BERLIN
MUN
BERLIN INTERNATIONAL MODEL UNITED NATIONS E.V.

Environmental, Extremist, Economic: New Challenges to International Security

5 – 10 August 2018

North Atlantic Treaty Organization

Official Study Guide

Borja Pampillón
Corentin Larmoire-Roussel

TABLE OF CONTENTS

Words of Welcome

Dear Delegates,

It is our utmost pleasure to welcome you in the North Atlantic Treaty Organization at BerlIn MUN 2018. For we will work together for a few days we believe you need to be assured that both your chairs will make everything to make you feel at home.

NATO is a committee that is based on cooperation, consensus and peaceful resolution. As such it will be the opportunity for you to practice your talents of argumentation and we are sure that this committee will produce fruitful debates and create bonds for a long time.

NATO has an important position in the world as it is a defence alliance that tackles everyday's issues. The world is changing and if there is one room that is not allowed to stay on the bench, it definitely is NATO. The members are always demanded to adapt to the environment, to the new threats. The past 10 years have seen their loads of extremism rising around the globe and NATO needed to be there to protect democracy, to protect the people.

If this committee is very demanding in time and energy, it is also really rewarding. Every decision is a step forward in the common security and there shall not be steps backwards.

We, the dias, invite you to live with passion, envy and imagination those days of debates. We will be there to help you, but most importantly, this committee is required to help itself to face our challenge of today and tomorrow.

Yours truly,

Corentin Larmoire Roussel and Borja Pampillón

Committee Overview

The North Atlantic Treaty

The North Atlantic Treaty was signed by 12 countries in Europe and in the American continent on April 1949. The core point of the treaty was to promote democracy and cooperation on the matter of security for a long-term alliance. The United States were willing to secure the European continent after the war. During the Cold War NATO was missioned to avoid a nuclear escalation between the Western and the Eastern blocks. After the Cold War NATO focused its effort on peacekeeping operations in the surroundings of the European signatories such as in Yugoslavia until 1999.

In order to defend its values, the treaty and its signatories gave a military capacity to the organization. As such, NATO is able to settle disputes peaceful or by the use of military power.

As of today, 29 countries signed the treaty. The members are the following: Belgium (1949), Canada (1949), Denmark (1949), France (1949), Iceland (1949), Italy (1949), Luxembourg (1949), Netherlands (1949), Norway (1949), Portugal (1949), The United Kingdom (1949), The United States (1949), Greece (1952), Turkey (1952), Germany (1955), Spain (1982), Czech Republic (1999), Hungary (1999), Poland (1999), Bulgaria (2004), Estonia (2004), Latvia (2004), Lithuania (2004), Romania (2004), Slovakia (2004), Slovenia (2004), Albania (2009), Croatia (2009), and the latest admitted in the Alliance, Montenegro (2017).

NATO and the New Challenges to International Security

As a founding principle, any member under armed attack is able to ask for the support of every member. Under Article 5 of the Treaty (shortly know as NAT, or the

Washington Treaty), an attack on one member is considered as an attack on all members.

The NAT is a privileged link between the American and the European continents. Every country at the table has the same voice; consequently every decision of the Organization is taken by consensus.

In 2010 NATO re-evaluated and modernized its objectives with the help of its partners in a strategic concept "Active Engagement, Modern Defence". This concept defines the new threats faced by the countries and their citizens. The North Atlantic Treaty Organization reiterates its will to protect the world from new attacks on democracy, on the people, and on the economy. In June 2016 Reuters rapported that NATO's Secretary General Stoltenberg stated that cyberwarfare declared on one of the member of the Organization could trigger a common response from the Alliance on the ground of the Article 5 of the Washington Treaty.

After the Cold War the states became more stable in most part of the world and the Atlantic Alliance did not face a threat from the Eastern bloc as cooperation became more important to include the former countries of the Soviet Union into a process of development. However the 21st century saw the rising of new threats. The extremism and the terrorism started to cause trouble regarding the efficiency of NATO, especially regarding the Article 5 of the Washington Treaty. Indeed it was harder to know who was the enemy and thus harder for the countries to defend themselves. As such the Article 5 was used once after 09/11 by the United States in order to get support from NATO in the Middle East for the first time. In the modern days and considering the threats created by ISIS, the attacks on NATO territory by unknown militias, it is important to reconsider the question of the common defence to adapt it to the threats of the modern world.

