

# The North Atlantic Treaty Organization



North Atlantic Council

Study Guide LIMUN 2012

# Contents

Introduction to NATO	3
Meet the Directors	4
Topic 1: Response to Cybersecurity and Cyberwarfare	5
Topic 2: The Decline in Military Budgets and Reduction in Operational Capability	11

# Introduction to NATO

The North Atlantic Treaty Organization was originally formed in 1949 as a military alliance, to, in the words of General Sir Hastings Ismay, its first secretary-general, “Keep the Russians Out [of Europe], the Americans in [Europe], and the Germans Down” – in that sense, NATO has been perhaps the most successful military alliance in history, safeguarding Western Europe against a Soviet invasion for 40 years.

As the Cold War ended, NATO evolved to fit the changing world, and NATO’s role has turned more towards peacekeeping than simply deterrence. It expanded rapidly in the early 1990s and 2000s, taking in many Eastern European Countries that were formerly members of the Warsaw Pact. Furthermore, NATO was heavily involved in peacekeeping during the Bosnian (1991-1995) and Kosovo Wars (1999), has only recently come out of a conflict in Libya, where it played a key role in providing air support to the Libyan Transitional Council’s campaign to oust Colonel Gadhafi.

NATO is currently involved in Afghanistan, under the auspices of the ISAF (International Security Assistance Force), where it is engaged in a long, drawn out counter-insurgency against the Taliban since 2001. The situation has improved markedly since 2008 with much of Afghanistan now relatively stable, though the Taliban still enjoys strong support in many parts of Southern and Eastern Afghanistan.

Throughout the years, NATO has expanded from the 12 original members to 28 current members, standardized weaponry grades between member nations, and introduced an integrated command system that allows for multinational forces to be coordinated effectively under an overall command. While it remains committed to its core principles of protecting the national sovereignty of its member states, NATO has greatly expanded its role,

This committee will simulate NATO’s North Atlantic Council – the Key decision making body of NATO. The two topics that we will be discussing show the key roles that NATO would face in an evolving world. The First Topic will be on the NATO **response to Cybersecurity and**

**Cyberwarfare**, will deal with the importance of the internet to the functioning of a modern state, and the possible defensive precautions that member states can take. The second, topic **The decline in Military Budgets and Reduction in Operational Capability**, will cover the conflicting demands of national governments, and demands of the alliance, and will also touch on issues concerning the alliance's future role in world affairs.

We hope you have an enjoyable and rewarding conference, and we look forward to meeting you.

Kai and Tagore,

Your Committee Directors

## **The Directors**

### **Tagore Nakornchai**

I'm Tagore, and I have the honour of being your committee director. I am a 2<sup>nd</sup> year undergraduate student at Imperial College London, and I am studying medicine. I am active in the Imperial College Model UN Society, of which I am Treasurer, and have attended numerous MUN conferences throughout the United Kingdom, including OXIMUN, CUIMUN, LIMUN, LSEMUN, and have been in pretty much every committee, from the SC, to Crisis to the HRC. Outside of MUN and my course, I'm a keen reader, gamer and historian. I'm really looking forward to meeting you all both in committee, and at the socials, and I hope we'll have a wonderful conference.

### **Kai Kröger**

My name is Kai Kröger. I work as an assistant professor in law at the FernUniversität Hagen, Germany. I've been involved with Model UN since the beginning of my studies more than a decade ago and participated in several roles in about 18 MUN-conferences since then. To have the opportunity to (co-)chair at Europe's largest university level MUN is a tremendous honour for me. I'm looking forward to working together with you and to contributing to a wonderful Model UN-experience for all of us.

