Sofia International Model United Nations

SOFIMUN

1st – 8th of August 2015

STUDY GUIDE

FOR THE

NORTH ATLANTIC

THREATY

ORGANISATION

TABLE OF CONTENTS

I. INTRODUCTION

MESSAGE FROM YOUR CHAIRS

Dear delegates,

As the Chairs of the North Atlantic Treaty Organization at SOFIMUN 2015, let us begin this message by saying that we are all very excited for this year's conference. We have come up with interesting and thought provoking topics which we hope will be the source of heated debates fused with enthusiasm and passion. We expect the delegates to read this study guide carefully and use the links provided in the future reading section to help them with their further research. Reading the study guide will give you useful insight on the topics, as well as guide you towards the issues that need to be tackled during the debate.

Remember that this committee will be judged by its work and the results produced. The Chairs will do their best to guide you towards writing the best possible resolutions, but it is ultimately you, the delegate who will benefit the most from making this committee and its work as fruitful as possible.

On that note, we look forward to seeing you all during the conference and feel free to contact us if you have any questions or inquiries.

Yavor Gochev, *Chair*, **yavor_gochev@yahoo.co.uk**

Silvia Fiore, *Co-chair*, **f-silvia@hotmail.it**

HISTORY OF THE NORTH ATLANTIC TREATY ORGANISATION

The North Atlantic Treaty Organization (NATO; French: Organisation du Traité de l'Atlantique Nord; OTAN), also called the North Atlantic Alliance is a political and military alliance of 28 North American and European countries, bound by shared democratic values, that have joined together to best pursue security and defense. In addition to the United States, the other NATO Allies are Albania, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, and the United Kingdom. The principle of collective defense is at the heart of NATO and is enshrined in Article 5 of the Alliance's founding Washington Treaty, which asserts that an attack on one Ally is to be considered an attack on all. NATO invoked Article 5 of the Washington Treaty for the first time in its history following the 9/11 terrorist attacks against the United States.

Founded in 1949, NATO played a unique role in maintaining stability and security in the trans-Atlantic area during the Cold War. Since the end of the Cold War the Alliance has transformed itself to meet the security challenges of the new century, continuing with adoption of a new NATO Strategic Concept at the Lisbon NATO Summit in 2010. Today, NATO's operations include leading the International Security Assistance Force (ISAF) mission in Afghanistan, ensuring a safe and secure environment in Kosovo through the KFOR mission, and contributing to international counter-piracy efforts off the Horn of Africa through Operation Ocean Shield. In 2011, NATO successfully carried out the UN-mandated mission in Libya to protect civilians, enforce a no-fly zone, and enforce a maritime arms embargo. NATO has also provided airlift and sealift support to the African Union (AU) missions in Somalia and Sudan, has engaged in a number of humanitarian relief operations in recent years, including delivery of over 100 tons of supplies from Europe to the United States following Hurricane Katrina, and leads the counterterrorism Operation Active Endeavor in the Mediterranean Sea.

Recognizing that the security challenges Allies face often emerge beyond Europe, NATO has become the hub of a global security network, establishing partnerships with over thirty countries. These ties provide opportunities for practical military cooperation and political dialogue. Partners have contributed significantly to NATO operations in Afghanistan, Kosovo, Iraq, and Libya.

II. TOPIC A: NATO's future involvement in the Middle East: Afghanistan Reflections and the issue of ISIS

RESEARCH QUESTION

In the last couple of years, NATO has begun concluding the ISAF mission in Afghanistan. After 11 years of operations, some 87 percent of the population will soon live in areas under Afghan control. Liaising with the Afghan government, civil society, and representatives of the international community and neighboring countries, the Afghan people have been afforded a level of organization and security, which should permit the stable transition into a functioning democracy and a strong and independent Afghanistan. Nevertheless, stressing the need for regional cooperation, many Afghans have expressed concerns over the potential re-destabilization of the post 2014 Afghanistan, especially considering the fact that in January 2015 Afghan officials confirmed that there ISIS had an increasing military presence in Afghanistan and they are in the process of recruiting militants[1].

