NORTH ATLANTIC TREATY ORGANIZATION

TOPIC BULLETIN

KRISHI DESAI
BRENDAN O'REILLY
CHAIRS

Contents:

Academy Model United Nations

- THE TWENTIETH ANNUAL CONFERENCE -

SECRETARIAT

CIRO RANDAZZO
SECRETARY GENERAL

NICOLE GERZON
CHARGÉE D' AFFAIRS

JENNIFER KONG
SHALIN PATEL
DIRECTORS OF EXTERNAL RELATIONS

JUN-DAVINCI CHOI
GRACE LIANG
DIRECTORS OF INTERNAL AFFAIRS

CHRISTIANA MONES
ISHAAN CHAWLA
DIRECTORS OF INTERNAL AFFAIRS

KAIRUI HUANG
JESSICA SHI
DIRECTORS OF ADMINISTRATION

RYAN LEUNG
DIRECTOR OF BUSINESS

AKSHAYA JAGADEESH
DIRECTOR OF OUTREACH

DEREK LIN
MICHELLE SURETS
DIRECTORS OF CRISIS

ANDREA BUCCINO
FACULTY ADVISOR

MARK KRAMER
FACULTY ADVISOR

Welcome Delegates,

My name is Krishi Desai and it is my pleasure to be your head chair of NATO for the 20th session of Academy Model United Nations. Model UN has been one of my favorite activities since freshman year. Discussing social, political, and economic issues from a global standpoint has always been a major interest of mine. In order to have successful committee sessions, I suggest that all delegates perform thorough research on their nations' government, geography, culture, and more, as well as on both topics.

Outside of Model UN, I enjoy writing for BCA's school newspaper, The Academy Chronicle as well as our political magazine, The Academy Global. I am a Junior in The Academy for Business and Finance, and my favorite subjects are History and English. Outside of school I enjoy eating penne vodka, watching Criminal Minds, New Girl, and Friends (just to name a few), and shopping on Amazon.

I encourage delegates to actively participate in discussions, be inclusive, and collaborate with others. I am looking forwards to seeing what everyone brings to the table at AMUN 2019, and I would be happy to answer any questions or concerns you may have, so please feel free to email me!

Sincerely,
Krishi Desai, Head Chair, NATO
krides20@bergen.org

Greetings Delegates,

My name is Brendan O'Reilly, and I am more than happy to serve as your vice chair of NATO for the twentieth year of the Academy Model United Nations. I am a student in the Academy for Business and Finance. International affairs, especially from an economic perspective, is a topic that has always interested me. Therefore, I am extremely excited to witness excellent debate surrounding the North Atlantic Treaty Organization. My passion is singing in my school's chamber choir. In college, I would love to study some aspect of business or economics, whether it be real estate, international business, business economics, etc. My dream job is to be a luxury real estate broker abroad.

Krishi and I would like to emphasize that everybody should be actively involved in all discussions and debates in order to maximize the time made available during Academy Model United Nations 2019. The more each delegate understands about his or her country's stance on a given topic, the more heated and interesting the committee will be. With full, passionate participation from every delegate, Krishi and I believe that AMUN 2019 will be one of the best yet.

With warm regards,
Brendan O'Reilly, Vice Chair, NATO
breore20@bergen.org

Topic A: NATO's Cyber Defense Efforts

Overview:

Cyberterrorism is defined as the politically motivated use of computers and information technology to cause damage to public life or economic, social, or political institutions. There are two main types of cyberattacks that are of NATO's concern: cyber-enabled espionage, and cyber-enabled sabotage. Cyber-enabled espionage involves gaining access to confidential information regarding a nation's political, economic, or social data, and potentially giving this information to adversaries. Meanwhile, cyber-enabled sabotage entails accessing control to a nation's infrastructure, such as energy or transportation, and potentially stopping their functions. NATO works to both protect the passage of information within its own networks and help its allied members develop their own cyber defense programs.

Topic History:

NATO Allies endorsed an enhanced policy and action plan on cyber defense at the Wales Summit in September 2014. The policy affirmed that cyber defense is a component of the Alliance's core task of collective defense, that international law applies in cyberspace, and that NATO will further collaborate with industry. Members made a Cyber Defense Pledge in July 2016 to improve upon cyber defense, and have worked together to make information sharing more efficient. NATO has several structures in place to manage cybersecurity. The NATO Computer Incident Response Capability (NCIRC) guards NATO's own networks by providing support to various NATO sites, keeping records of cyberattack incidents, and distributing incident-related information to security management and users. Cyber Rapid Reaction teams, a part of the NCIRC, are available 24 hours a day to aid Allies if needed. In addition, NATO's Defense Planning Process sets targets for Allies to reach regarding their countries' cyber defense capabilities and tracks progress in meeting those goals. NATO also offers cyber security education, training, and exercises to Allies through institutions such as The NATO School, The NATO Cyber Range, and The NATO Cooperative Cyber Defense Centre of Excellence (CCDCE). These organizations work to further develop strategic thinking, alliance operations, policies, and procedures. Furthermore, NATO's Industry Cyber Partnership (NICP) allows the committee to work with the private sector in order to gain expertise and technological innovations. The private sector can also aid in raising awareness and understanding about cyber risks.

