FFI-rapport 2014/01328

Norway, NATO and cyber defense

Siw Tynes Johnsen

FFI Forsvarets forskningsinstitutt

Norway, NATO and cyber defense

Siw Tynes Johnsen

Norwegian Defence Research Establishment (FFI)

10 July 2014

FFI-rapport 2014/01328

Prosjekt 3919

P: ISBN 978-82-464-2412-5
E: ISBN 978-82-464-2413-2

Keywords

Cyberforsvar

Cyber

Nato

Approved by

Frode Rutledal	Project Manager
Espen Skjelland	Director

English summary

NATO is the cornerstone of Norwegian security policy, and has in recent years intensified its efforts relating to the cyber domain. Cyber defense has gained increased attention in Norway as well, and the Norwegian Armed Forces have been tasked with contributing to NATO's efforts in countering cyber attacks. This report explores the challenges and opportunities for Norway, as a small state in NATO, in dealing with the cyber domain.

Perhaps the most important finding is that cyber related challenges do not necessarily need to be treated as something completely different from other challenges that are dealt with within the NATO framework. While the cyber domain in itself might be a domain *sui generis*, the challenges and opportunities for a small state are far from fundamentally different from other areas.

Norway is, as a small state, completely dependent on its allies in NATO for collective defense in case of attack. It should therefore make efforts towards keeping NATO relevant, also in a post-ISAF environment, by integrating emerging challenges such as cyber defense into the alliance realm. The United States has voiced increased concern with the lack of burden sharing in the alliance, and one can imagine that Norway could gain increased influence in NATO by shouldering a larger share of the cyber defense burden than what is expected from a small state. Further, Norway should aim to build fruitful relationships with other allies, promoting shared interests such as collective defense and burden-sharing, also when considering cyber defense. It is also in Norway's vested interest to be seen as a state which takes threats in the cyber domain seriously, and can provide secure and resilient systems. This should be promoted in NATO fora, and showcased in exercises and operations. Finally, the participation in cyber defense exercises and interoperability initiatives can benefit Norway both nationally and as an ally, as it will help enable effective and successful cooperation when deployed.

In conclusion, the report arrives at the following recommendations for Norwegian policy on NATO and cyber defense:

- Keep NATO relevant by integrating cyber defense in the work of the alliance
- Share the burden through increased engagement in cyber defense
- Be constructive and forge relationships to influence decision-making on cyber defense
- Secure own systems and demonstrate resilience
- Participate in exercises and interoperability initiatives on cyber defense

Sammendrag

Nato er selve hjørnesteinen i norsk sikkerhetspolitikk, og har i løpet av de siste årene intensivert sin aktivitet knyttet til cyberdomenet. Cyberforsvar har fått økt oppmerksomhet også i Norge, og det norske Forsvaret har fått i oppgave å støtte Nato i alliansens arbeid med cyberforsvar. Denne rapporten utforsker utfordringene og mulighetene for Norge som småstat i Nato, innenfor cyberdomenet.

Rapportens kanskje viktigste funn er at det ikke er nødvendig å behandle cyberrelaterte utfordringer som noe fullstendig annerledes enn de andre utfordringene som håndteres i Nato. Mens cyberdomenet i seg selv er et domene *sui generis*, er mulighetene og utfordringene for en småstat langt fra fundamentalt ulike de man møter på andre områder.

Norge er som småstat fullstendig avhengig av allierte i Nato for kollektivt selvforsvar om man skulle bli angrepet. Man bør derfor arbeide for å opprettholde Natos relevans, også i tiden post-ISAF, ved å integrere nyere utfordringer som cyberforsvar i alliansesfæren. USA har ytret økt bekymring for mangel på deling av byrdene i alliansen, og det kan tenkes at Norge kan oppnå økt innflytelse i Nato ved å bære en større del av cyberforsvarsbyrden enn det som forventes av en småstat. Videre bør Norge søke å bygge gode forhold til andre allierte, ved å promotere felles interesser som kollektivt selvforsvar og deling av byrdene også når det gjelder cyberforsvar. Det er også i Norges interesse å bli sett på som en stat som tar trusler i cyberdomenet på alvor og kan vise til sikre og robuste systemer. Dette bør promoteres i Nato-fora, og vises frem på øvelser og i operasjoner. Det vil være fordelaktig både nasjonalt og som en del av alliansen om Norge deltar aktivt i Natos cyberøvelser og interoperabilitetsinitiativer, for å kunne yte og samarbeide bedre når det gjelder.

Rapportens konklusjon fremhever de følgende anbefalingene for norsk policy for Nato og cyberforsvar:

- Sikre Natos relevans gjennom integrering av cyberforsvar i alliansens arbeid
- Del byrdene gjennom økt satsing på cyberforsvar
- Vær konstruktiv og utvikle forhold for å påvirke beslutninger om cyberforsvar
- Sikre egne systemer og vis at de er robuste
- Delta i øvelser og interoperabilitetsinitiativer for cyberforsvar

Contents

1 Introduction

> 'We are all closely connected, so an attack on one ally, if it is not dealt with quickly and effectively, can affect us all. Cyber defense is only as effective as the weakest link in the chain. By working together we strengthen the chain.'
>
> – NATO Secretary General Anders Fogh Rasmussen[1]

States are becoming increasingly dependent on the cyber domain, a man-made domain where developments continue to take place at an extremely rapid pace. Cyberspace as a global commons serves as a vital part of international security, and transcends national borders by its nature and design. This represents a range of new challenges, which need to be addressed in a multinational manner.

NATO has in recent years intensified its efforts relating to the cyber domain. Its division for Emerging Security Challenges has cyberspace as one of its main focus areas, and the organization has stated in its Cyber Defense Policy that in order to perform its 'core tasks of collective defense and crisis management, the integrity and continuous functioning of its information systems must be guaranteed' (NATO 2011).

This report will explore the challenges and opportunities for Norway, as a small state in NATO, in dealing with the emerging challenges related to cyberspace. Ensuring continued use and unhindered access to cyberspace, both in peacetime, crisis, and war, is of vital importance to both Norway and NATO. How can a small state such as Norway contribute to NATO's cyber defense activities? And how is Norway affected by the efforts made by its allies in NATO?