## **Topic 1: Response to Cybersecurity and Cyberwarfare**

*“Cyber attacks that may constitute a national security threat are not a science-fiction thing anymore.”*

*Jaak Aviksoo, Estonian Defence Minister*

### **Introduction**

NATO is an organization aimed at enhancing the cooperation and capability of its members for collective self-defence against security threats from outside. Throughout its history and especially after the end of the Cold War, NATO’s primary challenge has been to adapt to new threats and deal with entirely new situations. Modern information society could not have been anticipated when NATO was founded, neither could the rapid developments in computer technology. The societies of all NATO-members profit enormously from an ever more interconnected and globalized world. Together with the enormous potential the dangers connected with it, especially through its misuse by criminals and terrorists have grown at the same pace. Among these dangers is a relatively new term, which is considered by some as the (current or future) fifth domain of warfare<sup>1</sup>: Cyberwarfare. While its actual (current) extent might be considered quite limited, its future potential is enormous and extremely difficult to predict. It is clear however, that cyberwarfare poses an ever increasing threat for the security of all NATO-members.

### **Defining cyberwarfare**

Cyberwarfare can be defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."<sup>2</sup> This is however only a rough

---

<sup>1</sup> The Economist: Cyber War – The threat from the internet, 1 July 2010 ([http://www.economist.com/node/16481504?story\\_id=16481504&source=features\\_box1](http://www.economist.com/node/16481504?story_id=16481504&source=features_box1)). The previous four domains being land, sea, air and space.

<sup>2</sup> Clarke, Richard A.: Cyber War, 2010.

and in no way conclusive definition. Serious security threats may also come from non-state-actors, such as companies, organizational units or terrorist networks. Several incidents of alleged government involved cyberattacks have been reported during the past years, many of them associated with conflicts in the Middle East and the Caucasus region.

### **The scale of the problem**

But what exactly are the dangers associated with cyberwarfare and cybersecurity breaches? Large parts of the world's economies are dependent on interconnected networks and the use of automated computer systems. Many important infrastructure systems, such as power stations, water supply systems, communications networks etc. are especially vulnerable to attacks that seek to interrupt vital services.

Most cyberattacks belong to one of the following two groups:

- 1) Distributed Denial-of-Service (DDoS), which could also be considered as sabotage,
- 2) Espionage.

A DDoS attack occurred on parts of Estonia's infrastructure in 2007. Several government computer systems ceased operation, the country's financial system was also targeted. It was alleged, however not proven, that neighbour Russia was behind these attacks.

DDoS attacks in its simplest form are done by overloading the targeted system with data and network requests in order to slow and ultimately shut down the system entirely. The distribution of malicious software may also be part of such an attack.

Espionage attacks are aimed at gathering information from often classified sources. Unlike DDoS, espionage attacks are normally covert operations that are quite difficult to be detected. Victims will recognize the very existence of an attack with a significant delay, if at all. As *Lewis* stated, sometimes "a consumer might notice that his computer is running a little slower and then blame Microsoft."<sup>3</sup>

Inherent to cyberattacks are the extreme speed in which they cause effects after being launched, and the numerous difficulties in tracing the sources of the attack. The internet offers perpetrators

---

<sup>3</sup> Lewis, James Andrew: Cyberwarfare and its impact on international security, UNODA Occasional Papers 2010, p 11 (<http://www.un.org/disarmament/HomePage/ODAPublications/OccasionalPapers/PDF/OP19.pdf>).

several possibilities to remain anonymous and to cover their tracks, with the use of botnets being only one possible way to disguise one's identity. Indeed the anonymity of the internet is one of its defining factors and may have contributed significantly to its rapid growth. This fact also makes it increasingly difficult to verify government involvement in such attacks, as in most cases of purported government-lead attacks the actual "work" is done by civilian hacker groups.<sup>4</sup> Intelligence information gathered (and made public) by NATO-members suggests, that countries such as China and Russia but also several dictatorial regimes including Iran, Syria and North Korea are involved in sabotage or espionage efforts using cyberspace. Several NATO-members themselves have been involved in cyberattacks as well. However it is worth noting that so far not a single incident of cyberterrorism was confirmed.

