UTMUN

SPECIALIZED COMMITTEES | 2014

# NORTH ATLANTIC TREATY ORGANIZATION

# (NATO)

UTMUN

Background Guide

NATO (North Atlantic Treaty Organization)

2013-2014

http://www.utmun.org

## Topic I: Cyber-Warfare

### I. Introduction to the Topic

#### A. General Background

A great debate circles around the concept of cyber-warfare. While some claim that cyber-warfare is the fifth domain of warfare (after land, sea, air and space), others simply claim the term is an attempt at sensationalism. From a more specific perspective, cyber-warfare refers to any action by a nation-state to penetrate another nation's computer networks for the purpose of causing some sort of damage. However, broader definitions claim that cyber-warfare also includes acts of 'cyber-hooliganism', cyber-vandalism or cyber-terrorism. [1]

Cyber-warfare imposes an intensifying threat on national and private sectors. Attacks are intensifying day by day due to the international connectivity and the domination of computer-controlled systems. Hence a nation's infrastructure and private data are more exposed and vulnerable than ever, especially in areas of communication, transportation, and power. Now that nations in the international arena are in a new race for "information", cyber-terrorism has become a worldwide practice invested in by leading countries. This issue is of severe importance, since the origin of cyber-attacks is often untraceable. Such attacks can cause complete breakdowns of governmental systems and nations' infrastructures, as well as infiltrating the personal life of civilians. (quote)

#### B. Definition of Key Terms

**Cyber-warfare**

There is no official international definition for cyber-warfare. However, the U.S. government security expert Richard A. Clarke, in his book *Cyber War* (May 2010), defines cyber-warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." [2]

**Espionage**

Espionage involves a government or individual obtaining information considered secret or confidential without the permission of the holder of the information. [3]

**Cyber deterrence**

This term is used to describe systems that designed to prevent cyber-attacks.

**Sabotage**

Sabotage is a deliberate action aimed at weakening another entity through subversion, obstruction, disruption, or destruction. In a workplace setting, sabotage is the conscious withdrawal of efficiency generally directed at causing some change in workplace conditions. [4]

**SCADA** (Supervisory Control and Data Acquisition)

Computer controlled systems that monitor industrial processes.

**Trojan**

A Trojan horse, or Trojan, is a non-self-replicating type of malware, which gains privileged access to the operating system while appearing to perform a desirable function but instead drops a malicious payload; often including a backdoor allowing unauthorized access to the target's computer. [5]

**Computer Virus**

A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other files; when replication succeeds, the files are then said to be “infected". [6]

## C. UN Involvement

The discussion of this topic in the United Nations in 1998 proposed several resolutions since.

In 1998, the Russian Federation proposed draft resolution 53/70 which was adopted in January 1999. The main key elements consisted of the following:

- Recognition of the military potential of information and communication technology for the first time as well as an expression of concern about the use of such technology – inconsistent with the objectives of maintaining international stability and security;

- Clarifying the need to prevent cyber-crime and cyber terrorism;

- Inviting all member states to propose their opinion towards this topic.

Later, the Russian Federation proposed several resolutions in order to specify the rather general one proposed in 1999. Henceforward, the proposed resolution in 2005, which was sponsored not only by Russia, but also by the People's Republic of China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan, and Uzbekistan, was adopted by many more votes, with only the USA voting against the implementation of this resolution. This matter shows that there was an international clash.

### NATO Involvement:

In opposition to the notion of increasing dependence on technology and web-based communications, NATO is advancing its efforts to confront the wide range of cyber threats targeting the Alliance's networks on a daily basis. NATO's Strategic Concept and the 2012 Chicago Summit Declaration recognized that the growing sophistication of cyber attacks makes the protection of the Alliance's information and communications systems an urgent task for NATO.

In June 2011, NATO adopted a new cyber defense policy and an associated Action Plan, which sets out a clear vision of how the Alliance plans to bolster its cyber defense efforts. This policy reiterates that the priority is the protection of the NATO network but that any collective defense response is subject to a decision by the North Atlantic Council, NATO's principal political decision-making body.

### D. Recent Events

Experts say that concentrated cyber-attacks have the ability to cripple a nation's ability to defend itself and destroy its economy and national wealth. Here is a list of some large recent cyber attacks:

1) **2011:** Operation Shady RAT is an ongoing series of cyber attacks that began in mid-2006 and have been targeted at national governments, military contractors and organizations such as the United Nations.

2) **December 2010:** The Pakistan Cyber Army hacked into the website of India's Central Bureau of Investigation.