The Norwegian Defence Research Establishment (FFI) has through years of research developed an extensive body of knowledge on the small state perspective in international security and military operations.[2] This study seeks to apply this theoretical basis to the case of Norway and cyber defense efforts in NATO. The report will first explain some of the most relevant definitions, such as the cyber domain, cyber power, cyber operations, small states, and alliances (Chapter 2). Second, the report will look into NATO's activities and policies related to cyber defense (Chapter 3). The focus here will be the core elements of NATO, and how cyber defense affects these. The chapter will discuss NATO transformation efforts, organizational management structures, interoperability and exercises, Articles 4 and 5 of the North Atlantic Treaty, and burden sharing, all seen through the lens of cyber defense. Third will be an analysis of implications and consequences for Norway, given its national priorities and its small state status in the alliance (Chapter 4). Finally, a conclusion will summarize the findings of the report.

[1] Reuters (2013)

[2] See for example Kjølberg, Anders and Tore Nyhamar (2011), *Småstater i internasjonale operasjoner*, FFI-rapport 2011/01698 and Kjølberg, Anders (2007), *Livet i hegemonens skygge: en småstats sikkerhetslogikk*, FFI-rapport 2007/01626.

This report was written for the Norwegian Department of Defense, and the target audience is the policy-maker community. It is not a precondition that the reader is neither a NATO expert, nor a cyber one, and the report is focused on policy rather than purely technical issues.

2 Definitions

The *cyber domain* is defined as the physical and logical interconnection of information systems, including network devices, communications infrastructure, media, and data (Windvik and Diesen 2013). For the purpose of this report, the terms *cyber domain* and *cyberspace* will be used interchangeably.

In the cyber domain, actors wield *cyber power*: the ability to apply or project power in or through the cyber domain. This can be done for example through conducting military operations in or through the cyber domain, so-called *cyber operations* (Windvik and Diesen 2013).

Cyber operations are generally divided into *defensive cyber operations* and *offensive operations* (Windvik and Diesen 2013). This report will focus on defensive efforts in the cyber domain, especially since NATO is only given a defensive mandate by its member states when it comes to cyber operations.

There is no universally accepted definition of a *small state* within the social sciences; however, there are a wide range of definitions which take related, but different aspects into account. This report will make use of the work by Anders Kjølberg and Tore Nyhamar on small states and international security, exploring the topic with cyber defense in NATO in mind (Kjølberg and Nyhamar 2011; Kjølberg 2007).

Alan K. Henrikson defined in 2005 a *small country* as ‘one that cannot protect itself by its own efforts’. Assessing Norway by this definition, it is clear that Norway is a small country, which relies on its allies in NATO for collective defense in case of a major military attack. Ivan Arreguin-Toft defines the strength of a state by using the product of population and military might, which Kjølberg and Nyhamar (2011) built on when defining a *small state* as ‘a state with a low score compared to important international actors on four indicators of size: population, geographic extent, gross domestic product, and military capacity.’ Also by this more comprehensive definition, Norway easily falls under the small state category.

Erich Reiter and Heinz Gärtner (2001:2) define *alliances* as ‘formal associations of states bound by the mutual commitment to use military force against non-member states to defend member states’ integrity.’

3 NATO and Cyberspace

NATO was established in 1949, as 15 states signed the North Atlantic Treaty, and has since become the largest defense alliance in the world, currently comprised of 28 member nations. The Alliance is governed by the North Atlantic Council, which is led by the Secretary General and consists of representatives from all member states. All decisions made by the NAC are reached by consensus, as is the case for decisions made in the various committees where the member states are represented, including the highest military organ, the Military Committee (NATO 2012c).

There is no doubt that cyber challenges are high on the agenda for the NATO leadership, and that it will remain a focus area in the years to come. Secretary General Anders Fogh Rasmussen continuously highlights that the cyber domain becomes increasingly important for the security of the alliance, and that the member states have to focus on improving their cyber defense capabilities. Former SACEUR and head of the US European Command, Admiral James Stavridis, wrote in April 2013 that cyber security should be one of three focus areas for NATO in the coming years. He characterized the cyber domain as an environment where the threat is high and the level of preparedness is low, compared to the other areas within the alliance's purview (Kveberg and Johnsen 2014; NATO Allied Command Operations 2013).

3.1 NATO transformation efforts

Transformation is defined by NATO as 'A continuous and proactive process of developing and integrating innovative concepts, doctrines and capabilities in order to improve the effectiveness and interoperability of military forces' (NATO Standardisation Agency 2008). That includes defining capability requirements for the multinational operations of the future, as well as education and training to enable allies to implement future concepts and capabilities. In order to renew the alliance's relevance in the post-ISAF environment, transformation has perhaps been more central for NATO and its allies over the last few years than it has been for long. NATO's Allied Command Transformation (ACT) in Virginia, USA is led by the Supreme Allied Commander Transformation, and is responsible for NATO's transformation processes. ACT is following technological developments closely, with the aim of assessing how it influences NATO in the future. ACT's *Futures* studies emphasize that thus far, NATO allies have been more technologically advanced than their adversaries, however it is not a given that this advantage will persist if other nations increasingly focus on developing their cyber capabilities (Kveberg and Johnsen 2014).

While technically not a NATO institution, the NATO-accredited Collaborative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia, is also part of the transformation and futures-related work of the alliance. The centre works on doctrine and strategy for NATO, and aspires to develop further its expertise in the field of cooperative cyber defense (Cavelty 2011).

Norwegian Parliamentary Proposition 73 S (Prop 73 S) highlights NATO's ability to adapt to changing circumstances as one of the most important factors for why NATO is still relevant. To remain relevant post-ISAF, NATO must show that it is up to dealing with not only the challenges

of today, but also the challenges of tomorrow (Forsvarsdepartementet 2012a). There is no doubt that the cyber domain will become increasingly important, a development that NATO itself has emphasized on a number of occasions. At the Lisbon summit in 2010, NATO launched a new Strategic Concept for the alliance, where cyberspace received more attention than ever before. It is emphasized that allied security depends on the ability to protect NATO's ICT systems in the best possible way, as soon as possible (NATO 2013c).

For NATO, it has largely been cyber defense and increased resilience among allies which has been at the core, rather than offensive cyber capabilities, and the alliance has only been granted a defensive mandate by the member states. This does not entail that the cyber domain is seen as less of a challenge. Cyber defense has been declared a core capability of the alliance, to cope with the increasing level of threats in cyberspace (Kveberg and Johnsen 2014).

