



STUDY GUIDE



NORTH ATLANTIC TREATY
ORGANIZATION

Hamburg Model United Nations

'Speak Up, Stand Up - Be the Change'

Nov 30 - Dec 3, 2017

www.hammun.de

Content

Content	2
Topic A: A security plan to deter Russian aggression in the Baltic States	3
Introduction to the Committee	3
NATO's mandate	4
*NATO in Areas of Conflict and relevant past actions	4
Russian aggression in the Baltic States	5
What could be done	9
Guiding and pointing questions to ask yourself when reading the SG and writing a resolution	13
Auxiliary and Further Reading	14
Topic B: Articles IV and V in the context of cyber attacks	16
Introduction	16
Consensus Decision-making	17
Description of the Issue	17
Chronology of events	22
Conclusion	24
Bibliography	24

Topic A: A security plan to deter Russian aggression in the Baltic States

Introduction to the Committee

"The Parties to this Treaty reaffirm their faith in the purposes and principles of the Charter of the United Nations and their desire to live in peace with all peoples and all governments." ¹

– Washington D.C. April 4th ,1949.

The North Atlantic Treaty, originally known as the Washington Treaty, is a 1949 agreement which established the North Atlantic Treaty Organization, a mutual defence pact. It currently has 29 members States.

It was founded by 12 countries in Europe and North America to stand strong against communist aggression (or at least as it was perceived by the West) in the post-World War II era.

NATO was established to create an alliance that would unite a specific type of overseas community with shared virtues pertaining to their approach of international cooperation and desire for a non-violent existence. ²

At the heart of the treaty is the mutual protection principle: that an attack against one would be an attack on all. Should a member of the alliance face any sort of danger, the other members would be required to aid in solving said conflict.

The signing of the Washington Treaty eventually led to the formation and instituting of the alliance as an official organization: NATO. This organization provides a platform for members to coordinate their defence policies and respond collectively to threats. ³

¹ Nato. "The North Atlantic Treaty." NATO. N.p., n.d. Web. 06 Feb. 2017.
<http://www.nato.int/cps/en/natohq/official_texts_17120.htm>.

² "What Is NATO?" What Is NATO? N.p., n.d. Web. 06 Feb. 2017.
<http://www.nato.int/nato_welcome/index.html>.

³ "The Founding of NATO." The Founding of NATO | History Today. N.p., n.d. Web. 06 Feb. 2017.
<<http://www.historytoday.com/richard-cavendish/founding-nato>>.

NATO's mandate

An intergovernmental military organization, NATO operates under the constraints of NATO's charter and treaty.

However, unlike most UN bodies, NATO doesn't really have a tangible mandate, and you could say that NATO's mandate is to provide a common defense for the European and Atlantic areas, and to address common issues faced by the member countries, (which is why NATO was formed in the first place). It is also reiterated in Article Seven of the treaty that "UN Security Council responsibility for international peace and security will always take precedence over any NATO obligations"⁴

It is run by a council (led by the NATO Secretary General) of 29 members (29-member countries), and all the resolutions must be adopted **unanimously**, to ensure compliance by member states.

Despite its "tricky" formation and structure, NATO is considered one of the fastest responders to international security crises, and has been involved in several notable global events and armed conflicts: the Bosnia and Herzegovina conflict/Bosnian war⁵; 1999 Kosovo intervention⁶; ISAF (War in Afghanistan)⁷; War in Iraq⁸; Operation Unified Protector (War in Libya)⁹; Operation Ocean Shield (Gulf of Adan)¹⁰ Etc.

NATO in Areas of Conflict and relevant past actions

As we've seen before, NATO is no stranger to conflicts.

In this section, we'll only refer to the Ukraine conflict, and very succinctly. Further information can be found in the auxiliary reading section.