The powers of NATO

The North Atlantic Treaty Organization is meant to coordinate, react and organize the defence of the Members and its Allies. As such NATO works to release a framework for a more efficient common defence. In order to do so the Members States gather and discuss on the capacity of every one of them to analyse the need of the latter from the Alliance.

NATO also disposes of the power of military reaction in case of the use of the Article 5 of the Washington Treaty. When a member calls upon NATO to react under this article it must be determined who the enemy is, and then every member will defend the ally under attack.

It must be considered that NATO produces frameworks most of the time in order to increase the security of the world, but the Organization also has the military capacity and as a committee it must be determined under what circumstances this will be used.

Topic A: Cybersecurity and Terrorism

Introduction

To be able to work on an issue with efficiency, NATO needs to define the issue. As NATO is a global organization it needs to be able to have solid basis of work. Proposing a definition for an issue is always the first step to resolving it and NATO should be able to rely on its own definition but so far never issued a statement on the link between cybersecurity and terrorism.

Many organizations and countries have offered definitions but the diversity of those lets some gaps that slow down the process of reaction for NATO against cyberattacks. Indeed every small difference that can be spotted between each definition leads to a point of discussion at NATO's table.

NATO defines terrorism as "the unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives."

Cybersecurity is defined as "the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems" according to ISACA, a global association working on the protection of information systems. Although it is an internationally accepted definition, it is not issued by any legal organization and can always be a point of friction when it comes to action from NATO or any UN body.

In that context and regarding this definition it is possible to imagine that what is protected can be endangered by attacks. Those cyberattacks would lead to a certain amount of threats and destabilization. Those threats are often called cyberterrorism, and rely partly on the definitions given of terrorism to be tackled.

The European Union defined terrorism in 2002 as “any serious offences against persons and property which: given their nature or context, may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population; or unduly compelling a Government or international organization to perform or abstain from performing any act; or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization.”

The United States of America defined on its part terrorism in the Title 22 Chapter 38 U.S. Code § 2656f as "premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents."

The OSCE defines cyber terrorism as “cyber-related terrorism and more specifically, for our purposes, as terrorist attacks on cyber infrastructure particularly on control systems for non-nuclear critical energy infrastructure.”

The diversity of definitions between organisations needs to be considered regarding the connection between terrorism and cyber threats.

The perks of a wide organization like NATO is that it has a huge capability to react to threats, the loss is that to have a common ground to work on the organization needs to have common terms of definition to react to the same things.

The world faces new threats, from warfare on the ground to warfare on the web, endangering not only soldiers but also directly citizens, governments and companies. Cyberterrorism needs to be defined, tackled and solved. NATO has risen to be the widest organization to focus on cyberwarfare.

NATO's role “is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation. Our vision is to be the main source of expertise in the field of cooperative cyber defence by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners." according to the Cooperative Cyber Defence Centre of Excellence.

Legal aspect of cybersecurity

As a transnational organization, NATO needs to deal with different levels of legislation and consideration. Indeed every country or transnational organization, such as the European Union, does not have the same legislation over espionage, terrorism, or to be more accurate, cyber threats.

The Council of Europe signed a Convention on Cybercrime in 2001. This convention demonstrates the importance of considering the crimes committed on the Internet as serious as a crime committed "in real life". The convention is used to define the crimes that must be dealt with, and to define which party would be relevant to deal with the attacker or the victim regarding territorial legislation. This Convention has been completed in 2006 and many countries, such as the United States of America, have signed it but ever since the European Union has not improved its legislation over cyber threats.

The Cybercrime Laws of the United States of America, enforced in 2006 define the crimes that could be perpetrated on the Internet and consider the need of sanctions for those crimes.

In order to react, every country has its own considerations of the crimes committed online. NATO, as a military organization cannot take a role into every crime committed online and needs to select what kind of crimes can be faced by the organization. If a country's law define the cybercrime as falling under the work frame of NATO which is based on three main points: Collective Defence, Crisis Management and Cooperative Security. Then if cyber threats fall under the definition of one of that point, the members of the Alliance are able to call upon the help of the Organization. In order to prevent those threats NATO also works to focus on the possible threats that could endanger the states under their definition of cybercrimes and terrorism.