3.2 NATO and cyber defense

In June 2011, NATO adopted a revised Cyber Defense Policy, and made the first steps in defining the political and operational mechanisms that amount to NATO's response to cyber attacks. This policy integrated cyber defense into the defense planning process, along with other allied capabilities. The policy also describes, in broad strokes, how NATO can support allies in national cyber defense efforts upon request, for instance through optimizing information-sharing and situational awareness, cooperation, and interoperability (NATO 2013c). The Cyber Defense Policy and its accompanying Action Plan are described by the Atlantic Council as 'by far the most important steps the Alliance has taken so far to mature its cyber capabilities' (Healey and van Bochoven 2011:3). The NATO cyber defense management hierarchy is displayed in the figure below.

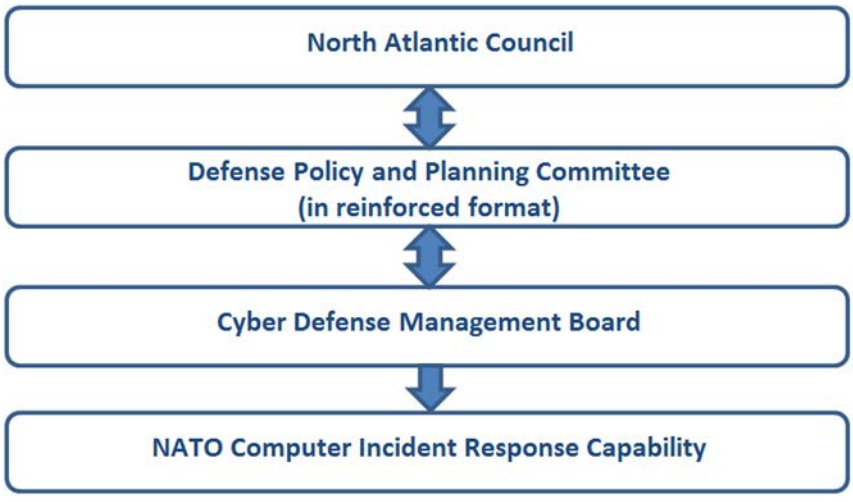

Figure 3.1 NATO Cyber Defense Management[3]

[3] This figure is based on one found in Healey and von Bochoven (2011).

The NATO defense planning process is led by the Defense Policy and Planning Committee (DPPC), where all member states are represented. It oversees the work of all planning bodies and committees on behalf of the North Atlantic Council. When dealing with cyber defense issues, the DPPC meets 'in reinforced format'. This means that the committee is chaired by the Deputy Secretary General, rather than an Assistant Secretary General, and that specific experts are brought in to support the committee's work.

The Cyber Defense Management Board (CDMB) is comprised of 'Leaders of NATO political military, operational, and technical staffs with responsibilities for cyber defense.' They are tasked with coordinating cyber defense efforts across the NATO system. The NATO International Staff is spread across seven divisions, that all have to take the cyber domain into account in one way or another, either with regard to defense planning, media and communications, or in NATO's operations abroad. There is, however, one division where the cyber domain is one of the main topics: the Emerging Security Challenges Division (ESC), which was established in 2010. Along with terrorism, weapons of mass destruction, and energy security, cyber defense is one of the division's core focus areas, and the CDMB operates under its auspices (Healey and van Bochoven 2011:3; NATO 2010c).

While the work in the ESC is focused around the work in the CDMB, the DPPC, and the political-military spectrum, another recent cyber development is on the more technical side. The NATO Computer Incident Response Capability (NCIRC) was established in the beginning of 2012, with the aim of reaching full operational capability within the end of the year. A Cyber Threat Awareness Cell was tasked with enabling sharing of information and improving situational awareness for the alliance. NCIRC is responsible for monitoring and protecting NATO's own networks, which is a comprehensive and complex task on its own (NATO 2013a).

Protecting NATO's own systems is the number one task for NATO when it comes to the cyber domain, according to Deputy Assistant Secretary General for the Emerging Security Challenges division, Dr. Jamie Shea. He highlights that while that might sound easy, 'it's not.' 'We now have well over 30 major networks, and we have just recently completed an upgrade of our NATO Computer Incident Response Capability, so that it can protect 24/7 55 critical NATO sites: NATO Headquarters, NATO Command Structure, et cetera.' He further highlights that as cyber threats are becoming increasingly sophisticated, NATO needs to constantly verify that it is able to protect its own systems; it has become a continuous effort (Young Professionals in Foreign Policy 2014).

Another major challenge for NATO is that its own internal systems are connected to a number of national systems, and these systems are becoming increasingly interdependent. In order to protect NATO systems, there is a need to do considerable mapping of where these systems connect, and which security regimes govern these national systems. This work is ongoing, as allies have been tasked with providing NATO an overview over these connections (Young Professionals in Foreign Policy 2014).

NATO is also looking at how they can support allies when needed, with assistance and advice when cyber incidents occur. The aim is to develop NATO into a more 'cohesive cyber community,' where all member states are at the same high level of cyber security and cyber defense. This is done for instance through conducting major cyber exercises with participants both from allies and partner nations, focusing both on technical and procedural issues (Young Professionals in Foreign Policy 2014).

3.3 Interoperability and exercises

NATO describes *interoperability* as 'the ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives. Specifically, it enables forces, units and/or systems to operate together and allows them to share common doctrine and procedures, each other's infrastructure and bases, and to be able to communicate. Interoperability reduces duplication, enables pooling of resources, and produces synergies among the 28 Allies, and whenever possible with partner countries' (NATO 2012a).

The Collaborative Cyber Defence Centre of Excellence supports NATOs efforts for increased interoperability in the cyber domain, and has as one of its main objectives to work for increased secure interoperability in the NNEC environment (NATO Network Enabled Capability). Norway is at present not a member of the center, which at 17 June 2014 has 14 NATO countries as sponsors (Collaborative Cyber Defence Centre of Excellence 2014). One can, however, not ignore that while interoperability is usually described in highly positive terms, it can also be quite expensive in practice (Aabakken 2002), which is an important factor to consider in the current financial climate.

In order to conduct coalition operations successfully, coalition partners need to practice and exercise together before the need to deploy coalition forces materializes. This also holds true for cyber defense. The NATO Crisis Management Exercise of 2012 was conducted in parallel with a separate cyber exercise, Cyber Coalition, a cyber exercise running for the fifth time. The aim was to practice NATO's procedures for dealing with cyber attacks against critical infrastructure (Kveberg and Johnsen 2014; Nasjonal Sikkerhetsmyndighet 2012).