⁴ http://www.nato.int/cps/ic/natohq/official_texts_17120.htm

⁵ https://en.wikipedia.org/wiki/NATO_intervention_in_Bosnia_and_Herzegovina
https://en.wikipedia.org/wiki/Implementation_Force

⁶ https://en.wikipedia.org/wiki/NATO_bombing_of_Yugoslavia
https://en.wikipedia.org/wiki/Kosovo_Force

⁷ https://en.wikipedia.org/wiki/International_Security_Assistance_Force

⁸ https://en.wikipedia.org/wiki/NATO_Training_Mission_%E2%80%93_Iraq

⁹ https://en.wikipedia.org/wiki/Operation_Unified_Protector

¹⁰ https://en.wikipedia.org/wiki/Operation_Ocean_Shield

Following the Ukraine crisis and the Crimea annexation, NATO members responded with tools readily at their disposal: economic sanctions on Russia and conventional military exercises geared toward demonstrating force readiness and new capabilities. NATO leaders clearly stated their intent to continue down this path in the 2014 Wales Summit Declaration, when they announced a Readiness Action Plan that will create a more capable and responsive NATO Response Force and provide a more robust rotational presence in Eastern Europe. They also expressed support for expanding economic sanctions already imposed on Russia.

These measures indicate a common rejection of Russia's actions and a shared commitment to certain concrete steps in response. There is broad agreement that NATO and the EU seek to make Russia pay for its aggression, deter plausible future Russian coercion and threats, reassure NATO member states, and help support the security of non-NATO states.

However, neither the NATO Alliance nor its individual members currently have a comprehensive strategy for accomplishing these goals.

That does not mean that NATO is sitting idly by, but it seems that NATO has yet to come up with a complete comprehensive M.O. and game plan.

In the next part of the study guide, a few suggestions will be brought, but it is highly encouraged that you as delegates will come up with your own ideas and suggestions.

Russian aggression in the Baltic States

As the cold war came to end, it was evident that Russia (USSR successor) was losing its prominent role as one of the two global superpowers, leaving the US as the sole remaining superpower.

The aftermath of the cold war left a bleeding Russia, which focused on its own financial, social, and political problems, rather than cultivating a strong foreign influence or military capability.

However, in recent years, under the leadership of President Putin, Russia is rebuilding a strong powerful army with vast military capabilities, regaining a prominent role in world diplomacy, and perhaps even trying to once again achieve the status of a global superpower.

That, of course, comes at the expense of the US and other prominent European powers.

Acts such as Russia's continuing intervention in Ukraine, including its annexation of Crimea, presents an unequivocal challenge to European security.

Russia's actions are not just a stark rejection of Euro-Atlantic integration; Russia has undermined and possibly even shattered the vision of a stable, secure, and economically healthy Europe that has guided North Atlantic Treaty Organization (NATO) and European Union (EU) policy for two decades.

Aiming to restore its domination in the post-Soviet area and to change the post-Cold War order, the Kremlin seeks to weaken the West which is perceived as the main opponent of its plans to build a new security order in Eurasia and globally.

The Baltic Sea region – with exposed Baltic states as well as non-aligned Sweden and Finland – is perceived by Russia as a convenient test bed in attempting to achieve this goal, aided by the politico-military geography of the Baltic Sea region.

The three Baltic states with a significant Russian-speaking population (such as Latvia and Estonia) and minor military capabilities constitute NATO's exposed peninsula.

To the west Lithuania is surrounded by the militarized Kaliningrad Oblast. To the south, Lithuania and Latvia border Belarus: which has integrated its military with Russia. To the north lie the non-aligned nations of Sweden and Finland, and to the West a nervous Poland, which many believe is exposed to Russian military posturing on its Eastern flank.

The United States and other NATO members and partners are responding with the tools readily at their disposal: economic sanctions on Russia and NATO conventional military exercises to demonstrate force-readiness and new capabilities.

NATO leaders clearly stated their intent to continue this path in the 2014 Wales Summit Declaration, when they announced a Readiness Action Plan that will create a more capable and responsive NATO Response Force and provide a more robust rotational presence in Eastern Europe. They also expressed support for the graduating economic sanctions already imposed upon Russia.

These measures indicate a common rejection of Russia's actions and a shared commitment to certain concrete steps in response. There is broad agreement that NATO and the EU should seek to make Russia pay for its aggression, deter plausible future Russian coercion and threats, reassure NATO member states, and support the security of non-NATO states.

The election of Donald Trump, Brexit, and the outcome of presidential and parliamentary elections in France and Germany in 2017 creates new risks and challenges to the security of the Baltic Sea region.

Russia may anticipate a new US-Russian reset following President Trump's campaign declarations about improving relations with Moscow and including Russia in the wider alliance against ISIS: perceived by the new US administration to be the most important security threat. Russia expects US concessions: loosening of sanctions, curbing the US military presence in the Baltic Sea region and rollback of decisions and measures taken by NATO in 2016.