Cybersecurity and cyber threats

Cybersecurity and the everyday life

As we entered a digital era our societies focused on the possibility to extend our physical networks to digital ones. By doing so we exposed ourselves to new threats, even though the perks of having all the administrations' data in the "Cloud" are numerous, countless new possibilities are given to target those data.

Not only are we using the internet to stock our files, bank data, money and personal data, but we also rely a lot on the information the internet provides us. As such the network has become a powerful way to influence the people. The fundamental Intel on the internet gathers our personal data and the day-to-day information provided by the media.

International trade, transportation, energy security, among others, became at the same time more secured thanks to the digital era, allowing the administrations to register every data without physical document that could be destroyed but also more vulnerable as some criminals also were given the chance to have an access to it if they are the capacities to access the digital security.

Our interactions, on a personal basis but also on a state-level, are more and more inclined to happen online and every state should be able to protect itself to avoid digital piracy, hacking and thefts. NATO works to ensure the cybersecurity of the citizens of the members of the Alliance and its allies after facing several attacks such as those detailed below.

Unknown and uncontrollable threats

On the opposite of a classical warfare that the world has been facing for centuries, attacks on civilians on a peaceful ground created a new form of war. The enemy is not state-named; the danger is not only on the battlefield. Before 9/11 the world would never have considered that planes could be weaponized, before November 13th 2015 no one would have thought a concert could have turned into a bloodbath. The warfare has changed into a demonstration of fear and shocking acts where they were not expected.

The enemy is unknown and strikes on multiple new places. As such, the Internet could be one of the new places targeted. An attack on a train can nowadays be lead from a computer; a plane can be de-routed from behind a monitor. Many houses now have the capability, through this monitor, to attack any other monitor across the world and endanger either one specific person or a whole group. The access to the internet and computer hardware evolved so drastically in a few decades that it has been a challenge to keep tracks on every possible breach.

Terrorists do not need much to attack a country, a sole Internet connection even in the most remote places of the world, can provide access to data in any office of any country and this danger needs to be understood and tackled by the common defence organization that is NATO.

The recent cyber interference in democracy

For more than 10 years cyberattacks affected international organizations, administrations and countries in general. In 2003 the so-called "Operation Titan Rain" labelled as coming from a Chinese group, gained access to private security contractors in the United States of America but also to the NASA and the FBI. As it concerned sensitive information, tensions between the People's Republic of China and the United States of America appeared, even though it was never proven if the attack was nation-lead.

In 2006, the Operation Shady RAT affected up to 71 organizations, including the United Nations, which were breach on a servers-level, giving access to the hackers to information that could have led to a massive breach of security for the citizens but also to the services across the world such as armies and contractors.

In 2007, Estonia faced a cyberattack on every level, from newspaper to banks to the Parliament. The Russia Federation was strongly criticized and several members of the Russian Douma claimed responsibility. This attacked revealed to the world that a country would be able to interfere with another by the means of the internet networks on various levels, leading to a possible instability. A Russian official even stated that considering the success of the attack, it was clear that the Alliance was in no position to defend itself from a possible Russian attack. This attack was the starting point for the creation of NATO Cooperative Cyber Defence Centre of Excellence to tackle this issue on a multinational level and organize a common defence in the cyber warfare.

The hackers, being state-financed or independent, now have the power to interfere with everyday life by targeting the press, the financial system, but also the electoral system or military. As such, terrorists that are able to have access to those systems have the capacity to destabilize a country, or even endanger the life of those whose information are crucial for their protection, such as military corps on the ground.

In 2016, it is believed that a massive interference caused by a cyber-attack might have changed the course of democracy in the United States of America. Hundreds of documents over the Presidential Campaigns of Bernie Sanders and Hillary Clinton were released to the press and issued by WikiLeaks. In those documents the public learnt that the Democrats would favor Clinton over Sanders which lead to a mistrust of the party. The destabilisation of the candidates is believed by many to have led to a change of opinion over them and then to a victory of Donald Trump in the race for the White House. As there was never any attack on the machines used to vote it is considered by experts that the hacking concerned the people and not only the machine, changing their opinion. On another level Cambridge Analytica (CA) was accused to have used targeted ads on social networks to meddle with the elections and the general opinion. Those news based on some hacked information are called very frequently now “fake news” and are a massive part of the influence that hackers can have over the population.