That exercise was followed up by Cyber Coalition 2013, which focused on NATO's ability to defend its networks from cyber attacks. Coordination and cooperation between allies, partners, and NATO were at the core of the activities. Dr. Jamie Shea, from NATO's ESC division, stated that 'NATO has to keep pace with this evolving threat and Cyber Coalition 2013 will allow us to fully test our systems and procedures to effectively defend our networks – today and in the future.' Over 30 states were involved, counting over 300 cyber defense experts from both national and NATO stakeholder institutions (NATO 2013b).

3.4 Articles 4 and 5 of the North Atlantic Treaty

The North Atlantic Treaty (NATO, 1949)

Article 4: "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."

Article 5: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."

At the very core of NATO's *raison d'être* sit Articles 4 and 5 of the North Atlantic Treaty. Article 4 gives the right to consult with allies when a member state is threatened, and the Group of Experts which was assembled ahead of the alliance's new Strategic Concept recommended that NATO makes 'more creative and regular use of the consultations authorized' in the Treaty. It highlighted that this could prevent crises from escalating, and that such consultations are especially well-suited for use on 'unconventional dangers'. 'Article 4 provides an opportunity to share information, promote a convergence of views, avoid unpleasant surprises, and clear a path for successful action – whether that action is of a diplomatic, precautionary, remedial, or coercive nature,' it continued (NATO 2010b).

A fiercely debated topic within NATO has been whether a cyber attack could trigger Article 5, the article of the North Atlantic Treaty dealing with collective defense. Former Norwegian Defense Minister Espen Barth Eide stated that Norway's official position was that the cyber attack had to have impact on the physical world in order to fall under Article 5, describing a situation where 'the intrusion takes place via the computer system, but that the consequences impact life and health, or creates great destruction in the physical space' [author's translation]. He did however emphasize that NATO could become involved on the grounds of international law, as per normal (Teknisk Ukeblad 2012).

Several NATO officials have emphasized that whether or not a cyber attack could trigger an Article 5 response would very much depend on the context and the specific circumstances surrounding the attack. Secretary General Fogh Rasmussen elaborated on the process leading to an Article 5 decision during a 2010 press conference. An ally subject to cyber attack would likely

ask for consultations according to Article 4 first, which could then eventually 'lead to the conclusion that we need a common approach according to Article 5,' he explained (NATO 2010a). The Secretary General highlighted that it is the case with all attacks that there is not necessary a 'clear Article 5 case in advance.' The North Atlantic Council will decide on these issues once an attack has taken place, and this type of 'constructive ambiguity' gives the Council the necessary freedom of action. Fogh Rasmussen has explained that 'that's exactly the strength of Article 5, that potential aggressors never know when the Alliance will invoke Article 5,' while adding that 'a cyber attack might be at end of the day considered an Article 5' (NATO 2010a).

The previously mentioned Group of Experts came to the conclusion that 'a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5 (NATO 2010b). Suggesting that the issue is maturing in the alliance, Brooks Tigner from Jane's Defense quotes a senior NATO official on 22 October 2013, saying that 'as more and more allies experience cyber attacks, then clearly NATO also has to accept that collective defense solidarity assistance applies in the cyber realm as much as it applies to any other type of armed attack' (Jane's Defence 2013).

The question of attribution also comes into play in the Article 5 discussion. For NATO to be able to retaliate, Dr. Jamie Shea, from the ESC division, elaborates that the alliance 'would need a high degree of confidence that NATO can identify the source of the attack. In the meantime, countries suspected of launching cyber attacks can be put under a legal obligation to cooperate with an investigation on behalf of the victim. At that same time, Article 5 applies as much to NATO's willingness to assist one of its members to survive a cyber onslaught and recover quickly as to a retaliation or counter attack' (Atlantic Community 2011).

3.5 Burden sharing

Kjølberg (2007) points to the most important condition for NATO to continue to be an institution which will defend the security interest of smaller European countries: the United States needs to continue to view NATO as relevant, important, and useful.

The United States views cyberspace as a domain to be defended by the US military in the same way as the traditional domains of air, land, and sea. In the US International Strategy for Cyberspace the increased dependency on cyber assets is highlighted as a feature that can hardly be overestimated. The US also emphasizes that the continued access to cyberspace is critical for conducting military operations in the modern world. As cyberspace emerges as an increasingly contested domain, technologically advanced armed forces are becoming more vulnerable to adversary actions (United States Department of Defense 2012; White House 2011).

A typical divide in NATO between smaller and larger nations, is on the extent of NATO's role on specific issues. Smaller nations are likely to favor a bigger role for NATO than larger ones, as they do not possess the same capabilities and capacity. This holds true also for cyber defense, and Reuters refers to this divide by claiming that 'Smaller countries with limited resources are keen to take advantage of NATO's cyber defense capabilities and Rasmussen believes NATO should have

a capacity to help. But larger members, such as the United States, Britain, France and Germany, disagree. Since they spend large sums on cyber defense at home, they are reluctant to divert money to NATO activities that will largely benefit others' (Reuters 2013).

The United States has voiced increased concern with the lack of burden sharing in the alliance. Former Secretary of Defense Robert Gates said upon leaving his post that the imbalance in burden sharing is 'not sustainable in a world where projecting stability is the order of the day.' He expressed worries that if the European allies did not step up to the place, NATO could in the future become a 'two-tiered alliance,' where only some of the members has capabilities and are willing to use them (Global Post 2011).

In terms of cyber defense, similar worries were expressed by an unidentified ambassador to NATO who stressed that NATO efforts in cyberspace 'must not replace the will of individual members to defend themselves in cyber(space) as in other areas' (Reuters 2013). Dr. Jamie Shea, from the ESC division, has stated that NATO, among other things, are focusing on raising the level of cyber security and cyber defense among allies to the level of nations such as the United States, which have invested heavily in this area for a long time (Young Professionals in Foreign Policy 2014).

4 Challenges and Opportunities for Norway

Among the strategies available for states when ensuring security, Norway has chosen to be a formal member of an alliance for collective defense, and NATO is described as the cornerstone of Norwegian security policy (Utenriksdepartementet 2009). This type of mutual defense commitment is of crucial importance for Norway, ensuring that it would receive the support needed in the event of an attack on its integrity.