Current Situation:

Recently, Microsoft reported discovering more evidence of Russian government hacking efforts in conservative think tanks in the U.S. Facebook recently identified and removed about 650 disinformation (misleading information) pages out of Iran and Russia that were aimed at interfering with politics in the U.S., UK, Latin America, and the Middle East. Facebook's investigation began due to a tip from the private cybersecurity firm, FireEye, regarding the suspicious activities of a network called "Liberty Front Press" that was eventually linked to Iranian state media. FireEye said the operation "is leveraging a network of inauthentic news sites and clusters of associated accounts across multiple social media platforms to promote political narratives in line with Iranian interests." These narratives include pro-Palestinian, anti-Saudi, and anti-Israeli themes, and rally support for Iranian policies from citizens in the U.S.

The spread of disinformation can be harmful as it can contaminate elections by spreading inaccurate information and manipulating citizens. Disinformation campaigns and hacking were experienced during the 2016 U.S. Presidential Election, and could potentially impact the upcoming 2018 U.S. Midterm Elections.

Possible Solutions:

Artificial intelligence (AI) could prove to be highly valuable in combatting cyberterrorism. AI algorithms use Machine Learning and can be adapted over time to counter evolving types of malware. AI also has the ability to categorize attacks based on their threat level. Still, AI has its limits, as malware can grow more complex and require the expertise of a human being rather than a machine.

NATO can benefit from collaborating with the EU more actively. The EU's Cyber Crime Centre can offer insights into criminal cyber activity.

Delegates should consider how NATO can further its cooperation with the private sector, which was proven to be advantageous in the situation with FireEye and Facebook.

It can be helpful to make citizens more aware of potential cyber threats and instruct online users to report any unusual activity they witness regarding fake personas and disinformation campaigns.

Bloc Positions:

The United States has been proactive in its cybersecurity efforts, especially with the help of U.S. based corporations such as Facebook and Microsoft. The Department of Homeland Security has been working to strengthen state defenses by providing guidance and services. Countries like the U.S., UK, Netherlands, Canada, etc. can more easily procure funding for election security and cybersecurity overall. They can also produce legislation regarding cybersecurity more efficiently than nations with struggling government institutions. It could be beneficial for these nations to act as leaders in cybersecurity and share their information with other Allies.

Countries like Estonia or Latvia that are near Russia, a country well known for its connections to cyberterrorism, may express reservations regarding punishments for cyberterrorism. Taking physical (military) action against Russia could impact Estonia, Latvia, and other surrounding nations. These nations may be hesitant to act unless NATO can acquire concrete evidence that Russia is the perpetrator in a possible cyberattack. Even then, the repercussions of attacking a neighbor country like Russia may leave these countries unwilling to participate.

Some countries (e.g. Turkey) are currently in economic/political

turmoil. These countries often lack the resources necessary to allocate funding towards cybersecurity or may not be able to make cybersecurity a priority if they have larger ongoing issues. These nations will need the assistance of NATO's cybersecurity leaders. Although, delegates must keep political relationships in mind when considering whether leader Allies will be willing to aid the struggling Allies. For instance, there are currently growing hostilities between countries such as the U.S. and Turkey. Some nations may want to keep their resources and information to themselves instead of sharing it.

Questions to Consider:

A major problem with cybersecurity is that it is difficult to identify the perpetrator of a cyberattack by way of conclusive evidence. How can NATO find more efficient ways to gather this evidence before military action can be taken against a nation?

What is considered an act of war in terms of cyberspace?

What course of action will NATO take in response to a member nation being attacked by cyberterrorism? Clear ramifications need to be specified so post-attack decisions are not as difficult to make.

How will the course of action for a cyberattack on a governmental institution differ from that on a private sector institution?

How will NATO react if a member nation invokes Article 5 of The North Atlantic Treaty (the article that states that an attack against one Ally is considered an attack against all Allies) in response to a cyberattack?

Topic B: Environmental Impact of Military Operations

Introduction:

Founded in 1949, NATO, or the North Atlantic Treaty Organization, is a peace-building body comprised of twenty-nine nations that works to battle political and military issues in and around the member countries' borders. NATO's overall mission has two components: prevent conflict surrounding nations' political spheres, and utilize military efforts in crisis-related situations to ensure the peaceful termination of detrimental disputes between countries. In 1995, NATO participated in its first principle crisis-management operation. Today, NATO's members vote on a wide variety of plans regarding the implementation of military and political endeavors throughout Europe and the United States of America.

This topic guide will explore the history of NATO's military operations, while offering an extended discussion of the modern-day situation and policies that NATO's member nations have

enforced surrounding military operational sustainability.

Topic History:

While the North Atlantic Treaty Organization has been guaranteeing peace via political and military operations since 1949 [1], environmental sustainability issues around the world have been evolving at an increasing rate throughout the twentieth and twenty-first centuries.