In a forensic analysis post-attack traces of two Russian-hacking groups were found in the servers of the Democratic National Committee. The same persistent traces were found after the much criticized election of 2014 in Ukraine. It is commonly believed that the Russian Federation interfered with the information the people of both countries was getting before the election to arrive to the best outcome for the Kremlin.

In 2017 North Korea was accused to be the point of origin of the WannaCry RansomWare attack that targeted users of Microsoft across the world, claiming ransoms in Bitcoins. The malware affected almost 250.000 computers in 150 countries, in companies such as the National Health Service in Scotland, the Ministry of Foreign Affairs of Russia, various hospitals and banks and a lot more. This malware, when affecting the computer, was able to encrypt all the data, keeping the user without the control of its computer, leading to a huge security breach.

In 2017, Ukraine was the victim of the cyberattack called “Petya” that lead to numerous shutting down of banks, metro systems, and the radiation monitoring system of Chernobyl. Ukraine was, at that time, in a crisis affecting the political life of the country and in no position to protect itself from a new threat. In that kind of situation it is important for NATO to decide if a cyber-attack on one of its allies should lead to a reaction of the coalition. On another level, the problem with that kind of attacks, just like with “normal terrorism”, is that it takes time and efforts to really identify the attacker.

The necessity for a better understanding

The North Atlantic Treaty Organization, by its leadership position on the common defence area should never be late to understand and analyse the new threats. As such it is important to make this Alliance more efficient and more reactive to the evolving world.

NATO has worked a lot to stay at the state of the art regarding common security, creating working groups such as the Cooperative Cyber Defence Centre of Excellence (CCDOE) and taking very seriously the possibility of a global cyberwarfare. As a committee it is important to analyse and create the best response to the threats of tomorrow.

In 2008 the CCDOE was created in Tallinn. The point of this centre is to improve cybersecurity by training personnel, analysing former attacks and organizing summits to raise awareness on the dangers of cyber threats.

In 2014 Wales Summit the Alliance reaffirmed the importance to prepare itself for the increasing number of cyberattacks that will occur in the years to come, recalling the importance of the coalition and its need to work altogether. NATO recalls also that enhancing cyber defence capabilities amongst the countries of the Alliance and their allies should be of the utmost importance in the future.

In 2016 in Warsaw, NATO declared that the Internet Network was, as the air, the sea and the ground, a place that needed to be defended. As such, an attack on any nation through the web would allow a response of the entire Alliance according to Article 5 of the Washington Treaty. NATO reaffirmed the importance of giving every country the equipment necessary to take measures again the cyber threats. NATO also addressed the “hybrid warfare”, covering the usual warfare that includes soldiers and the cyberwarfare.

The constant need for improvement

Every year NATO's institutional network faces new threats (*i.e.* a rise of 60% between 2015 and 2016 according to the Atlantic Council). As the world leader in the matter of defence NATO needs to be ready to face those new threats. As for now, NATO

Computer Incidence Response Capability (NCIRC) is focusing on the defence of the organization's protection and by extension its allies' network. However, there are several experts that believe that leaving room only for response to the attacks in the matter of cybersecurity would not be the most sustainable and efficient way to protect the network.

By this idea, NATO would have to change the rules of its doctrine by not only allowing the countries to response to cyber threats by waiting on their threshold but also to allow every country and the organization itself to act offensively.

The disparity between the digital capabilities of every member country of the Alliance could be a problem in order to create an efficient offensive network. Indeed some countries are not prepared to have experts able to protect the digital network of their country by an offensive policy. The inequalities amongst the members of NATO are a relevant issue that needs to be addressed by the organization in the years to come. As it is for now, some countries do not have the capacity to protect themselves from cyber threats as they do not have either the money or the personnel to step in when it comes to cyber expertise. The new threats that are cyber-attacks cannot be handled by neophytes, and many countries just do not have yet reached this threshold. As such, it is of the utmost importance to reinforce cooperation between the members of the Alliance themselves but also to reinforce the ties with the allies outside of the organization.