As in NATO at large, threats in cyberspace have gained increased attention also within Norway. Prop. 73 S described the threat against society's ICT systems as 'high and increasing,' highlighting that managing these threats are challenging for society as a whole (Forsvarsdepartementet 2012a). Minister of Defense Ine Eriksen Søreide stated that digital threats are high on the agenda, both nationally and in the NATO context (ABC Nyheter 2014). Prop. 73 S further emphasized the need for the Norwegian Armed Forces as a whole to maintain the ability to prevent, detect, assess, defend against, and recover normal functionality in case of cyber attacks (Forsvarsdepartementet 2012a).

This chapter will look at the challenges and opportunities for Norway when considering NATO and cyber defense. The aim is to draw from the areas explored in the previous chapter, sketching out some ways Norway can both contribute to and benefit from NATO cyber defense activity, arriving at recommendations for Norwegian policy on NATO and cyber defense.

An important finding from this chapter is that the policy implications for a small nation when considering cyber defense are not so different than those for other alliance matters. While the cyber domain might be a domain *sui generis*, cyber defense policy might not be.

4.1 Keep NATO relevant by integrating cyber defense in the work of the alliance

There are generally three main strategies which all states can employ to further their own security interests: (1) Using own resources to ensure continued existence and independence, (2) Looking towards other states, seeking either to cooperate with, adapt behavior to, or isolate themselves from selected states, or (3) Looking towards the international system in itself, seeking to promote internationally valid norms which decrease probability of attacks (Choe 1999 in Kjølberg 2007). While there are certainly exceptions to the rule, small states are in general dependent either on the resources of other states for protection, or on the cost of breaching international norms being too high, causing potential adversaries to abstain from armed aggression (Kjølberg 2007).

NATO has proved to be the most durable example of an alliance based on collective self-defense. Henrikson (2005 in Kjølberg and Nyhamar 2011) claims that 'Small countries require allies – or to be allies,' which highlights the obvious advantage of being part of an alliance: other states will come to your rescue should you be attacked. There are, however, not only advantages of being in such an alliance. In order to ensure that other states will aid the small state if attacked, there will be instances where small states will have to go along with the interests of the larger states. Such larger states in NATO are the United States in particular, along with the United Kingdom, France, and Germany. A small state like Norway for instance runs the risk of having to participate in military operations it would have rather avoided, if given the option (Kjølberg 2007).

For a small state like Norway, international institutions are important due to the limitations they put on states' freedom of action. The development of international institutions and norms limits the anarchical aspects of the international political arena, making it costly for states to break those norms by attacking another state. The threshold for armed aggression is raised, which is to the benefit of small states with limited defensive resources. NATO can be viewed as what Karl Deutsch called a 'security community,' where the states in the community have a level of trust among them, and that an attack on one member by the other is considered out of the question (Kjølberg 2007).

Norway as a small state does not have the capacity and capabilities to defend itself on its own against large military attacks, and is dependent on its allies in NATO for collective defense in such cases. For NATO to continue to be an institution which will defend the security interest of smaller European countries, the United States needs to continue to view the alliance as relevant, important, and useful. It is therefore paramount for Norway, as a small state in NATO, to contribute to this continued relevance in the eyes of the US.

After the fall of the Soviet Union, many worried about decreased relevance with the loss of its *raison d'être*, however NATO soon took on security tasks 'out of area,' which has dominated the efforts of the alliance during the last couple of decades. New threats to allies, such as those in

cyberspace, must be integrated to make sure that NATO is not seen as an organization that only deals with the 'threats of yesterday'. Norway has on several occasions called out for more focus on NATO's core task, collective defense. As the cyber domain becomes increasingly important for both everyday life and military operations, and threats from cyberspace increase in numbers, it is important to make sure that cyber defense stays on NATO's agenda. For collective defense to be complete and relevant, defense against cyber operations needs to be included.

4.2 Share the burden through increased engagement in cyber defense

Stortingsmelding 15 (2008–2009) predicts that NATO is likely to continue to develop towards becoming a 'collective security organization with responsibility both for contributing to stability, security and defense of human rights in areas far from the territory of its member states, and for the defense of member states' territory.' It highlights that this type of objective will demand more from the member states, 'especially when it comes to active participation and burden sharing connected to NATO operations in conflict areas around the world' [author's translation] (Utenriksdepartementet 2009).

At the same time, the financial crisis in Europe has heightened the pressure on European defense budgets, and Norway has been one of the only countries with an increase in the defense budget. Theories on collective goods as well as historical practice shows that so-called freeloading is widespread, and that it is even natural that small countries contribute a relatively smaller share to the alliance's defense spending compared to larger states (Kvalvik and Nyhamar, forthcoming).

For decades, the United States has voiced concern with the lack of burden sharing in the alliance, and today, the United States contributes around three fourths of the total defense expenditure in NATO (Forsvarsdepartementet 2012a). As mentioned in Section 3.5, former Secretary of Defense Robert Gates claimed in 2011 that if the European allies do not step up to the plate, NATO can in the future become a 'two-tiered alliance,' where only some of the members have capabilities and are willing to use them (Global Post 2011). This would decrease its relevance, as discussed in Section 4.1.

When considering the cyber domain, a potential option for Norway is to shoulder a larger share of the burden than what is generally expected from a small state. On February 18, 2013, the former head of the Norwegian Armed Forces Cyber Defence, Major General Roar Sundseth, stated at Oslo Militære Samfund that Norway is 'a nation with all the prerequisites to be great in this new area. We are a technologically advanced nation, and we have the technology, competencies, and knowledge to protect us for the future – if we are willing to prioritize and commit resources to it' [author's translation] (Oslo Militære Samfund 2013). Hence, such an option could contribute to keep NATO relevant as well as to strengthen the Norwegian influence in the alliance.

4.3 Be constructive and forge relationships to influence decision-making on cyber defense

While a collective defense guarantee is of vital importance, it is also important to be able to influence the decisions made by the alliance to further Norwegian interests. Through memberships in alliances small states 'obtain access to deliberations from which they would be excluded in the absence of alignment, and they assume responsibility for the management of interests and relationships that otherwise would prove elusive or beyond their influence' (Holst 1985:261 in Kjølberg 2007).

As described in Chapter 3, major decisions in NATO are all made by consensus. This means that no state, no matter how small, can be forced to participate in action against its will. At the same time, no state can prevent other states from conducting collective action without the state in question. Such action will, however, not be official NATO action. This procedure gives Norway veto power, despite being a small state, should it disagree with the other member states on an issue. Using the veto power is rare though, even for larger allies. For small nations it is even less of an attractive option, if they want to be perceived as constructive allies. What is usually the case in practice, if NATO is unable to reach consensus, is that states can choose to 'opt out.' This was the case with Greece's opt-out of the Kosovo operation – it chose not to participate in the air strikes, however, did not veto them as it was the only ally that opposed (Kjølberg 2007; Honkanen 2002).

