en

NATO. (2012a). *Australia-NATO Joint Political Declaration.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_94097.htm?selectedLocale=en

NATO. (2012b). *Chicago Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Chicago on 20 May 2012.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO. (2012c). *Deterrence and Defence Posture Review.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_87597.htm?selectedLocale=en

NATO. (2012d). *Individual Parternship and Cooperation Programme between New Zealand and NATO.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_88720.htm?selectedLocale=en

NATO. (2012e). *Meeting of the NATO-Russia Council at the Level of Foreign Ministers held in Brussels on 19 April 2012: Chairman's Statement*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_86211.htm?selectedLocale=en

NATO. (2012f). *Secretary General's Annual Report 2011*. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_82646.htm?selectedLocale=en

NATO. (2012g). *Summit Declaration on Defence Capabilities: Toward NATO Forces 2020*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_87594.htm?selectedLocale=en

NATO. (2013a). *Joint Political Declaration between Japan and the North Atlantic Treaty Organisation.* Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_99562.htm?selectedLocale=en

NATO. (2013b). *Secretary General's Annual Report 2012.* Retrieved from: https://www.nato.int/cps/en/natohq/opinions_94220.htm?selectedLocale=en

NATO. (2018, February 19). *Cyber Defence.* Retrieved from: https://www.nato.int/cps/en/natohq/topics_78170.htm

Nocetti, J. (2015). Contest and Conquest: Russia and Global Internet Governance. *International Affairs, 91*(1), 111-130.

Paloméros, J.P. (2014, January 23). *Opening Statement by the Supreme Allied Commander Transformation: General Jean-Paul Paloméros, at the Joint Press Point Following the 170th NATO Chiefs of Defence Meeting* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_106455.htm?selectedLocale=en

Peoples, C. & Vaughan-Williams, N. (2015). *Critical Security Studies: An Introduction.* Abingdon: Routledge.

Radu, R.G. (2012). The Monopoly of Violence in the Cyber Space: Challenges of Cyber Security. In E. Fels, J.F. Kremer & K. Kronenberg (eds.), *Power in the 21st Century: International Security and International Political Economy in a Changing World* (pp. 137-150). Heidelberg: Springer.

Rasmussen, A.F. (2009, October 22). *New Challenges – Better Capabilities: Speech by NATO Secretary General Anders Fogh Rasmussen at the Bratislava Security Conference* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_58248.htm?selectedLocale=en

Rasmussen, A.F. (2010, 22 April). *On Alliance Solidarity in the 21st Century: Speech by NATO Secretary General Anders Fogh Rasmussen – Tallinn, Estonia* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_62699.htm?selectedLocale=en

Rasmussen, A.F. (2011, February 9). *Speech: By NATO Secretary General Anders Fogh Rasmussen at the 11th Herzliya Conference in Herzliya, Israel* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_70537.htm?selectedLocale=en

Rasmussen, A.F. (2012, July 4). *NATO – Delivering Security in the 21st Century: Speech by NATO Secretary General Anders Fogh Rasmussen, Chatham House, London* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_88886.htm?selectedLocale=en

Rasmussen, A.F. (2013, September 19). *NATO: Ready, Robust, Rebalanced: Speech by NATO Secretary General Anders Fogh Rasmussen at the Carnegie Europe Event* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_103231.htm?selectedLocale=en

Rasmussen, A.F. (2014, February 26). *Opening Remarks by NATO Secretary General Anders Fogh Rasmussen* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_107406.htm?selectedLocale=en

Ruggie, J.G. (1995). The False Premise of Realism. *International Security, 20*(1), 62-70.

Simpson, E. (2012). *War from the Ground Up: Twenty-First-Century Combat as Politics*. Oxford: Oxford University Press.

Schlag, G. (2016). Securitisation Theory and the Evolution of NATO. In M. Webber & A. Hyde-Price (eds.), *Theorising NATO: New Perspectives on the Atlantic Alliance* (pp. 161-182). Abingdon: Routledge.

Smith, R. (2005). *The Utility of Force: The Art of War in the Modern World*. London: Allen Lane.

Vershbow, A.R. (2013, June 24). *Address by Ambassador Alexander Vershbow NATO Deputy Secretary General at the 30th International Workshop on Global Security, Hôtel National des Invalides – Paris France, 24 June 2013* [transcript]. Retrieved from: https://www.nato.int/cps/en/natohq/opinions_101606.htm?selectedLocale=en

Versluis E., Keulen, M. van & Stephenson, P. (2011). Doing EU Policy Analysis. In E. Versluis, M. van Keulen & P. Stephenson (eds.), *Analyzing the European Union Policy Process* (pp. 11-30). Basingstoke: Palgrave Macmillan.

Watson. S.D. (2012). 'Framing' the Copenhagen School: Integrating the Literature on Threat Construction. *Millenium, 40*(2), 279-301.

Wendt, A. (1992). Anarchy is What States Make of It: The Social Construction of Power Politics. *International Organization, 46*(2), 391-425.

Williams, M.C. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly, 47*(4), 511-531.

Annex

Table 1. *Summary of Findings.*

Variable	Findings
IV: NATO's framing of cybersecurity issues.	Militaristic frame; cybersecurity issues framed as means of hybrid warfare: • Cybersecurity issues framed as existential threats. • Extraordinary measures required. - Counter attack capability. - Article 5 trigger.
DV: NATO's involvement in cybersecurity governance.	Very limited involvement from 2002 to 2007. Much higher level of involvement after 2007. 2002-2007: • Few concrete actions. 2007-2014: • Creation and expansion of CDMA, NCRIC, CCDCOE. • Cooperation with extra-NATO partners. • Expansion of NATO mission definition. • Integration of cyber defence in NATO military structures. • (Financial) investments in cyber defence capabilities.
CV: Changed objective context of cybersecurity issues.	Yes: • 2007 Estonian cyberattacks. • No evidence of Stuxnet effect.