This last point leads to another point of reflexion that cyber experts are working on: the identification of the enemy. Since 2016, NATO considers the web as the air, the seas and the ground, and as such, any attack perpetrated by a foreign power on a country member of the Alliance should be able to call for the Article 5 of the Washington Treaty. Nonetheless it is very frequent that when a cyber-attack is conducted toward a country, the attacker remains unknown, and thus it is impossible for the Alliance to react properly. In the case of Ukraine in 2017, just like in the case of

WannaCry Ransomware or the attack on Estonia, the source of the attack remains unknown and NATO does not have yet the capacity to analyse and react quickly enough to sanction to attacker.

In order to have a better understanding of the threats and to be able to not only react to an attack but also sanction and avoid new threats, NATO, along with many other cyber-security organization, have been looking for a proactive way of tackling the issue. Indeed, for now, NATO only adopts a reactive attitude. From a reaction and a warning to the users, NATO is trying to find a path to intelligence gathering in order to predict malicious behaviours from cyber terrorists.

The warfare the world knew with armies on a battlefield has evolved, including now the Internet, fake news and influence. NATO, as a common defence organization, needs to work on the best way to protect the citizens of the North Atlantic coalition. Fighting on several fronts from the battlefield to the net, from national armies to militias, NATO needs to adapt itself to prevent attacks and to detect the threats. The troops rely on the Intel provided through the net, but they also trust that their protection as some crucial Intel on their position and life are stocked up on the Internet. It is the council duty to work efficiently so that no new terrorist attack, whether it is by militias on the ground killing citizens or by the use of internet to interfere with democracy will endanger the life of the people and the stability of the world.

Questions an Outcome should answer

- How to equalize the capacities of sovereign cybersecurity within the Alliance?
- Should a country under cyberattack be able to invoke Article 5 of the Washington Treaty?
- How could NATO be more efficient to prevent a cyberattack without a passive position of reaction?

Bibliography

http://www.academia.edu/11915903/ISIS_Cyber_Terrorism_Analysis

http://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-an-offensive-cybersecurity-policy

https://ccdcoe.org/cyber-security-strategy-documents.html

https://ccdcoe.org/cyber-definitions.html

http://www.citibank.com/tts/sa/conference/tfc/2015/docs/presentations/0507_charles_blauner.pdf

https://www.cybersecurity-review.com/tag/nato/

https://dema.az.gov/sites/default/files/Publications/AR-Terrorism%20Definitions-BORUNDA.pdf

http://www.gmfus.org/publications/nato-cybersecurity-roadmap-resilience

https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defence-nato-security-role/EN/index.htm

https://www.nato.int/cps/en/SID-9EB36583-C7D51115/natolive/topics_69482.htm
https://www.nato.int/nato-welcome/index.html

https://www.nato.int/cps/en/natohq/official_texts_112964.htm

https://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=https://www.qwant.com/&httpsredir=1&article=2673&context=facpub

https://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE

TOPIC B: Reviewing Article 5 of the North Atlantic Treaty

The North Atlantic Treaty

Understanding when and why the North Atlantic Treaty was born and signed is crucial to understand why the possible malfunction of Article 5 cause its outdated is still very important today, although it is true that Europe didn't suffer a major war since World War II.

NATO wasn't created as a military supra national organization, not like UN, ASEAN or many other that were created as a political international organization; so the main purpose of NATO should always be to assure a effective protection of the allied countries. (Amadeo, 2018)

In 1948 five European countries (France, Belgium, the Netherlands, Luxembourg and the United Kingdom) signed the Brussels treaty (1948) as a military alliance; they were concern about the Union of Soviet Socialist Republics (USSR) power, as they were already threatening the sovereignty of countries as Greece, Czech Republic or Norway. This alliance was called the Western European Union and its main purpose was to protect the member states of any eventual attack or danger to its sovereignty.

One year later, after seeing the fast expansion of the communist countries, these countries decided to create a bigger and stronger alliance. The Western European Union negotiated with the United States of America and Canada, other countries as Denmark, Iceland, Italy, Norway or Portugal were invited too. (Masters, 2017)

These negotiations resulted in the North Atlantic Treaty (1949) that was the starting point of the North Atlantic Treaty Organization. The Treaty is based in article 51 of the United Nations:

“Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.” (UN, 1945)

NATOs foundations were based on the right to self-defence of a country or of an ally.