If Europe's security provider and guarantor (the US) pulls back, European post-Cold War security architecture will be left in jeopardy. Western European does not currently have sufficient military capability assume the US's leading role in European security and defense. The uncertainty will grow as Russia will strive to enforce the idea of spheres of influence in Europe, with the Baltic Sea region (both NATO and non-NATO countries) foreseen to function as a grey zone between Russia and

With US commitment to European security uncertain, it is possible that Russia will use its expanded military presence to test US resolve in the region. This may include

the large-scale Russian military exercises that will take place in Russian Western military district and Belarus in autumn this year.

The provocative behavior of Russian air force and navy units in the Baltic Sea region is considered by many Western nations to be rising, increasing the risk of unintended clashes between Russia and NATO. This will be used to make the US and the newly elected leaders in Western Europe understand that if Russian ‘legitimate’ security concerns about the increased US and NATO military presence in the Baltic Sea region will not be reconsidered and scaled back, the ‘third world war’ may be looming.

In the worst-case scenario, Russia may be willing to military test or even confront the West – by questioning and infringing sovereignty or territorial integrity of the states in the Baltic Sea region. Such a move would likely be based on the assumption the US and Western European countries will be extremely hesitant on how to respond and would prefer to shy away from the conflict and instead strike a new geopolitical deal with Russia.

As part of its effort to demonstrate resistance to hostile actions, the US has increased the number of US jet fighters participating in the Baltic Air Policing mission to defend NATO airspace, established a rotating company-sized contingent in the Baltic states and Poland (ca. 150 soldiers per country) and stepped up US involvement in scheduled military exercises in the Baltic Sea region.¹¹ This includes the deployment of the U.S. Army’s 3rd Armored Brigade Combat Team of the 4th Infantry Division (3/4 ABCT) to the region. The ABCT numbers ca. 4,000 soldiers and will permanently rotate every 9-month period.¹² These are moves made for deterrence: if a NATO member invokes Article 5 of the North Atlantic Treaty a full scale military confrontation would be inevitable.

¹¹ April 2015, NATO’s presence in the Baltic states – reassurance of allies or deterrence for Russia? Available from: <https://www.osw.waw.pl/en/publikacje/osw-commentary/2015-04-29/natos-presence-baltic-states-reassurance-allies-or-deterrence>. [5 December 2016].

¹² Gotkowska, J, 13 July 2016, NATO’s Eastern Flank – a new paradigm. Available from: <https://www.osw.waw.pl/en/publikacje/analyses/2016-07-13/natos-eastern-flank-a-new-paradigm> [14 December 2016].

What could be done

NATO

- NATO's priority is to avoid a scenario in which Russia attempts to test its resolve. Therefore NATO must convince the Kremlin that there are no political or military doubts about the reaction to Russia's hostile actions. NATO's deterrence posture in the Baltic Sea region should be therefore maintained in order not to allow for misperceptions and miscalculations in Moscow. Only a substantial NATO and US military presence in the Baltic states and Poland will convince Russia that all allies are politically and militarily committed to collective defence principle. The Kremlin is a rational actor that calculates the chances and risks of its actions; it is aware of its own military dominance in the region but also of Western/US military superiority in general.
- European allies, and especially Baltic Sea region states along with non-aligned Sweden and Finland will have to face the old-new US demands on burden-sharing. That will mean maintaining or increasing the defence allies and partners are not only preoccupied with ensuring own security but are also responding to security concerns of their allies. That will be one of the arguments for maintaining US presence in the Baltic Sea region.
- The decisions taken at the NATO-Warsaw summit in 2016 were important but at the same time a first step in which will enable effective co-operation between all the elements in the NATO chain of military response.
- The NATO command structure needs to be adjusted in order to effectively run collective defense operations after years of concentrating on crisis management missions out-of-area. The Polish-German Danish Headquarters Multinational Corps Northeast in Stettin needs to continue its preparations to adapt to the new role and tasks related to commanding the NRF forces in the event of their deployment in the Baltic Sea region. It is important to further increase international (US and regional) participation and make the headquarters a regional hub for military cooperation. All NATO forces in the

region (battalion-sized battlegroups, the VJTF/NRF) should be subordinated to one chain of command and should be able to effectively co-operate with US troops and national armed forces. Infrastructure to speed the deployment of rapid response units to the Eastern flank may also need to be improved.. The concept of follow-on forces which would support the VJTF/NRF in large-scale conflict should be fully developed and implemented. NATO needs to invest in early warning capabilities to have at its disposal better intelligence to make quicker political and military decisions. Contingency plans prepared for the Baltic Sea region needs constant updating underpinned by command post and field exercises based on collective defense scenario. There is also a need to adjust the rhetoric and strategy around NATO nuclear policy to Russia's doctrine of using tactical nuclear weapons.