The internet is not only anonymous it can also be used to mislead others. The use of botnets or so called 'zombie-computers' connects the computers of unsuspecting users and sends out information and/or malicious software using their identity instead of the original perpetrator.

### **Efforts to prevent, efforts to protect**

Several national governments began to set up own cyber-security plans. The US government created a new agency to deal with the issue and develop effective defence mechanisms against cyberattacks.

The effects of a specific cybercrime are not restricted to the country it originated from. They are, by their nature, international crimes. Therefore, although criminal justice is regarded mostly as a domestic issue of every nation, cybercrime requires a coordinated international approach.

Among the attempts to create an international framework to deal with cybercrime, its prosecution and prevention, especially the Council of Europe's Convention on Cybercrime is worth mentioning. Adopted on 8 November 2001 and having entered into force on 1 July 2004, the Convention is a very early attempt to harmonize national laws and improve cooperation among nations in the area of computer- and cybercrime.

---

<sup>4</sup> Draft General Report by Lord JOPLING (United Kingdom), General Rapporteur (074 CDS 11 E - INFORMATION AND NATIONAL SECURITY), p.5 (<http://www.nato-pa.int/default.asp?SHORTCUT=2443>).

The primary focus of NATO's efforts to counter threats from cyberspace is on protecting its own systems and networks. NATO has, unlike for example the European Union or to some extent the Council of Europe, no influence on the legislation of its member states. Therefore the organization can only call upon its members to introduce effective measures to protect their crucial infrastructure and offer assistance and advise where needed. This, strictly speaking, secondary goal however should not be regarded as being of minor importance. NATO depends on the contributions of its members and on the functioning of their infrastructure to fulfil its tasks. NATO-members also have an obligation to assist in the case of an attack from cyberspace against one or several other member states.

The decision for the development of a revised cyber defence policy was made at the NATO Summit at Lisbon in 2010. A first draft of the new concept was published to NATO defence ministers in March 2011, before being approved on 8 June 2011.

In response to the cyberattacks on Estonian infrastructure the Cooperative Cyber Defence Centre of Excellence was created in Tallinn, Estonia, and accredited as a NATO Centre of Excellence in 2008.

### **Future threats**

An attack on the infrastructure of a specific country most likely will not be any kind of large scale attack that would shut down the whole country, but a more precise, targeted hit on one or few targeted systems. This would also make it more difficult and more time consuming to determine the existence, cause and actual scale of such an attack.

It is worth noting that no attack, no crime, no threat originating in cyberspace so far could have been considered an 'act of war'. They were criminal acts and in some cases part of a broader political or economic campaign, but they were not 'war'. What is called 'cyberwarfare' today is not warfare in any traditional or conventional sense.

When demanding extensive restrictions and control of online sources and the several actors, it has to be made clear, that while probably effective in preventing and prosecuting online crimes, such measures always include an immense loss in privacy rights of all citizens. The right to free access to information and the freedom of speech are at risk, both of them of crucial importance

for an open society as could be witnessed during last year's developments in the Arab world. An open society with (largely) unrestricted and uncensored internet access to all its members has virtually no possibility to prevent all attacks that might come from online-sources within the same country or from abroad.

## **Conclusion**

The tasks before the NATO-Council are as complex as cyberspace itself:

- To identify the threats existing now and possibly in the future.
- To develop strategies to protect NATO, the organization's systems and the infrastructure of its members from threats from cyberspace.
- To address the issue of anonymity, civil liberties and privacy rights on the internet with regard to the reduction and prevention of cybercrime.
- To enhance cooperation among its members with regard to prevention, deterrence and prosecution.

Further complicating the situation are efforts by groups like WikiLeaks to gather classified material and make it available to the public. While such actions will constitute a crime in most countries, any criminal prosecution might encounter enormous obstacles, with the documents already being mirrored by numerous supporters around the world.