3) **November 2010:** The Indian Cyber Army accessed websites operated by the Pakistan Army and several government ministries, including the foreign affairs, education and finance ministries.

4) **November 2010:** The United States Department of Defense admits its internet traffic was rerouted through China for a period of 18 minutes in April. China denied the

claim. [7]

A recent report published by Reuters on September 17, 2013, stated that researchers have discovered a group of highly sophisticated hackers operating for hire out of China. A US computer security company known as Symantec Corp linked them to some of the best-known espionage attacks in recent years. This company believes that this group has been involved with the 2009 Operation Aurora attacks, the most well known cyber espionage campaign uncovered to date against U.S. companies. In Operation Aurora, hackers attacked Google Inc., Adobe Systems Inc. and dozens of other companies. [8]

Another report published on October 3, 2013 says that Adobe, the American multinational computer software company, was hit by a massive cyber attack. The company says that an intrusion led to an untold number of Adobe IDs and passwords falling into the hands of hackers, which may have compromised around 2.9 million customers. Among that data set are customer names, encrypted credit / debit card numbers, and expiration dates.[9]

### E. Possible Solutions

A first attempt to solve such an issue can be through acknowledging cyber attacks as an infringement on human rights, and a threat to national security. Organizations could be established to monitor international computer systems to better control cyber attacks and strive for more clandestineness. There could be conflicts regarding national interest if such a solution was established. It is up to the delegate to discuss a wide range of possibilities and ideas in order to reach the best solution for this issue.

## II. References:

http://www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/cyberwarfare/ [1]

http://encyclopedia.thefreedictionary.com/cyber+warfare [2]

http://encyclopedia.thefreedictionary.com/espionage [3]

http://encyclopedia.thefreedictionary.com/sabotage [4]

http://encyclopedia.thefreedictionary.com/Trojan+horse+(computing) [5]

http://encyclopedia.thefreedictionary.com/pc+Virus [6]

http://www.telegraph.co.uk/news/worldnews/asia/japan/8775632/A-history-of-major-

cyber-attacks.html [7]

http://www.reuters.com/article/2013/09/17/us-cyberattacks-china-idUSBRE98G0M720130917 [8]

http://www.theverge.com/2013/10/3/4800042/adobe-suffers-cyber-attack-millions-of-customers-affected [9]

## Topic II: NATO membership expansion in Eastern Europe

### I. Introduction to the Topic

### A. Background Information

NATO's expansion has been a vital episode in history. In early 1952, Turkey and Greece were the two nations participating in the first expansion of NATO. In 2004, NATO saw its biggest expansion yet, where seven nations were accepted to become member states in the North Atlantic Treaty Organization. Those countries included Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia and Slovenia, symbolizing NATO's biggest expansion in Eastern Europe. However, the year 2009 marked the last NATO enlargement, when Albania and Croatia's bids where both accepted.

NATO still has its doors open for expansion; NATO's "open door policy" is based on Article 10 of its founding treaty[1], which states:

"The Parties may, by unanimous agreement, invite any other European State in a position to further the principles of this Treaty and to contribute to the security of the North Atlantic area to accede to this Treaty. Any State so invited may become a Party to the Treaty by depositing its instrument of accession with the Government of the United States of America. The Government of the United States of America will inform each of the Parties of the deposit of each such instrument of accession."[2]

Delegates will be required to discuss the possibilities of further expansions for NATO in Eastern Europe. They are encouraged to tackle the likelihood of Ukraine, Georgia or Russia joining in, and discuss what could be the consequences and further strive to find the best compromised solution.

### B. NATO-Russia Relations

The 28 Allies in NATO and Russia work together as equal partners in the NATO-Russia Council (NRC), which was established in 2002. The NRC provides a framework for consultation on current security issues and practical cooperation in a wide range of areas of common interest. Its agenda builds on the basis for bilateral cooperation that was set out in the 1997 NATO-Russia Founding Act, which provided the formal basis for relations.

Cooperation between Russia and NATO member states is directed by the NRC and developed through various subordinate working groups and committees. Every year, NRC member countries agree on an annual work program.

Key areas of cooperation include: the fight against terrorism, defense reform, military-to-military cooperation, counter-narcotics training of Afghan, Central Asian and Pakistani personnel, theatre missile defense/missile defense, counter-piracy, crisis management, non-proliferation, airspace management, civil emergency planning, scientific cooperation and environmental security.[3]

### C. Should NATO expands more?

Many question whether NATO should expand into Eastern Europe or not. Some see it as a threat to Russia, since with every expansion into that area means that NATO must establish its defense systems in that country. Some others see it as further accomplishing one of its main goals, which is to advance a Europe whole, free and at peace by integrating once vulnerable European nations into a community of free-market democracies committed to one another's' collective defense. Delegates are encouraged to tackle this issue and discuss what is more beneficial for NATO and Europe's security. Should NATO decided to expand, what countries may join the Organization? What might be the reaction of neighboring countries; will they consider it as a threat?