***Poland and the Baltic states**

- Poland and Estonia should stick to the 2% of GDP spending level and speed-up implementing the modernization program of their armed forces. Policy-makers in Lithuania and Latvia need to strive for keeping defence spending and modernization of armed forces out of political games (the second relates to Estonia and Poland as well) in order to preserve the recently established consensus on defence budget at least at 2% of GDP level. Policy-makers in the Baltic states should consider synchronising their armed forces modernisation plans, which would create scope for joint money-saving procurements. They also need to intensify efforts to build mutual trust between them in order to enhance trilateral cooperation.
- Poland and the Baltic states should continue to invest (with the help of NATO and the US) in host nation support measures, including military infrastructure in their countries (air and naval bases, training grounds) in order to be able to receive and accommodate larger NATO forces in case of crisis or conflict in the region.
- Poland along with its regional partners from Visegrad and Baltic region should start a rethink of how to maintain and deepen the cooperation with the US

under the new leadership of President Donald Trump. Poland with the Baltic states may also consider increasing their diplomatic efforts in Washington to convince the new administration that Baltic Sea region security is tightly linked to US security interests. Actions should be undertaken that counter Russian efforts to trivialize the need of US' and NATO's deterrence posture in the Baltic Sea region.

- The Baltics states should improve their strategic communication with regards to reporting on Russian actions in the Baltic Sea region. On the one hand, it should aim to adequately inform own public and allies about risks, threats and challenges Baltic states are facing. On the other hand, it should not have a side effect of spreading too much fear among the population and the allies and therefore serve Russian goals of intimidating the region and the West. Adequate communications strategy needs to be developed in order to counter propaganda and provocations with regards to the deployment and activities of NATO's battalion-sized battlegroups in the Baltic states and Poland. Russia may conduct disinformation campaign along with provoking incidents involving allied soldiers in order to spread distrust against NATO amongst local people.

***Sweden and Finland**

- Sweden should increase its defence spending more significantly, above the amount that has been agreed upon in 2015. As a non-aligned country that is strategically located in the Baltic Sea region, Sweden should develop capabilities to defend its own territory, especially its military infrastructure in southern and central Sweden as well as to prevent any Russian attempts to take control of the Gotland island in case of a conflict in the Baltic Sea region. Sweden also has problems with not enough of military personnel serving in its armed forces, which impedes its operational readiness and capacity to conduct operations for a longer period of time. Wise and partial reintroduction of conscription, as already planned, should help.

- Finland should put more money in its total defence system in order to make it more credible. On the one hand, rehearsal exercises, conscription and maintaining impressive reserve are sending a clear signal, which demonstrates the will to defend the country. On the other hand, Finland has only 8 000 professional soldiers, which are focused on conscripts training on everyday basis. That limits crucial rapid response capabilities to special forces, air force and elements of navy. Without broad political agreement on increasing defence funding, it won't be possible to conduct major planned procurement programs like acquiring new corvettes or replacing F/A-18 Hornet jets.
- Sweden and Finland both should work on a strategy how to counter Russian disinformation and propaganda campaigns targeting both countries. Swedish government should develop a strategy countering Russian disinformation with regard to security and defence. Up to now there are no signs of coordinated efforts in this respect, though the government plans to develop a psychological defence concept. Sweden should also work on improving the cybersecurity of the government's, state agencies' and critical infrastructure networks as well as public broadcasters since they have become the target of attacks. Finland should improve inter-institutional communication regarding security policy and

Russia policy. Insufficient flow of information between the President, government and the parties in the Parliament sometimes leads to confusion and misunderstandings and give the impression of polyphony in crucial issues like security and defence policy. Any Finnish political initiatives involving Russia should be carefully planned and coordinated with partners from NATO and the EU in order to prevent to misuse them by Russian diplomacy as it was the case with the so called Niinistö plan.

- Sweden and Finland should further increase its relations with NATO and the US to the extent possible. However, both countries should take into consideration that they – as partner countries – are reaching the limits of cooperation with NATO. Swedish conservative block should offensively put the question of Swedish NATO membership as one of the main topics for

parliamentary elections' campaign in 2018. With rising public support, this will move forward the political debate and may bring Sweden closer to the accession to NATO.