Delegates should bear in mind that there are still rapid technological advances which might make it difficult, if not impossible, to predict any future threat. Whatever the council decides during these four days might be outdated the next day. The only answer to this can be to develop a framework enabled to adjust itself to rapidly changing and developing technologies and threats.

## Research links:

- Council of Europe (2011) *Cybercrime* Retrieved from the Council of Europe Website: <http://www.coe.int/lportal/web/coe-portal/what-we-do/rule-of-law/cybercrime>
- International Telecommunications Union (2011). *Home Page* Retrieved from <http://www.itu.int/en/Pages/default.aspx>
- Financial Times (2011) *Cyberwarfare* Retrieved from the Financial Times' website <http://www.ft.com/intl/indepth/cyber-warfare>
- Masters, J. (2011) *Confronting the Cyber Threat*. Retrieved from the Council on Foreign Relations Website [http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577?cid=nlc-dailybrief-daily\\_news\\_brief-link15-20111213](http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577?cid=nlc-dailybrief-daily_news_brief-link15-20111213)
- Munk School of Global Affairs (2011) *Infowar Monitor: Tracking Cyberpower*. Retrieved from the University of Toronto Munk School of Global Affairs – Infowar Monitor) website: <http://www.infowar-monitor.net/>
- NATO Cooperative Cyberdefence Center of Excellence (2011) *Home Page* Retrieved from <http://www.ccdcoe.org/>
- NATO Multimedia Library (2011) *Cyberspace Security*. Retrieved from: <http://natolibguides.info/cybersecurity>
- New York Times (2011) *Cyberwar* Retrieved from the New York Times' Website <http://topics.nytimes.com/topics/features/timestopics/series/cyberwar/index.html>
- North Atlantic Treaty Organization (2011). *Defending Against Cyberattacks*. Retrieved from the North Atlantic Treaty Organization Website: <http://www.nato.int/cps/en/SID-A92C48B5-CECB080C/natolive/75747.htm>
- Office of the National Counterintelligence Executive (2011). *ONCIX reports to Congress: Foreign Economic and Industrial Espionage* . Retrieved from [http://www.ncix.gov/publications/reports/fecie\\_all/index.html](http://www.ncix.gov/publications/reports/fecie_all/index.html)
- United States Department of Defence (2010). *United States Cyber Command* .Retrieved from [http://www.defense.gov/home/features/2010/0410\\_cybersec/](http://www.defense.gov/home/features/2010/0410_cybersec/)

## **Topic 2: The decline in Military Budgets and Reduction in Operational Capability**

Since the end of the Cold War, military spending has plummeted in most NATO countries, especially in Europe – the United States’ share of the combined NATO budget has increased from 50% in 1990 to 75% today.<sup>5</sup> While NATO countries still outstrip the rest of the world put together in absolute terms (with over 70% of the World’s Total defense spending), this is worth significantly less in real terms, and countries such as China and Russia are often perceived to have “undeclared” military budgets which are much higher than their actual spending.

The current recession has further exacerbated the defense cuts, and the Eurozone Debt Crisis has aggravated matters further – countries like Greece and Italy are slashing their military budgets by a quarter, while even the United States faces savage cuts (of \$1.5 trillion) to the Pentagon’s previously untouchable budget. A main victim of these cuts are procurement programs – future weapon systems are often put off in favour of maintaining current programs and hardware. While well-developed programs like the Eurofighter Typhoon or the Airbus 400M that are currently delivering military hardware are unlikely to be cancelled or drastically curtailed, programs further back in the development process have faced serious cuts. The United States drastically reduced the numbers of F-22 Raptors on order, and is considering similarly serious cuts to the much larger F-35 Joint Strike Fighter program. The reduction in American commitment to the F-35 program puts the future of the program in peril, as it would increase price per unit of F-35s for other states involved in the program (such as the United Kingdom, Italy, Canada, the Netherlands, Denmark, Norway and Turkey), thereby further reducing affordability.