In the light of the concluding ISAF mission, what should NATO's mandate regarding operation and presence post 2014 be? Recognizing the need for efficient and integrated strategic planning and Smart Defense what should be NATO's minimum engagement in post 2014 Afghanistan? Could cooperation with regional security organizations, such as the Shanghai Cooperation Organization, and OSCE, as well as further engagement with regional partners (such as Russia and Pakistan) contribute to NATO's follow-on mission to support the development of ANSF capacity? Analyzing and assessing the newly posed threats by ISIS and the effect that they might have on the situation in Afghanistan post 2014. In the interest of cultural significance, should the mandate promote the utilization of Muslim assets for a steady and lasting transition to a democratic Afghanistan?

CONTEXTUAL BACKGROUND

A) AFGHANISTAN

Afghanistan's geostrategic importance is crucial in analyzing the challenges of Afghan state building, as Afghanistan has extensively experienced frequent invasions by external players. Afghanistan is a country at crossroad of ideologies, religions, economic and geopolitical interests[2]. It encompasses a variety of tribes, ethnic, linguistic and religious entities. These lines of division have generated a certain lack of a united Afghan national identity, as well as served as a premise for numerous points of clash and violence between and among Afghans over the years[2]. On several occasions in Afghanistan's history, often times of profound crises, national borders have been drawn and efforts

[1] Aljazeera.com, (2015) *Officials confirm ISIL present in Afghanistan.* [online] Available at: http://www.aljazeera.com/news/asia/2015/01/afghan-officials-confirm-isil-presence-201511815245847478.html

[2] Young, D. (2015) *Overcoming The Obstacles To Establishing A Democratic State In Afghanistan*. 3rd ed. Maroon Ebooks.

made to produce and stabilize a central government. These have been rather unsuccessful partly if not mainly due to the consolidated local strata of tribal and religious loyalists.

In 1747, however, the Pashtun tribes were unified by Ahmad Shah Duranni, forming what is now known as Afghanistan[3]. The state immediately became a buffer zone between the two great British and Russian empires up until its independence from the former in 1919. Afghanistan attempted the rule of democracy for the next 54 years, which lead to a coup d'etat in 1973, and a 1978 Communist countercoup. A prolonged conflict was generated by the Soviet invasion of Afghanistan in 1979 in attempts to strengthen the wavering Afghan Communist regime. The Afghan war was lost by the USSR, as the communist superpower withdrew in 1989 under unyielding pressure by internationally backed anti-Communist mujahedin rebels[3].

The void present upon the withdrawal of the perceived enemy, as well as the destabilized internal situation which lead Afghanistan towards a path of multiple civil wars, resulted in the fall of Kabul in the hands of the Taliban. Having experienced the occupation under the British and the Soviets, Afghanistan's connection to NATO commences with this historical event the installation of the Taliban regime in Kabul in 1996. Taliban, a hardline Pakistani sponsored movement that emerged in 1994 to end the country's civil war and anarchy, comprised of a group of religious students that left Pakistan, were successful at seizing the void created by the withdrawal of the Soviet Union from Afghanistan, as they emerged on a fight against what they claimed to be the corrupt government of Kabul. For the next two years, Taliban, headed by Mullah Omar as its supreme leader, propagated the unification and purification of Afghanistan through extremist measures[4]. This proved to be 'successful' as by 1998, except for certain northeastern provinces and Kabul, Taliban acquired control over Afghanistan[5].

This was possible through the support received from the government of Pakistan. Pakistan had been both a supporter and a combater of Taliban in Afghanistan. Desiring a proxy government over which they could establish control and influence, Pakistan, during the rule of Taliban in Afghanistan from 1996 till 2001, provided support and directions to Taliban's activities[6]. Theocratic in its nature, Taliban relying heavily on recruitment from Pakistan was based on its own interpretation of Islamic law. This resulted in a harsh and oppressive set of policies directed towards Afghans, as citizens were subjected to totalitarian and oppressive form of governance.

The UN sponsored Bonn Conference in 2001 proposed a process for political rebuilding of Afghanistan. After the September 11, terrorist attack on the World Trade center, the Coalition forces, headed mainly by the United States in coordination with NATO, defeated the Taliban in 2001, bringing an end to their rule in Afghanistan. Taliban was not defeat however, but rather simply dispersed into the mainstream Afghan population or diffused across the Durand line, Afghanistan's eastern border with Pakistan [4]. Since its retreat, the Taliban has reclaimed control over certain parts of Afghanistan, particularly in the southern and eastern regions, remaining a substantial impediment towards a stable, secure and democratic Afghanistan[3].