Guiding and pointing questions to ask yourself when reading the SG and writing a resolution

- What may be your country's red lines regarding the issue?
- Has your country signed any other agreements that have to do with the issue, and do they limit your voting options?
- What is the extent of your country's economic involvement with Russia?
- What can your country gain/loss from cooperation with Russia/NATO?
- We recently witnessed some events such as the election of new leaders in the USA, France, Austria, Germany, and experienced the Brexit. Can (and how) those new circumstances affect the issue and the policies of NATO members and your own?
- What would be your country's position on a possible conflict with Russia?
- Is this topic a high pressing issue for your country? Are there any other issues which you deem to be more pressing and would be willing to compromise on this issue in order to promote them

Auxiliary and Further Reading

<http://www.cbc.ca/news/world/fast-facts-about-nato-1.778864>

<https://www.britannica.com/topic/North-Atlantic-Treaty-Organization>

<https://pdfs.semanticscholar.org/f949/69546bb48c1fe2e155cb550054c09a86ad6d.pdf>

Russia and the security in the Baltic Sea Region; Some recommendations for policy-makers- By Justyna Gotkowska & Piotr Szymański

http://www.centrumbalticum.org/files/2157/BSR_Policy_Briefing_1_2017.pdf

Deterring Russian Aggression in the Baltic States What it Takes to Win- By David A. Shlapak

<https://www.rand.org/pubs/testimonies/CT467.html>

Securing the Nordic Baltic Region-
<http://www.nato.int/docu/review/2016/Also-in-2016/security-baltic-defense-nato/EN/index.htm>

***The Enlargement of NATO-**

Michta, Andrew A. "NATO Enlargement Post-1989: Successful Adaptation or Decline?" Contemporary European History, vol. 18, no. 3, 2009, pp. 363–376.

"North Atlantic Council." International Organization, vol. 4, no. 2, 1950, pp. 335–335.

https://en.wikipedia.org/wiki/Enlargement_of_NATO#Macedonia

NATO in areas of Conflict

http://www.nato.int/docu/review/index_EN.htm

http://www.nato.int/cps/ua/natohq/topics_52060.htm

https://en.wikipedia.org/wiki/NATO#Military_operations

https://en.wikipedia.org/wiki/2011_military_intervention_in_Libya

https://www.files.ethz.ch/isn/137753/Report_Libya_31Agu11.pdf

Topic B: Articles IV and V in the context of cyber attacks

Introduction

The North Atlantic Treaty Organisation (NATO) was established under the North Atlantic Treaty that was signed on 4 April 1949 in Washington, D.C USA and the

Headquarters of NATO are in Brussels, Belgium. The treaty was signed by the following 12 nations: Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, United Kingdom and United States, making them the founding members of NATO. However, NATO now consists of 29 independent members. The following 17 members joined as follows:

Greece (1952)	Estonia (2004)
Turkey (1952)	Latvia (2004)
Federal Republic of Germany (1955)	Lithuania (2004)
Spain (1982)	Romania (2004)
Czech Republic (1999)	Slovakia (2004)
Hungary (1999)	Slovenia (2004)
Poland (1999)	Albania (2009)
Bulgaria (2004)	Croatia (2009)
	Montenegro (2017)

NATO's main purpose is to protect the freedom and security of all its members through political or military intervention. Article 5 known as 'Collective defence' is the groundwork of the Alliance, which creates a universal solidarity between states. During Cold War, NATO used collective defence when facing potential threats from the Soviet Union. However, empirical evidence does not necessarily suggest that conflict has reduced among states in the years following the entry into force of the UN Charter. Of the 243 wars listed by the Correlates of War (COW)¹³ project between 1945 and 2007, 36 are codified as interstate wars.¹⁴ Today, we live in a gravely conflicted world and the frequency of war has increased since UN's non-intervention principle was made into law. As delegates, when researching and addressing the issue debate, you must question the political context in which NATO was created and compare the threats the faced then and the ones we face now. This will enable you to satisfactorily address the issue at hand; the complications developed in threats today can lead to eminent stagnation of progress.

¹³ <http://www.correlatesofwar.org>

¹⁴ Glenn Palmer, Vito D'Orazio, Michael Kenwick, and Matthew Lane. 2015. "The MID4 Data Set." *Conflict Management and Peace Science*. Forthcoming.