Joseph Nye jr defined hard and soft power as *hard power* being based on coercion and payment, while *soft power* is based on framing agendas, attraction or persuasion (Nye 2010). It is a likely assumption that soft power strategies are a more viable option for Norway in terms of gaining influence in NATO. One such soft power strategy is to, in lieu of using the veto power, seeking to influence NATO decision-making by employing what is termed a 'glue strategy.' This is when the small state seeks to promote its own interests through promoting the organization's mutual interests and values. The aim of such a strategy is to emphasize those interests that are shared by both small and large states, hoping to remove the focus away from the specifically national interest of the large and powerful members (Sens 1996 in Kjølberg 2007).

For Norway, it would therefore make sense to focus on the promotion of collective defense and increased burden sharing, also when considering cyber defense. An example of such an effort could be to reach out to allies with proposals of smart defense efforts on cyber defense, where Norway provides expertise and financial support to a larger extent than expected from a small state.

As Kjølberg (2007) concludes: 'Regardless, it is the application of regulations, appeals to common values and interest, and the use of networks, and not resources which forms the most important basis for the influence of small states in NATO' [author's translation]. In other words, Norway does not have the political, military or economic might to wield power based on resources in NATO, and must rather seek to forge agreements with other allies, perhaps especi-

ally larger and more powerful ones. This holds true not only for cyber defense, but for all issues within NATO.

4.4 Secure own systems and demonstrate resilience

In order to execute operations effectively, one needs resilient and defendable cyber resources, networks, and systems. In the context of the alliance, it is in Norway's vested interest to be seen as a state which takes the cyber domain seriously, and can show its allies secure and resilient systems (Kveberg and Johnsen 2014).

An important step towards this aim was the official establishment of the Norwegian Armed Forces Cyber Defence (CYDEF) on 18 September 2012. CYDEF effectively replaced the Norwegian Armed Forces Information Infrastructure (INI). This represented, according to former Minister of Defense Espen Barth Eide, 'a change of pace in recognizing that ICT plays an increasingly larger and more critical role for the activities of the Armed Forces' [author's translation] (Forsvarsdepartementet 2012b). Prop. 73 S described the cyber domain as a new area of warfare, which will become crucial in future conflicts, and stated that the establishment of CYDEF was intended to reflect this increased importance (Forsvarsdepartementet 2012a). CYDEF's main task is to maintain, secure, and defend the Armed Forces' own systems, networks, and technologically advanced platforms against attacks in and through the cyber domain. Further, the Norwegian Armed Forces are tasked with contributing to NATO's robustness in cyberspace, for instance by contributing to NATO's collective efforts to counter cyber attacks (Forsvaret 2014).

As NATO's own internal systems are connected to a number of national systems, and these systems are becoming increasingly interdependent (as explained in Section 3.2), it is important for Norway to present itself both verbally and in practice as a state with highly developed cyber defense skills, systems, and processes. An example of a small state which has been very vocal, both outside and inside NATO, about its expertise on cyber security is Estonia. It has managed to turn the unfortunate experience of being victim of a rather serious cyber attack into an opportunity to promote itself as a 'cyber security hot spot'. This has resulted both in praise from NATO leadership, a NATO-accredited Center of Excellence for cyber defense, and a role as an opinion-leader on many cyber-related issues in the international public debate. Note that even the Estonian President is regularly raising cyber defense as a crucial issue in his national and international engagements.[4]

NATO is aiming to develop into a more 'cohesive cyber community,' where all member states are at the same high level of cyber security and cyber defense (see Section 3.2). This is currently

[4] See for instance former SACEUR and current Dean of the Fletcher School Admiral (ret.) James Stavridis' interview with Estonian President Toomas Hendrik Ilves for the Tufts University website (http://sites.tufts.edu/fletcherdean/my-interview-with-cyber-expert-estonian-president-toomas-hendrik-ilves/), and the President's own Op-Ed in the New York Times (http://www.nytimes.com/2013/04/12/opinion/global/cybersecurity-a-view-from-the-front.html?pagewanted=all&_r=0).

done *inter alia* through cyber exercises with participants both from allies and partner nations, focusing both on technical and procedural issues (Young Professionals in Foreign Policy 2014). As mentioned in Section 3.5, larger allies are skeptical of in effect sponsoring smaller and less capable allies though NATO common-funded activities aimed at raising the level of over-all NATO cyber security (Reuters 2013). For Norway, proving that it would not be one of the small states in need of sponsoring would likely contribute towards increased goodwill from the larger states in the alliance. If Norway could also provide support to other small nations alongside larger allies, instead of being on the receiving end, it could result in having a more influential voice in the NATO cyber defense consultations.

To paraphrase Major General Sundseth's statement from Section 4.2 (Oslo Militære Samfund 2013), Norway is a nation with all the prerequisites to be great when it comes to cyber defense. It should therefore take any opportunity to show the larger member states that it is committed to contributing to a higher level of cyber security in the alliance. Such opportunities include bilateral visits to cyber facilities, participation in NATO cyber symposiums, as well as active participation in NATO interoperability initiatives and exercises, which leads to the section below.

4.5 Participate in exercises and interoperability initiatives on cyber defense

As argued in Section 3.3, it is a precondition for the successful conduction of coalition operations that the participants have practiced and exercised together in advance of deploying forces. This also holds true for cyber defense. It also goes hand in hand with showing that Norway is a nation where cyber security is a priority, and is an opportunity to showcase capabilities and skills to the broader NATO audience.

Norway has participated in NATO's cyber exercises, such as Cyber Coalition, which aimed to practice NATO procedures for dealing with cyber attacks. Ideally, these exercises benefit both NATO and the nations equally. In Cyber Coalition 2012, the national cooperation between the Norwegian Armed Forces, the National Security Authority, various ministries, and other civilian entities was also put to the test, as the focus of the exercise was cyber attacks against critical infrastructure (Nasjonal Sikkerhetsmyndighet 2012).