Several positive developments emerged with the end of Taliban rule in Afghanistan. A

new constitution was drafted, along with the elections of the new president and national legislature following the Bonn Agreement of December 2001. The economic situation showed

[3] Cia.gov, (2015) *The World Factbook.* [online] Available at: https://www.cia.gov/library/publications/resources/the-world-factbook/geos/af.html

[4] Young, D. (2015) *Overcoming The Obstacles To Establishing A Democratic State In Afghanistan*. 3rd ed. Maroon Ebooks.

[5] Tanner, S. (2009) *Afghanistan.* Philadelphia: Da Capo.

[6] Marsden, P. (1998) *The Taliban.* Karachi: Oxford University Press.

significant improvement. Relatively stable Afghan currency, along with a workable banking system, and a speeding growth rate of 10% for the past five years, has emerged in a very short time. Improvements in energy distributions, access to health services, and education are visible. Six million Afghan children are now in school, two million of whom are girls. Health care has also become much more available: by one estimate 80% of the population now has access to basic health services[7].

Afghanistan, nevertheless remains deeply troubled by rising concerns about the capability of the Afghan state to provide for its citizens, and an awareness that the Afghan government and the international community has lost a great deal of momentum since the fall of the Taliban regime at the end of 2001[7]. Therefore, the fragmented Afghanistan in its diverse, heterogeneous composition, with a lack of democratic tradition, low economic development, as well as profound and complex social issues, especially in regards to opium production, still suffers from numerous impediments to the creation of a democratic, secure, and united nation[8].

B) ISIS

The Islamic State of Iraq and the Levant (ISIL(, also known as the Islamic State of Iraq and Syria or the Islamic State of Iraq and ash- Sham(ISIS)[9], or simply as the Islamic State, is an Islamic extremist rebel group controlling territory in Iraq and Syria, and, according to some sources, Libya and Nigeria. The group also has operations or affiliates in Lebanon, Egypt, and other areas of the Middle East, including Afghanistan[10].

On 29 June 2014, the group proclaimed itself to be a worldwide caliphate, with Abu Bakr al-Baghdadi being named its caliph[11] and renamed itself "Islamic State". The new name and the idea of a caliphate has been widely criticised and condemned, with the UN, various governments, and mainstream Muslim groups all refusing to acknowledge it. As caliphate, it claims religious, political and military authority over all Muslims worldwide and that "the legality of all emirates, groups, states, and organisations, becomes null by the expansion of the khilāfah's [caliphate's] authority and arrival of its troops to their areas". Many Islamic and non-Islamic communities judge the group unrepresentative of Islam.

The United Nations has held ISIL responsible for human rights abuses and war crimes, and Amnesty International has reported ethnic cleansing by the group on a "historic scale". The group has been designated as a terrorist organisation by the United Nations, the European Union, the United Kingdom, the United States, Australia, Canada, Indonesia, Malaysia, Turkey, Saudi Arabia, the United Arab Emirates, Syria, Egypt, India, and Russia. Over 60 countries are directly or indirectly waging war against ISIL.

---

[7] Cia.gov, (2015) *The World Factbook.* [online] Available at: https://www.cia.gov/library/publications/resources/the-world-factbook/geos/af.html

[8] NATO, (2015) *ISAF's mission in Afghanistan (2001-2014).* [online] Available at: http://www.nato.int/cps/en/natolive/topics_69366.htm

[9] BBC News, (2015) *What is Islamic State? - BBC News.* [online] Available at: http://www.bbc.co.uk/news/world-middle-east-29052144

[10] Cbsnews.com, (2015) *ISIS active in south Afghanistan, officials confirm for first time.* [online] Available at: http://www.cbsnews.com/news/isis-active-in-south-afghanistan-officials-confirm-for-first-time/

[11] The Independent, (2014) *Iraq crisis: Isis declares its territories a new Islamic state with 'restoration of caliphate' in Middle East.* [online] Available at: http://www.independent.co.uk/news/world/middle-east/isis-declares-new-islamic-state-in-middle-east-with-abu-bakr-albaghdadi-as-emir-removing-iraq-and-syria-from-its-name-9571374.html