Consensus Decision-making

The NATO council is based on reports submitted by five committees: Committee on the civil dimension of Security, Defence and Security committee, Economics and Security Committee, Political Committee; and Science and Technology Committee. Some of the agencies that come under NATO include Central Europe Pipeline System and NATO pipeline System. The decision-making body is the North Atlantic Council (NAC) as mentioned in Article 9 of the treaty. It is a regional collective defence body, which means the decision-making process is different than a UN Committee. As a result, there are no resolution, the council forms solutions and makes decision through its 'Communiqués', which have to pass by consensus. A Communiqué is a result of thorough deliberations, offering a suggestion that binds all members of the NATO Alliance. For example: *Chicago Summit Declaration*.

http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

Description of the Issue

To begin with, Article 5 is the foundation of the NATO Alliance, their primary objective is 'Collective defence', which means if one ally is under an armed attack, each and every other ally will take action it deems necessary to combat the threat.

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 recognized 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.”

NATO has warned the US about triggering Article 5 after the recent Ukraine hacking. This is because a cyber attack against any member of the NATO alliance would automatically trigger NATO’s collective defence clause. The warning was issued shortly after a massive computer hack completely disrupted government ministers and many businesses in Ukraine before spreading to other countries. Extortion and political unrest seems to be the main aim of the latest global cyber attack. Ukraine officials have blamed Russia, which is significant as they are fighting a war against Ukraine in the east of the country and have been accused for alleged cyber attacks on Kiev. There is a consensus among NATO members that Russia has carried out dozens of cyber attacks against other countries sometimes to help or harm political candidates, to cause chaos or evidently proclaim its superiority. NATO believes that Russia has attacked many former Soviet Union countries like Estonia, Georgia, and Ukraine and expanded to Germany and the United States. Intelligence officials infer that these cyber attacks linked with online propaganda, which was launched by Russian intelligence a decade ago.

NBC quoted a statement of Mike McFaul, the former US ambassador to Russia, “ for years now, the Kremlin has looked for ways to disrupt democracies, to help the people that they like to come to power and to undermine the credibility of the democratic process.”¹⁵ He also claimed that Russia seeks to weaken international institutions like the EU and NATO. In 2014, three days before the Ukraine’s presidential election, a Russian-based hacking group attacked the country’s election commission overnight allegedly; it also managed to destroy the backup system. It was later proven that Russia hacked the system to support the pro-Russian candidate despite their efforts Russia’s preferred candidate lost. Having said that Russia consistently coordinated a military and cyber action in the same year when a DDOS attack in Ukraine happened. This attack was 32 times larger than the previous largest one known that occurred

15

<http://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111>

during the Russian invasion of Georgia that disrupted the Internet in Ukraine while pro-Russian rebels were seizing control of the Crimea. They also hacked the computer network in German Bundestag, which is the most prominent hack in German history. Germany's intelligence service said Russia was behind the attack and that they were seeking information and access to Chancellor Angela Merkel's Christian Democratic party. Furthermore, the most significant attack was in November 2016, when Russian hackers attacked computers of the US Democratic Party and gained access to the personal emails of Democratic officials, which were distributed to the media by Wikileaks. The CIA and FBI both believe these hacks were carried out to undermine the election and damage Hillary Clinton, helping Trump to win. One can clearly see the proximity of the issue at hand. Many confidential election information, intelligence reports and military strategies are threatened by Cyber terrorism. The advances of technology have not only made problems more complex and damaging. Therefore, the alliance of today faces a consistently evolving threat that was unseen in the past domains of operation. The only way forward is improving partnerships with other international institutions and other nations to play an effective role in addressing the challenge of cyber defense. As a result, NATO's Science for Peace and Security (SPS) Programme has called for proposals, prioritizing its cyber defense. Priorities stated by the NATO are as follows:

Advanced infrastructure protection, developing cyber defense capabilities, including new technology and raising awareness on the issue. As delegates, one must consider the possible merits and shortcomings of these proposals. Is the only way to tackle Cyber terrorism is new technological advances, stringent penalties for violating laws, or are the key actors in the international political system responsible for their actions in the pursuit of global dominance? Another key factor to consider is, the scope of all these proposals, major areas covered is Security of Physical Cyber systems such as SUAVs, mobile networks, and physical domain (malware, network protocol attacks etc.¹⁶ This can cost a lot of money, the capital used to develop these programmes come from those countries in the limelight such as Russia. How can we create a funding mechanism that works in building an effective defense system without