The F-35 Joint Strike Fighter Aircraft – a cooperative development between the United States and several NATO and non-NATO allies

---

- <sup>5</sup> Gienger, V. 2011 *NATO Risks 'Irrelevance' Unless U.S. Allies Boost Contribution, Gates Says*.  
<http://www.bloomberg.com/news/2011-06-10/gates-says-european-defense-spending-lag-risks-rendering-nato-irrelevant.html>

Existing forces are also facing savage cuts throughout most of Europe – both France and Germany are reducing the sizes of their armed forces by 40,000 men each and the UK’s Royal Navy is in the process of decommissioning its last Cold War-era aircraft carrier, with the replacement not due for completion until 2016. This reduction makes NATO increasingly reliant on the United States for its strike and expeditionary capability - currently, apart from the US Navy, only the French Navy is a true Blue-Water Navy capable of independent operation with air support.

NATO has a combined force of 3.5 million troops, 17 Aircraft or Helicopter Carriers, 92 Nuclear Submarines, and over 70 destroyers, 100 frigates and 6,000 Aircraft. Most of NATO’s military strength comes from the United States, and while the paper strength of the European members is impressive, deployment is hampered by lack of strategic airlift capabilities, logistical capabilities and unit fatigue. The US, UK and France are the only members of NATO that maintain large military bases outside of Europe and North America. Future NATO operational deployment would rely on the continuing existence of these bases, and it is imperative that these far-flung outposts are spared from defence cuts.

Libya is a prime example of NATO’s European members’ limited capabilities, even in its own backyard – the NATO response was disunited (members such as Germany abstained on the resolution authorizing intervention in Libya), haphazard and relied heavily on American logistical support and capabilities. While the campaign was ultimately successful, this was still a huge strategic commitment for even the UK and France – traditionally the two European powers capable of operating independently. There are serious concerns about the ability of European countries to conduct a similar operation in the future, as the defence cuts really begin to bite.

NATO’s “Comprehensive Political Guidance”, commits members of the alliance to being able to “conduct a full range of military operations and missions”, and “being able to respond to unforeseen circumstances”, and that NATO’s forces member states should contribute “flexible and sustainable contributions, and also by a fair sharing of the burden” – it commits NATO states to having a mere 8% of their total armed forces to be deployed abroad at any one time,

though with another 40% being capable of operational deployment. The document also places an emphasis on “joint expeditionary forces and the capability to deploy and sustain them[,] high-readiness forces [and] the ability to deal with asymmetric forces”<sup>6</sup>

Finally, the last major consideration is, despite NATO’s greatly expanded role, its core principle remains the defense of its member states’ sovereign territory in Europe and North America, as enshrined in Article 5 of the Washington Treaty, which commits all of NATO’s members to a collective response in case of an attack. While there is currently no direct military threat to Europe or North America, the principle of collective defence is vital to the future function of the alliance, and is something that will have to be discussed, even in hypothetical terms.

### **Policy Options:**

This committee will have to address how NATO will be able to maintain its operational capability, particularly for peacekeeping operations around the globe, out of range of airbases in Europe or North America. The discussions will have to take into account NATO’s experiences of the requirements of a modern peacekeeping operation in Kosovo and Afghanistan, but also have to look at possible future involvement in places such as Somalia or other, hypothetical countries.

The primary issue at stake is defence spending levels, particularly the reduction in defence spending that has occurred in the last 20 years. NATO has an unwritten (and often ignored) commitment which expects all its member states to contribute at least 2% of their GDP to defence – presently, only 6 countries stick to this. More stringent enforcement of the 2% limit, or perhaps a reduction in expected spending, given the circumstances, will be on the table.