The group originated as Jama'at al-Tawhid wal-Jihad in 1999, which was renamed Tanzim Qaidat al-Jihad fi Bilad al-Rafidayn—commonly known as al-Qaeda in Iraq (AQI)—when the group pledged allegiance to al-Qaeda in 2004. As Jama'at and later AQI, beginning in August 2003, the group participated in the Iraqi insurgency, which had followed the March 2003 invasion of Iraq. In January 2006, it joined other Sunni insurgent groups to form the Mujahideen Shura Council, which in October 2006 proclaimed the formation of the Islamic State of Iraq (ISI). The ISI gained a significant presence in the governorates of Al Anbar, Diyala, and Baghdad.

Under the leadership of al-Baghdadi, the ISI sent delegates into Syria in August 2011 after the Syrian Civil War began in March 2011. This group named itself Jabhat an-Nuṣrah li-Ahli ash-Shām or al-Nusra Front, and established a large presence in Sunni-majority areas of Syria within the governorates of Ar-Raqqah, Idlib, Deir ez-Zor and Aleppo. In April 2013, al-Baghdadi announced the merger of his ISI with al-Nusra Front, and announced that the name of the reunited group was now the Islamic State of Iraq and the Levant (ISIL). However, both Abu Mohammad al-Julani and Ayman al-Zawahiri, the leaders of al-Nusra and al-Qaeda respectively, rejected the merger. After an eight-month power struggle, al-Qaeda cut all ties with ISIL on 3 February 2014, citing its failure to consult and "notorious intransigence[12].

ISIL is known for its well-funded web and social media propaganda, which includes Internet videos of the beheadings of soldiers, civilians, journalists and aid workers, as well as the deliberate destruction of cultural heritage sites.

The group gained notoriety after it drove the Iraqi government forces out of key western cities in Iraq. In Syria, it conducted ground attacks against both government forces and rebel factions in the Syrian Civil War. It gained those territories after an offensive, initiated in early 2014, which senior US military commanders and members of the US House Committee on Foreign Affairs saw as a re-emergence of Sunni insurgents and al-Qaeda militants. This territorial loss almost caused a collapse of the Iraqi government that prompted renewal of US military action in Iraq[13].

ISIL's expanding claims to territory have brought it into armed conflict with many governments, militias and other armed groups. International rejection of ISIL as a terrorist entity and rejection of its claim to even exist have placed it in conflict with countries around the world.

The Global Coalition to counter the Islamic State of Iraq and the Levant (ISIL or Daesh), also referred to as the Counter-ISIL Coalition or Counter-DAESH Coalition[14] is a US-led group of nations and non-state actors that have committed to "work together under a common, multifaceted, and long-term strategy to degrade and defeat ISIL/Daesh". According to a joint statement issued by 59 national governments and the European Union, participants in the Counter-ISIL Coalition are focused on multiple lines of effort[15]:

---

[12] Washington Post, (2015). *Al-Qaeda backs away from radical fighters in Syria, Iraq.* [online] Available at: http://www.washingtonpost.com/world/middle_east/al-qaeda-disavows-any-ties-with-radical-islamist-isis-group-in-syria-iraq/2014/02/03/2c9afc3a-8cef-11e3-98ab-fe5228217bd1_story.html

[13] Encyclopedia Britannica, (2015) *Islamic State in Iraq and the Levant (ISIL) | militant organization.* [online] Available at: http://global.britannica.com/EBchecked/topic/1963547/Islamic-State-in-Iraq-and-the-Levant-ISIL

[14] Gulfnews.com, (2015) *Coalition commanders seek plan to counter Daesh advance.* [online] Available at: http://gulfnews.com/news/mena/iraq/coalition-commanders-seek-plan-to-counter-daesh-advance-1.1398681

[15] U.S. Department of State, (2015) *Joint Statement Issued by Partners at the Counter-ISIL Coalition Ministerial Meeting.* [online] Available at: http://www.state.gov/r/pa/prs/ps/2014/12/234627.htm

1. Supporting military operations, capacity building, and training;
2. Stopping the flow of foreign terrorist fighters;
3. Cutting off ISIL/Daesh's access to financing and funding;
4. Addressing associated humanitarian relief and crises; and
5. Exposing ISIL/Daesh's true nature (ideological delegitimisation).