Since the organization's onset, NATO has employed itself on numerous missions that have had a lasting impact on the world. For example, in 2005, Pakistan requested NATO's help after a deadly earthquake killed an estimated 53,000 individuals, and displaced over 4,000,000 natives within Pakistani borders [1]. NATO was able to supply the country with nearly 4,000 tons of provisions and resources, while also aiding the country by providing them with specialists, medics, etc. In the same year, Hurricane Katrina struck the United States of America, and NATO initiated a military operational plan to allocate resources and individuals where they needed to be [1]. Thus, the impact of NATO on the world is clear from its historical efforts and projects.

In 1969, NATO established the Committee on the Challenges of Modern Society, which tackles environmental issues being augmented by the body's military efforts [1]. The CCMS, through workshops, long and short-term projects, conferences, and more, is able to discuss and fix any issue within the sustainability realm regarding NATO.

From this section, delegates should be able to understand that the history of NATO and its acknowledgement of its environmental effects date all the way back to the organization's establishment. Delegates should also acknowledge the degree to which the North Atlantic Treaty Organization aids important crisis situations around the globe.

Current Situation:

According to the International Peace Bureau, military operations can have a slew of effects on the environment. These effects can include, but are not limited to, the pollution of the air, land, water, nuclear weapon creation, land use and deterioration, and diversion of resources. In the words of the Bureau, "The US military is the largest single source of US environmental pollution. The cost of clean-up of military related sites is estimated to be upwards of $500 billion. [2]." Delegates can see the degree to which the military affects the environment in just the United States alone.

As of 2006, NATO's Committee on the Challenges of Modern Society (CCMS) has merged with the NATO Science for Peace and Security (SPS) organization. The joint organization seeks to achieve the same goals as CCMS had, while incorporating more scientific approaches to their research.

Currently, NATO includes a list of actions on their website that the organization is approaching in order to better the environment. These actions include, but are not limited to, "protecting the environment from damaging effects of military operations; promoting environmentally friendly management practices in training areas and during operations; adapting military assets to a hostile physical environment; preparing for and responding to natural and man-made disasters; and, addressing the impact of climate change" [1].

All of the aforementioned subjects fall into one of two categories according to the North Atlantic Treaty Organization: environmental protection or environmental security. When discussing subjects in the environmental agenda, NATO distinguishes their committee conversation between these two fields. Environmental protection topics deal with protecting the natural environment from military operations' detrimental consequences, while environmental security topics deal with security

issues that come from the natural environment.

One specific topic that NATO has put on its forefront in recent years has been energy efficiency regarding its military operations. According to NATO Secretary General Anders Fogh Rasmussen, "energy security is becoming a truly strategic issue, with numerous implications for Allied security" [3]. In his 2014 speech, the secretary stated that Europe's demand for oil production has been steadily increasing in recent years, due to the increased demand for military tools and resources. Moreover, Rasmussen stated that the financial burden of military forces deployed far from NATO's borders require new energy efficiency resources. Is NATO prepared for these new energy efficiency resources? How will NATO obtain these environmentally sustainable resources? These are some of the questions delegates will begin to explore in their research.

Currently, over 20,000 soldiers are deployed on NATO missions worldwide, dealing with situations in every type of environment possible. As of 2018, NATO is operating within the borders of Afghanistan, Kosovo, and the Mediterranean. With each day that passes, NATO continues to discuss the topic of its military operations affecting the environment, and just as NATO does, delegates will begin to explore possible solutions to the issue based on their country's policies.

Country Policy:

United States

The United States' Environmental Protection Agency (EPA) is an independent regulatory agency that works to ensure that the United States' environment is healthy and not corrupt by pollution, contaminants, etc. Laws such as the Clean Air Act, the Clean Water Act, and the Toxic Substances Control Act work towards environmental sustainability within the States' borders. For the United States, the EPA is the main organizational body that controls and oversees

policies regarding the environment [4].

European Union

Like the United States, the European Union has strict policies surrounding environmental sustainability within its borders. In fact, the European Union itself states that the EU has "some of the world's highest environmental standards" [5]. The Union has over 500 directives, laws, and regulations to keep the environment safe and healthy.

Questions to Consider:

What is your country's policy surrounding environmental sustainability - especially within the military sector?

What can we do to quell some of the negative environmental effects of military operations?

What military operations specifically create the most issues?

Which member countries within NATO have begun to create solutions for military operational impacts? What are these emerging solutions?

What solutions are feasible based off of each delegate's country's resources?

What financial resources does your country have to implement a feasible solution?

References:

1. https://www.nato.int/cps/en/natohq/topics_91048.htm
2. http://www.ipb.org/wp-content/uploads/2017/03/briefing-paper.pdf
3. https://www.nato.int/docu/review/2014/nato-energy-security-running-on-empty/nato-energ
4. https://www.epa.gov
5. https://eur-lex.europa.eu/summary/chapter/environment.html?root_default=SUM_1_CODED%3D20
6. money.cnn.com
7. www.vox.com/policy-and-politics