At stake also is the military procurement process, particularly joint international procurement projects like the F-35 Joint Strike Fighter. There has been an increasing trend towards cooperation in development of military hardware, particularly of expensive and technically complex items such as combat aircraft – the Eurocopter Tiger, Eurofighter Typhoon. Most of these, however, have been agreements between individual nations, rather than NATO programs. Some countries, particularly smaller ones, might be interested in pursuing more multilateral

---

<sup>6</sup> See references

programs, while others, such as the United States, with unique requirements, might prefer to retain the status quo.

If the cuts were to continue to take place, however, discussions would have to be made about what sorts of capabilities should be prioritized, and where the cuts would fall most heavily on. Ground units have already taken large swinging cuts in the past 2 decades – and it would be these ground units that would provide the “boots on the ground” for peacekeeping operations. Navies are important for Power Projection and for supporting far-flung operations, and while aircraft are less important for peacekeeping, they are perhaps the most essential element in the sort of defensive conventional war that remains the core principle of NATO to this day.

Further options include “pooling” – countries agreeing to share military assets, and in doing so, tying together their foreign policies and national interests. Some smaller countries have already pooled together to purchase large transport aircraft to support their operations in Afghanistan. NATO has already moved towards multinational units (such as the Franco-German Brigade or the Heavy Airlift Wing), but these units are limited in scope and do not necessarily tie together the respective countries’ foreign policies. Pooling is also being considered by the British and French – who have plans to pool together their aircraft carriers in order to maintain the ability to launch strikes across the globe, even when their own aircraft carriers are in docks for repair.

A related, but distinct item on the agenda is co-coordinating the cuts of various nations in order to maintain NATO’s operational capability - countries would agree to spare certain aspects of their defence spending while cutting other areas, so as to fill a certain role within NATO. This, like pooling, would further integrate NATO’s countries and reduce the ability of countries to act independently. While countries such as the Netherlands have already taken steps to co-ordinate defence spending with their neighbours, other countries, such as France and the United Kingdom might be more interested in maintaining all aspects of their armed forces (shared aircraft carriers not withstanding)

## **Bloc Positions**

The United States has always contributed the Lion’s share of the budget in NATO, even during the Cold War, but the US is increasingly unhappy with taking the lead as European military spending nosedives, and wants Europe to play a bigger role in collective defence, as America’s

strategic priorities are diverted elsewhere. Facing drastic defence cuts of its own, it has recently pushed for greater European involvement in operations, particularly in Libya.

Many Southern and Western European Countries, facing large budgetary constraints, will be unhappy about any reversal of their current defense policy, and will be determined to continue with the current course. It will be incredibly hard for governments to justify continued large-scale military expenditure on new weaponry in peacetime while schools and hospitals face severe budget cuts and closures.

France and the United Kingdom are special cases – both are nations traditionally used to wielding much global influence through their military machines, and of independent foreign policies. They may resist moves for a more integrated NATO force, as they both value being able to conduct military operations independently, and indeed have done so in the past – France has been particularly active in foreign colonies like Sierra Leone.

Other countries, particularly, Eastern European Countries, are still, touchy about defence, especially due to the rise of an assertive, possibly hostile Russia under Vladimir Putin. These countries might be less concerned about operational and expeditionary capabilities, and more concerned with protecting their national sovereignty. The Baltic States have felt particularly vulnerable, especially after the cyberattacks on Estonia in 2007.

## **References and Further Reading**

It is **HIGHLY** Recommended that all delegates read and familiarizes themselves with the NATO Strategic Concept, and the NATO Comprehensive Political Guidance. These documents detail NATO's primary political objectives, and provide vital background information to the discussions that will take place. The links can be found below. Note that the **PDF** is the actual strategic concept, whilst the html link is the background and rationale.