¹⁶ <http://www.nato.int/cps/en/natolive/145824.html>

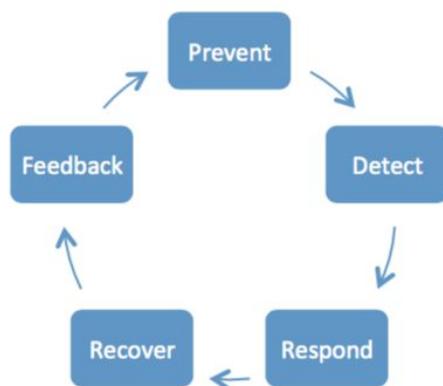
allowing the countries confidential insight on how the system works?

On the other hand, Article 4 can be said to be less controversial than Article 5 as it refers to the consultation process. Turkey on June 26th, 2012 invoked Article 4 of the North Atlantic Treaty. Article 4 states, “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.” This suggests that any country can invoke Article 4 of the North Atlantic Treaty. Once invoked, the issue is deliberated and can lead to a joint action or decision on behalf of the NATO alliance. Since 1949, Article 4 has been invoked a few times. On July 2015, Turkey urged that the NAC take action after the terrorist attacks. Similarly, Poland invoked article 4 in 2014 due to increased tension with Ukraine. However, Turkey requested a meeting under Article 4 twice. The second time was when Turkey asked to deploy Patriot missiles, which NATO agreed to help defend the Turkish population and territory.¹⁷ This article is mostly significant because it triggers united action, UK has also responded to the Ukraine hack, Michael Fallon; the British defense secretary conveyed that UK would consider military retaliations against Cyber attack by another state. This had led to some serious political havoc as the situation intensifies and militarization of Cyberspace is a serious concern. The issue is not only a threat to politics but business too, internet disruption continued in India, Australia and officials said a Cadbury’s chocolate factory in Tasmania stopped production after computers were infected. NCIRC stresses upon the prevention of threats, detection of intrusions, and applying lesson learned through feedback from previous successful recovery strategies. The figure below describes NCIRC’s methodology.¹⁸

¹⁷ http://www.nato.int/cps/en/natohq/topics_49187.html

¹⁸ <http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub>

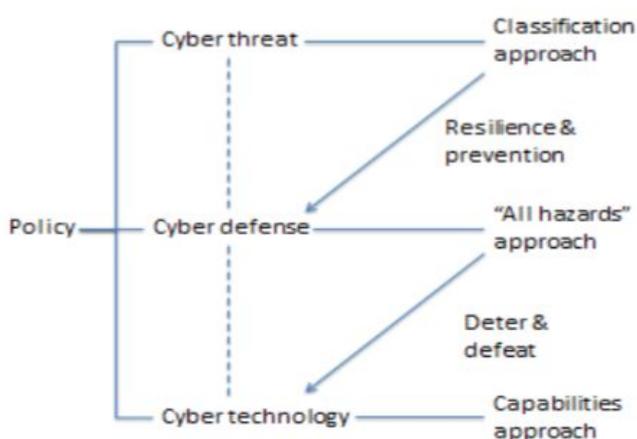
Figure 2. NCIRC's Methodology



NCIRC stresses upon the prevention of threats, detection of intrusions, and applying lesson learned through feedback from previous successful recovery strategies. The figure below describes NCIRC's methodology. The prevention system is outlined as follows:

- (1) Assessing the NATO's penetration testing
- (2) Improve its personnel awareness through training and academic materials.

They also monitor NATO system to detect intrusions that include checking emails for websites for infiltrations. The intrusion analysis determines the nature and scale of a threat and helps to gather a response. NCIRC intends on expanding its current forensic services (P. Fidler et al., 2013). Delegates have to assess the different pathways or approaches taken by NATO to promote Cyber security such as:



As delegates, you must discuss the merits and shortcoming of these approaches and come to a conclusion on what is the most suitable and likely to be effective in order to secure nations from cyber attacks.

Chronology of events

Cyber attacks first happen in 1988, ‘The Morris worm’ was the first worm discovered to affect the world’s nascent cyber infrastructure, mainly in the US.