Cyber Coalition 2013 was more focused on protecting own networks, and coordination and cooperation between allies, partners, and NATO were at the core or the activities (NATO 2013b). This type of activity is crucial for operating together in an effective and secure manner when actually in crisis. It is important to keep in mind that this type of exercise does not only serve to prepare NATO and its members for incidents that may take place in the future – Norway was already victim to cyber attacks in 2008 while deployed in Afghanistan. Norwegian closed military networks were penetrated, and the Head of the Norwegian Cyber Defence College at the time, Lt Colonel Roger Johnsen, told Norwegian broadcaster NRK that the likely perpetrator was foreign intelligence seeking to gather information and if possible degrade the systems in a critical situation (NRK 2012). This can happen to any coalition member, and it is therefore crucial that the procedures for prevention, mitigation, and response have been coordinated and trained with partners before deploying.

In addition to exercises, there are also several interoperability and capability development initiatives taking place where Norway could be, and in some cases is, an active participant. In order to achieve interoperability in operations which Norway is part of, this interoperability needs to be developed together with allies, within organizations of which Norway is part. Thus, if Norway intends to be an active participant in NATO-led operations, Norway needs to work towards increased interoperability within the NATO framework, also when it comes to cyber defense.

This includes participating in 'smart defense' programs, where nations come together to pool resources, with the intent of getting increased effect out of limited defense resources. A notable example is the cooperation between Norway, Canada, Denmark, The Netherlands, and Romania in the Multinational Cyber Defense Capability Development (known as MN CD2), 'in order to effectively and efficiently develop and acquire capabilities for national use through cooperation.' This smart defense and interoperability program also contributes back into the exercise cycle, by offering the other NATO allies the opportunity to use one of their products, the jointly developed Cyber Information and Incident Coordination System, for Cyber Coalition 2014 (NCI Agency 2014). Other initiatives of note include the efforts on the Future Mission Network and the Connected Forces Initiative.[5]

Finally, the NATO-accredited Collaborative Cyber Defence Centre of Excellence supports NATO's efforts for increased interoperability in the cyber domain, and has as one of its main objectives to work for increased secure interoperability in NATO. As mentioned in Section 3.3, Norway is at present not a member of the center, and could assess whether it should become one in the future (Collaborative Cyber Defence Centre of Excellence 2014).

[5] For more on the Connected Forces Initiative, see http://www.nato.int/cps/en/natolive/topics_98527; for more on the Future Mission Network, see http://www.act.nato.int/article-2013-1-16

5 Conclusion

This report has explored the challenges and opportunities for Norway, as a small state in NATO, in dealing with the emerging challenges related to cyberspace. Perhaps the most important finding in this report is that challenges related to the cyber domain do not need to be treated as something completely different from other challenges that are dealt with within the NATO framework. While the cyber domain in itself might be a domain *sui generis*, the challenges and opportunities for a small state are not fundamentally different from other areas.

In conclusion, the report arrives at the following recommendations for Norwegian policy on NATO and cyber defense:

- Keep NATO relevant by integrating cyber defense in the work of the alliance
- Share the burden through increased engagement in cyber defense
- Be constructive and forge relationships to influence decision-making on cyber defense
- Secure own systems and demonstrate resilience
- Participate in exercises and interoperability initiatives on cyber defense

Norway as a small state does not have the capacity and capabilities to defend itself on its own, and is dependent on its allies in NATO for collective defense in case of large military attacks. For NATO to continue to be an institution which will defend the security interest of smaller European countries, the United States needs to continue to view the alliance as relevant, important, and useful. It is therefore paramount for Norway, as a small state in NATO, to ensure continued relevance in the eyes of the US. As part of this effort, emerging and important challenges need to be fully incorporated into the alliance body of work, as is the case with cyber defense.

The United States has voiced increased concern with the lack of burden sharing in the alliance, and has claimed that the current situation is not sustainable. When considering the cyber domain, a potential option for Norway is to shoulder a larger share of the burden than what is generally expected from a small state, exploiting our resources in this area. Hence, such an option could contribute to keep NATO relevant as well as to strengthen the Norwegian influence in the alliance.

Major decisions in NATO are all made by consensus, meaning no state, no matter how small, can be forced to participate in action against its will. This gives Norway veto power, despite being a small state. This should be considered a last resort for small nations if they are to be considered as constructive allies. Norway must rather seek to forge agreements with other allies, perhaps especially larger and more powerful ones. It is suggested to focus on issues such as collective defense and burden sharing, also when considering cyber defense.

In order to execute operations effectively and securely, one needs resilient and defendable cyber resources. In the context of the alliance, it is in Norway's vested interest to be seen as a state which takes the cyber domain seriously, and can show its allies secure and resilient systems. This should be promoted in NATO fora, and showcased in exercises and operations.

In order to conduct coalition operations successfully, coalition partners need to practice and exercise together ahead of a potential conflict. This also holds true for cyber defense, and goes hand in hand with showing that cyber security is a Norwegian priority. Norway should work towards increased interoperability within NATO, to enable efficient and secure cooperation when conducting operations. Norway should also assess whether it should become a sponsoring member of the CCD COE.

Bibliography

Aabakken, Ola (2002), *INTEROPERABILITET: Kostnadsdriver og styrkemultiplikator*, FFI-rapport 2002/02320

ABC Nyheter (2014), *Frykter lammende IKT-angrep fra Russland og Kina*, last accessed 25 February 2014, http://www.abcnyheter.no/nyheter/2014/02/24/frykter-lammende-ikt-angrep-fra-russland-og-kina

Atlantic Community (2011), *Jamie Shea's answers to your questions*, Open Think Tank, last accessed 21 November 2013, http://www.atlantic-community.org/index.php/Open_Think_Tank_Article/Jamie_Shea's_Answers_to_Your_Questions

Cavelty, Myriam Dunn (2011), *Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture*, IP Global Edition, Vol. 12/3, pp. 11–158, 2011, last accessed 4 October 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997153

Collaborative Cyber Defence Center of Excellence (2014), *Official Website*, last accessed 17 June 2014, http://ccdcoe.org/

European Union (2013), *Collective defence*, last accessed 15 February 2014, http://europa.eu/legislation_summaries/glossary/collective_defence_en.htm

Forsvaret (2014), *Cyberforsvaret*, last accessed 17 June 2014, http://www.forsvaret.no/om-forsvaret/organisasjon/cyberforsvaret/sider/cyberforsvaret.aspx

Forsvarsdepartementet (2012a) *Prop 73 S (2011–2012): Et forsvar for vår tid*, last accessed 17 June 2014, http://www.regjeringen.no/nb/dep/fd/dok/regpubl/prop/2011-2012/prop-73-s-20112012.html?id=676029