### Official NATO Sources

- Braddon, D. (2009) *What lies ahead? Defence, budget cuts and the financial crisis*. Retrieved from the North Atlantic Treaty Organization's Website <http://www.nato.int/docu/review/2009/FinancialCrisis/Defence-Budget-Financial-Crisis/EN/index.htm>

- North Atlantic Treaty Organization (1949) *The North Atlantic Treaty*. Retrieved from the North Atlantic Treaty Organization's Website:  
[http://www.nato.int/cps/en/natolive/official\\_texts\\_17120.htm](http://www.nato.int/cps/en/natolive/official_texts_17120.htm)
- North Atlantic Treaty Organization (2006) *Comprehensive Political Guidance*. Retrieved from the North Atlantic Treaty Organization's Website:  
[http://www.nato.int/cps/en/natolive/official\\_texts\\_56425.htm](http://www.nato.int/cps/en/natolive/official_texts_56425.htm)
- North Atlantic Treaty Organization (2010) *Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization* . Retrieved from the North Atlantic Treaty Organization's Website: <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>
- North Atlantic Treaty Organization (2010) *The Strategic Concept* Retrieved from the North Atlantic Treaty Organization's Website: [http://www.nato.int/cps/en/SID-A0D68196-73090399/natolive/topics\\_56626.htm](http://www.nato.int/cps/en/SID-A0D68196-73090399/natolive/topics_56626.htm)
- Rasmussen, A.F. (2011) *Anders Fogh Rasmussen on NATO*. [Video File] Retrieved from: <http://www.economist.com/blogs/clausewitz/2011/09/anders-fogh-rasmussen-nato>

#### Journalistic and Media Sources

- Erlanger, S. (2011) *Panetta urges Europe to spend more on NATO or risk a hollowed-out alliance*. Retrieved from the New York Times' website  
<http://www.nytimes.com/2011/10/06/world/panetta-exhorts-european-nato-members-to-share-defense-spending.html>
- Gienger, V. (2011) *NATO Risks 'Irrelevance' Unless U.S. Allies Boost Contribution, Gates Says*. Retrieved from Bloomberg's website:  
<http://www.bloomberg.com/news/2011-06-10/gates-says-european-defense-spending-lag-risks-rendering-nato-irrelevant.html>
- Mason, D. (2011) *Do Defence Cuts threaten NATO's post-Libya role*. Retrieved from the Public Service Europe Website: <http://www.publicserviceeurope.com/article/779/do-defence-cuts-threaten-europes-post-libya-nato-role>
- Metzler, R. (2011), *NATO Coordination Key as Allies Face Cuts, Says Top US Official*. Retrieved from the US News and World Report Website:  
<http://www.usnews.com/news/articles/2011/12/02/nato-coordination-key-as-allies-face-cuts-says-top-us-official>

- The Economist (2011) *A Troublign Victory*. Retrieved from The Economist's website:  
<http://www.economist.com/node/21528248> (Note that a subscription may be required)

Think Tank Sources:

- Binnendijk, H. And Kugler R. (2010) *A Plan to blunt the impact on NATO of European Defence cuts*. Retrieved from:  
[http://www.europesworld.org/NewEnglish/Home\\_old/Article/tabid/191/ArticleType/ArticleView/ArticleID/21724/AplantoblunttheimpactonNATOofEuropeandefencecuts.aspx](http://www.europesworld.org/NewEnglish/Home_old/Article/tabid/191/ArticleType/ArticleView/ArticleID/21724/AplantoblunttheimpactonNATOofEuropeandefencecuts.aspx)
- Granastein, J.L. (2011) *NATO's Defence Spending Cuts*. Retrieved from the Canadian Defence and Foreign Affairs Institute Website:  
<http://www.cdfai.org/granatsteinarticles/NATOs%20Defence%20Spending%20Cuts.pdf>  
(This source is a MUST read for the Delegate of Canada)
- Valasek, T. (2011) *What Libya says about future NATO Operations.* Retrieved from the Centre for European Reform Website:  
<http://centreforeuropeanreform.blogspot.com/2011/08/what-libya-says-about-future-nato.html>