That is why we need to remark that the main purpose of the organization is the protection of all member states of NATO.

Other very important topic we need to understand and focus on is that the North Atlantic Treaty, negotiated, written and signed back in 1949 only had 2 minor changes in its more than sixty years since its ratification:

- “Article 6, as drafted at the signing of the Treaty in 1949, was modified by Article II of the Protocol to the North Atlantic Treaty on the Accession of Greece and Turkey in 1952.
- The Article dealing with French Algeria no longer became applicable from 3 July 1962, following the independence of Algeria.” (NATO 2, 2017)

So the question is, is the North Atlantic Treaty still an effective protection for the allied countries? Does it have enough measures to cover all the developments and non-conventional war methods?

Article 5

The 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.” (NATO, 1949)

Some important considerations we need to understand about Article 5. Firstly only after suffering an armed attack an allied country can ask to trigger Article 5, any other kind of attack is out of order.

Another very important issue is that the response to the attack doesn’t have to be an armed attack, this is very important because every action is discussed in the North Atlantic Council and the decisions come via consensus; so if there are countries without the will to attack could be difficult to act that way.

Purpose of Article 5

The main purpose of Article 5 is deterrence as the allied countries didn’t want the Soviet Union to keep on. This Article has been successful in the sense that no NATO member has been attacked by a conventional military strike, even during cold war.

The secondary purpose is if the main purpose fails and an allied country suffers an armed attack or invasion in their national soil, the allies have this tool as an exceptional and temporary measure to deal with military threats.

Using Article 5

Allied countries understand the importance of the Article and try to use it carefully, there was a couple times that allied countries considered using it:

- Italy after the Libyan missile attack to Lampedusa.
- France after the Paris terrorist attacks in Paris back in 2015.

Article 5 was triggered just once in more than 60 years since the foundation of the Treaty. This one time was after the terrorist attack in the United States soil, mainly in New York. Less than 24 hours after the attack USA triggered Article 5 with the approval of all member states.

After the terrorist attacks, NATO investigated the attack to get intelligence of the origins of the attack and took further decisions based on the results.

After studies concluded that the terrorist attack came from abroad, both NATO and United States of America used their self-defence rights to start military operations against the Al Qaeda terrorist group, starting October the 4th of the same year. (Herb, 2017)

The operation was requested by the United States of America and its aim was to defeat the terrorist group on its own bases in Middle East. This self-defence/anti-terrorist operation, named Eagle Assist took place from mid-October 2001 to mid-May 2002.

This was the first time that NATO military assets were deployed in support of an Article 5 operation. (The Telegraph, 2016)

Problems of not updating Article 5

As any of us can understand almost everything has changed in one way or another since 1949, technological evolution is probably the biggest change since 1980 until today, and it's one of the reasons that Article 5 could be consider to be outdated.

Let's study deeply some of the main problems of Article 5:

Reach of Article 5

First of them is that Article 5 is not very concrete about the term armed attack or the solutions to them; as solutions has to be made in consensus this turn out to be very difficult.

If we check the example of the only time that Article 5 was triggered we found out some things that are quite curious:

- The first operation took place one month after the attacks, with so many countries involved it's pretty obvious that it was not a logistics problem. The problem was that countries first needed to have much more intelligence about the attack to be 100% sure about whom and why those attacks were made.
- Even after getting the intelligence countries discussed a lot about if they have the right to attack in a third country, as the terrorist group was not a country by itself but it was placed in some areas of certain countries. The military operation was going to take place in a neutral country soil.

Article 5 has shown to be very difficult to use because it's based on the interpretation that the countries give to it, and as the decisions come via consensus and with countries mentalities are so different ones from one another, it is very difficult to reach an agreement to take some sort of action against a country or organization.

New non-conventional war strategies

As we already understand after read the first topic the phrasing of the Article 5 is outdated due to the evolution of war methods. First sentence of the Article says "The Parties agree that an armed attack against one or more of them", restricting the right to use Article 5 as self-defence to armed attacks.