This timeline should help delegates understand the countries involved in Cyber attacks, the institutions affected by it and how destructive cyber warfare can be. In order to examine possible solutions and assess the merits and shortcomings, delegate should focus on the events and the outcome or solutions used to tackle them and their effectiveness.

October 2007: According to China’s Ministry of State Security 42% of foreign hackers came from Taiwan and the other 25% from the US have been stealing Chinese information.

July 2008: The databases of Republican and Democratic presidential campaigns were hacked and downloaded by foreign hackers.

August 2008: Computer networks in Georgia were hacked and there were theories that it was Russia as they country had some conflict with Russia at the time. Graffiti appeared on the Georgian government websites.

January 2009: Israel’s Internet infrastructure was hacked during the military offensive in the Gaza Strip. This attack was executed by at least 5,000,000 computers. Israel believed these operations were carried out by an organisation in a former Soviet state and was paid to do so by either Hamas or Hezbollah.

January 2010: The ‘Iranian Cyber Army’ hacked a Chinese search engine called ‘Baidu’. All the users were directed to a page showing an Iranian political message. The same group had hacked twitter in December with a similar message.

January 2011: There was a cyber attack against the Canadian government agencies, which included, Defence Research and Development Canada, a research agency for Canada’s Department of National Defence. This led to the Finance Department and Treasury Board, Canada’s main economic agencies to disconnect from the World Wide Web.

July 2011: The US Deputy Secretary of Defence mentioned that a defence contractor was hacked and 24,000 files were stolen.

October 2012: Kaspersky, a Russian firm discovered a worldwide cyber attack dubbed ‘Red October’ had been operating since at least 2007. The main targets were countries in Eastern Europe, the former USSR and Central Asia, although Western Europe and North America reported victims as well. This virus had gathered information from many confidential government embassies, research firms, energy providers, military strategies, and nuclear infrastructures.

March 2013: South Korean financial institutions and the Korean broadcaster YTN had their networks disrupted, which was an allegedly North Korean effort.

June 2013: first ever meeting dedicated to cyber defence. NATO defence ministers agreed that the Alliance’s cyber defence should be fully operational by September.

October 2013: NCIRC Upgrade - The NATO Computer Incident Response Capability (NCIRC) upgrade project, a 58M-euro enhancement of NATO cyber defences.¹⁹

¹⁹ <http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm>

Conclusion

In conclusion, it is important to acknowledge that NATO has been the cornerstone of national security challenges faced by the members of the NATO alliance. Historically, NATO has been successful in overcoming the challenges when confronting the Soviet Union during the Cold War. Having said that, its progress has been prominent but limited in the current affairs of Cyber security, mainly because to some extent the US undermines NATO's authority amongst other international institutions. This is because states are the key actors of the international political system and any organisation, so in order to make NATO powerful and active in combating cyber terrorism and improve Cyber security, the allies of the organisation need to work together making it strong as a whole rather than a tug of war between powerful states. Therefore, as delegates it is your job to satisfactorily address the importance of states and how to create a sense of accountability and effectiveness within the organisation, limiting a single state to violate or undermine its authority.

Bibliography

Review N (2017) *The history of cyber attacks - a timeline*. [Online] Available at: <http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm>.

Windrem R (2017) *Timeline: Ten years of Russian cyber attacks on other countries*. [Online] Available at: <http://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111>

NATO (2017) *SPS - Special Call for Proposals - Cyber Defense*. [Online] Available at: <http://www.nato.int/cps/en/natolive/145824.html>

Collective defence - Article 5. [Online] Available at: http://www.nato.int/cps/en/natohq/topics_110496.html

The consultation process and Article 4. [Online] Available at:
http://www.nato.int/cps/en/natohq/topics_49187.html

Olliphant R and McGoogan C (2017) *NATO warns cyber attacks 'could trigger Article 5' as world reels from Ukraine hack* [Online] Available at:
<http://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransom-ware-attack-cripples/>.

P. Fidler D, Pregent R and Vandurme A (2013) *NATO, Cyber Defense, and International Law*. Indiana: Maurer School of Law: Indiana University Available at:
<http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub>.

Lewis J (2010) *Thresholds for Cyberwar*. Centre for Strategic and International Studies. Available at:
https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101001_ieee_insert.pdf

Coalson R (2017) *What Are NATO's Articles 4 And 5?*. [Online] Available at:
<https://www.rferl.org/a/explainer-nato-articles-4-and-5/24626653.html>.