### D. Possible Solutions

Delegates must discuss solutions concerning the addition of new members to NATO. They must see if this is necessary and study what could be the consequences of such action. For instance, accepting a possible bid from Ukraine or Georgia might be considered as a threat to Russia, therefore risks the NATO-Russia relations. Is there a road to compromise?

## II. References:

http://www.nato.int/cps/en/natolive/topics_49212.htm [1]

http://www.nato.int/cps/en/natolive/official_texts_17120.htm?selectedLocale=en [2]

http://www.nato.int/cps/en/natolive/topics_50090.htm? [3]

## Topic III: 1. Responding to the Crisis in Syria

### I. Introduction to the Topic

#### A. General Background

On the 15th of March 2011, protests broke out in Daraa, a city in the South West of Syria, and then spread to other cities across the country. These protests where part of the wider Middle Eastern protest movement known as the Arab Spring. Protesters demanded the resignation of President Bashar al-Assad, whose family has held the presidency in Syria since 1971, as well as the end of Ba'ath Party rule, which began in 1963.

In April 2011, the Syrian Army was deployed to quell the uprising; soldiers fired live ammunition on protesters across the country. [1] After several months of military sieges, the protests evolved into an unorganized, but armed, rebellion, mainly composed of defecting soldiers and civilian volunteers, without a central leadership.

Many foreign fighters from neighboring countries are currently involved in the conflict, fighting either with the Opposition or the Regime. Some of these groups are extremists, such as, but not limited to, Al Nusra Front and the Islamic State of Iraq and Syria (ISIS), whom are known to be fighting against the Regime, and are recognized as associates with Al-Qaeda. Some other foreigners, such as Hezbollah (also known as the Lebanese Resistance) and Liwaa Abul Fadel Al Abbassy from Iraq, are fighting with the Regime. Hezbollah's Secretary General has confirmed on 25 May 2013 that his soldiers are directly involved in fighting the rebels along side the Regime. Recent documents exposed by the Opposition activists have shown the presence of, not just Iranian, but also Russian, mercenaries fighting along side President Assad.

Whether these documents where to be true or not, the Syrian Crisis is getting out of control. According to the Syrian Observatory for Human Rights (SOHR) in a documented posted on the 30th of October 2013, more than 120,000 people are killed in Syria since the beginning of the uprising in March of 2011. [2]

#### B. NATO on the Crisis in Syria

NATO has always kept a close eye on the situation in Syria, especially after the national security of Turkey became threatened. Therefore, NATO deployed 6 patriot batteries on the borders between Syria and Turkey in the cities Kahramanmaras, Adana, and Gaziantep. Together, these Patriot batteries are actively defending 3.5 million people in Turkey against missile attacks. [3]

Furthermore, NATO's Secretary General Anders Fogh Rasmussen said that the option of carrying out a military strike or similar operation in Syria must be kept open as a way of dealing with the crisis. He continued: "I think, irrespective of the outcome of the deliberations in the U.N. Security Council, the military option will still be on the table." [4] Mr. Rasmussen also welcomed the U.S.-Russian agreement on the elimination of Syrian chemical weapons; however, he insisted that a military intervention must still be in order.

### C. Possible Solutions

The situation in Syria is deteriorating on a daily basis. A UN military intervention is out of question; both Russia and China have threatened to use VETO power to block any resolution that legalize a military intervention in Syria in the Security Council. NATO, however, can intervene militarily because NATO is a separate entity from the UN, therefore it has the independence on deciding whether a military intervention is to occur. Delegates are encouraged to envisage such a solution and evaluate the consequences of a NATO intervention in Syria. They must decide if NATO should use their military against specific targets on the ground, such as in Libya, or launch a full-scale battle against the Regime. Delegates must find short and long term solutions to end the crisis.

## II. References:

http://www.hrw.org/node/99345/section/5 [1]

http://syriahr.com/en/index.php?option=com_news&nid=1064&Itemid=2&task=displaynews#.Upuy6pGExuY [2]

http://www.nato.int/cps/en/SID-17A115FF-3B9BB9B3/natolive/news_98494.htm [3]

http://www.reuters.com/article/2013/09/19/us-syria-crisis-nato-idUSBRE98I06720130919 [4]