Nowadays countries try to maneuver in a more subtle ways of war, with Russia allegedly using Hybrid Warfare methods against some Easter European countries for many years now. Those Hybrid War methods included cyber war, publicity, psychological attacks and irregular warfare (militias) to conquer Crimea from Ukraine.

The use psychological war and cyber-attacks to impair decision making procedures during key moments of the allied countries, for example Russia allegedly used it to disturb the elections of Germany back in 2017.

The countries cannot give a joint response to these attacks as Article 5 doesn't allow them to do so, and the strength of the alliance comes from all countries joining in a collaborative response to the problem.

With this being said NATO is trying to solve it through defence but, is this going to be enough or will the tool that gave the alliance its strength in the past also be the end of the NATO?

Lack of protection of allied territories

Many of the allied countries have being complaining that the instruments of the North Atlantic Treaty are not enough to keep their country safe. We need to understand that Article 5 is geographically restricted by Article 6, and due to recent geopolitical problem this came to be a major issue. Some of the problems are the following:

- US-North Korean problem: at the peak of the confrontation Korea was said to have an intercontinental missile that could reach Hawaii, but even if Korea attacked Hawaii USA would not be able to trigger Article 5 as Article 6 says: "on the forces, vessels, or aircraft of any of the Parties, when in or over these territories or any other area in Europe in which occupation forces of any of the Parties were stationed on the date when the Treaty entered into force or the Mediterranean Sea or the North Atlantic area north of the Tropic of Cancer." And Hawaii is at the south of that tropic.(Gady, 2017)

- Even it's true that Turkey has being a challenging NATO member, it is true that it has being asking for more protection because of the Syrian war, and only receiving poor assistance of the alliance.(Saidel, 2018)
- Poland has being feeling left alone for some time now, as it's one of the countries that suffers the most the Russian Hybrid Warfare methods. Poland government stated a couple times that they are afraid of ending like Ukraine.(Goettig, 2014)

Those are some examples of safety feeling problem that NATO is facing right now.

Questions an Outcome Document should answer

1. Try to reach an agreement about reach the coverage that Article 5 offers as it is right now.
2. Is enough if NATO could build facilities and strategies in order to get more protection against hybrid warfare methods?
   a. How can NATO defend the allied countries against it?
3. Is there any need to rewrite the article to make it more clear and adapt it to the 21st century war methods?
   a. How could Article 5 be written to reach that purpose?
4. How can we solve the safety feeling problems NATO is facing?
5. Should Article 5 keep on being linked and conditioned to Article 6?

Bibliography

Amadeo, K. (2018, April 10th). The Balance. Retrieved from https://www.thebalance.com/nato-purpose-history-members-and-alliances-3306116

Gady, F.-S. (2017, May 29th). The Diplomat. Retrieved from https://thediplomat.com/2017/05/second-korean-war-would-nato-invoke-article-5/

Goettig, M. (2014, April 15th). Reuters. Retrieved from https://uk.reuters.com/article/uk-ukraine-crisis-poland/poland-nato-should-send-troops-to-east-europe-ignore-russias-objections-idUKBREA3E0RA20140415

Herb, J. (2017, July 6th). CNN. Retrieved from https://edition.cnn.com/2017/07/06/politics/what-is-article-5-nato-trump/index.html

Masters, J. (2017, may 15th). Council on Foreign Relations. Retrieved from https://www.cfr.org/backgrounder/north-atlantic-treaty-organization-nato

NATO. (1949, April 4th). North Atlantic Treaty Organization. Retrieved from https://www.nato.int/cps/en/natolive/official_texts_17120.htm

NATO 2. (2017, January 30th). Retrieved from https://www.nato.int/cps/ua/natohq/topics_67656.htm

Saidel, N. (2018, January 19th). CERL. Retrieved from https://www.law.upenn.edu/live/files/7539-turkey-nato-1192018

The Economist. (2015, March 9th). Retrieved from https://www.economist.com/the-economist-explains/2015/03/09/how-natos-article-5-works

The Telegraph. (2016, November 9th). Retrieved from https://www.telegraph.co.uk/news/0/what-is-nato-and-how-does-it-keep-europe-safe/

UN. (1945, June 26th). United Nations. Retrieved from http://www.un.org/en/sections/un-charter/chapter-vii/index.html