Forsvarsdepartementet (2012b), *Cyberforsvaret offisielt etablert i dag*, last accessed 4 October 2014, http://www.regjeringen.no/nb/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/Nyheter/2012/cyber.html?id=699271

Global Post (2011), *Robert Gates blasts NATO members in final speech*, last accessed 4 October 2013, http://www.globalpost.com/dispatch/news/war/military/110610/robert-gates-speech-nato-allies

Healey, Jason and Leendert van Bochoven (2011), *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, Issue Brief, Smarter Alliance Initiative, The Atlantic Council of the United States, Washington, DC

Honkanen, Karoliina (2002), *The influence of small states on NATO decision-making*, FOI – Swedish Defense Research Agency, November 2002, last accessed 17 June 2014, http://www.foi.se/reportfiles/foir_0548.pdf

Jane's Defence (2013), *NATO leaders approve new cyber measures*, last accessed 29 October 3013, http://www.janes.com/article/28785/nato-leaders-approve-new-cyber-measures?utm_content=bufferb0bff&utm_source=buffer&utm_medium=twitter&utm_campaign=Buffer

Kjølberg, Anders and Tore Nyhamar (2011), *Småstater i internasjonale operasjoner*, FFI-rapport 2011/01698

Kjølberg, Anders (2007), *Livet i hegemonens skygge: en småstats sikkerhetslogikk*, FFI-rapport 2007/01626

Kveberg, Torbjørn and Siw Tynes Johnsen (2014), *Cyberdomenet, cybermakt og norske interesser*, FFI-rapport 2013/02712

Kvalvik, Sverre and Tore Nyhamar (forthcoming), *Consequences of the financial crisis for NATO*

Nasjonal Sikkerhetsmyndighet (2012), *NSMs kvartalsrapport for 4. kvartal 2012*, 2012:5

NATO (1949), *The North Atlantic Treaty*, last accessed 21 November 2013, http://www.nato.int/cps/en/natolive/official_texts_17120.htm

NATO (2010a), *Monthly Press Briefing October*, last accessed 21 November 2013, http://www.nato.int/cps/en/natolive/opinions_66734.htm

NATO (2010b), *NATO 2020: assured security; dynamic engagement*, Analysis and recommendations of the group of experts on a new strategic concept for NATO, last accessed 20 November 2013, http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf

NATO (2010c), *New NATO division to deal with Emerging Security Challenges*, last accessed 4 October 2013, http://www.nato.int/cps/en/natolive/news_65107.htm

NATO (2011), *NATO Policy on Cyber Defence: Defending the Networks*, 2011

NATO (2012a), *Interoperability: Connecting NATO Forces*, last accessed 10 January 2014, http://www.nato.int/cps/en/natolive/topics_84112.htm

NATO (2012b), *Organizations and agencies*, last accessed 4 October 2013, http://www.nato.int/cps/en/natolive/topics_66470.htm

NATO (2012c), *The Military Committee*, http://www.nato.int/cps/en/natolive/topics_49633.htm, last accessed 30 April 2014

NATO (2012d), *The NATO Communications and Information Agency (NCI Agency)*, last accessed 13 November 2013, http://www.nato.int/cps/en/natolive/topics_69332.htm

NATO (2013a), *NATO and cyber defence*, last accessed 21 November 2013, http://www.nato.int/cps/en/natolive/topics_78170.htm?

NATO (2013b), *NATO holds annual cyber defence exercise*, last accessed 12 December 2013, http://www.nato.int/cps/en/natolive/news_105205.htm?selectedLocale=en

NATO (2013c), *NATO Strategic Concept*, last accessed 12 December 2013, http://www.nato.int/strategic-concept/roadmap-strategic-concept.html

NATO Allied Command Operations (2013), *SACEUR blog: Looking Ahead*, http://www.aco.nato.int/saceur/looking-ahead-building-bridges-three-big-issues.aspx, last accessed 21 November 2013

NATO Standardisation Agency (2008), *NATO Glossary of Terms and Definitions*, AAP-6, http://www.fas.org/irp/doddir/other/nato2008.pdf, last accessed 4 October 2013

NCI Agency (2014), *Welcome to MN CD2*, last accessed 17 June 2014, http://www.mncd2.ncia.nato.int/pages/default.aspx

NRK (2012), *Afghanistan-styrkene hacket*, last accessed 10 January 2014, http://www.nrk.no/nyheter/verden/1.8178990

Nye jr, Joseph S. (2010), *Cyber Power*, The Belfer Center, Kennedy School of Government, Harvard University

Oslo Militære Samfund (2013), *Foredrag av Generalmajor Roar Sundseth: Cyberoperasjoner – Utfordringer i Cyber*, last accessed 21 November 2013, http://www.oslomilsamfund.no/oms_arkiv/2013/2013-02-18-Sundseth.html

Reiter, Erich and Heinz Gärtner (2001), *Small States and Alliances*, Physica Verlag, A Springer Verlag Company, Heidelberg, Germany

Reuters (2013), *NATO boosts cyber defenses but members differ on its role*, last accessed 21 November 2013, http://www.reuters.com/article/2013/06/04/us-nato-cybersecurity-idUSBRE95318Q20130604

Teknisk Ukeblad (2012), *Norsk tillitskultur passer dårlig i cyberspace*, last accessed 15 October 2013, http://www.tu.no/it/2012/07/03/norsk-tillitskultur-passer-darlig-i-cyberspace

United States Department of Defense (2012), *United States Joint Operational Access Concept*, last accessed 10 January 2014, http://www.defense.gov/pubs/pdfs/joac_jan%202012_signed.pdf,

Utenriksdepartementet (2009), *St.meld. nr. 15 (2008–2009): Interesser, ansvar og muligheter*, last accessed 4 October 2014, http://www.regjeringen.no/nb/dep/ud/dok/regpubl/stmeld/2008-2009/stmeld-nr-15-2008-2009-/19.html?id=548769

White House (2011), *United States International Strategy for Cyberspace*, last accessed 10 January 2014, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Windvik, Ronny and Sverre Diesen (2013), *Cyber Power and the Role of the Armed Forces*. FFI-Forum, Oslo Militære Samfund, 26 November 2013

Young Professionals in Foreign Policy (2014), *Jamie Shea on NATO's role in countering cyber threats*, Leaders in the Spotlight, last accessed 10 February 2014, http://www.youtube.com/watch?v=qLHpMNkTIEk&list=PLq8hckfpW9xkINffFCGrJ12ay8oU_F9wD