Operation Inherent Resolve is the operational name given by the US to military operations against ISIL and Syrian al-Qaeda affiliates. Combined Joint Task Force – Operation Inherent Resolve (CJTF–OIR) is coordinating the military portion of the response.

The following multi-national organisations are part of the Counter-ISIL Coalition:

 European Union – declared to be part, most members are participating;
 NATO – all 28 members are taking part;
 Cooperation Council for the Arab States of the Gulf or GCC – all six current members and the two pending members, Jordan and Morocco, are taking part.

NATO's ISAF MISSION AND INTERNATIONAL ENGAGEMENT

In 2001, following the Bonn conference, the International Security Assistance Force (ISAF) was established under the authority of the United Nations Security Council (UNSC). Resolution 1386 authorised the establishment of the force to assist the Afghan government in the maintenance of security in Kabul and its surrounding areas – in particular to enable the Afghan authorities as well as UN personnel to operate in a secure environment[16]. The resolution stressed the need of all Afghan forces to adhere strictly to their obligations under human rights law, including respect for the rights of women, while reaffirming its strong commitment to the sovereignty, independence, territorial integrity and national unity of Afghanistan (UNSC Resolutions). The situation in Afghanistan was seen to constitute a threat to international peace and security, however, the operation was initially restricted to the Kabul area, and its command was assumed by ISAF nations on a rotational basis.

In 2003, following resolutions 1413, 1444 and 1510, on the situation in Afghanistan, NATO took command of ISAF as requested by the UN and the Government of the Islamic Republic of Afghanistan[16]. NATO was given the command, coordination and planning of the force, including the provision of a force commander and headquarters on the ground in Afghanistan, bringing the six month national rotations to an end[17]. Soon after, the UNSC mandated ISAF's enlargement outside of Kabul. This new leadership overcame the problem of a continual search to find new nations to lead the mission and the difficulties of setting up a new headquarters every six months in a complex environment. A continuing NATO headquarters also enables small countries, less able to take over leadership responsibility, to play a strong role within a multinational headquarters. Since then the ISAF mission has been enforced under Chapter VII of the UN Charter in around fifteen UNSC

[16] NATO, (2015) *ISAF's mission in Afghanistan (2001-2014).* [online] Available at: http://www.nato.int/cps/en/natolive/topics_69366.htm
[17] Jones, W. (2015) *History | Resolute Support Mission.* [online] Rs.nato.int. Available at: http://www.rs.nato.int/history.html

resolutions including 1386, 1413, 1444, 1510, 1563, 1623, 1707, 1776, 1817, 1833, 1890, 1917, 1943, 2011 and 2069[18].

ISAF's expansion beyond Kabul occurred in four stage[19]. Firstly, the ISAF expansion began with the takeover of the German led military component of the Provincial Reconstruction Team (PRT) in Kunduz, with the other eight PRTs under the US lead command of Operation Enduring Freedom[20]. Four other PRTs were established following the Istanbul Summit in 2004 in Mazare Sharif, Meymana, Feyzabad and Baghlan. After the completion of this first stage of expansion, ISAF extended over some 3,600 square kilometers in the north.

The second stage of expansion towards the west was announced in 2005[20]. It began when ISAF took on command of two PRTs and a logistic base, in the provinces of Herat and Farah. With the two newly operational PRTs in the Ghor and Badghis province the ISAF's expansion into the west was completed. With the competition of the northwest expansion, ISAF provided security and support for approximately 50% of the Afghan territories encompassing a total of nine operational PRTs.

Stage three of ISAF expansion was endorsed in 2005 and implemented in 2006 with the addition of four ISAF led meant to provide security and assistance to six southern provinces: Daikundi, Helmand, Kandahar, Nimroz, Uruzgan and Zabul[20]. This lead to a doubling of ISAF forces, as compared to the pre expansion level, and the expansion of ISAF lead to a total of 13 PRTs across Afghanistan.

The final stage of expansion occurred in 2006, with ISAF taking command of eastern Afghanistan from the US led international military forces. Following this wave of ISAF expansion, the NATO lead mission in Afghanistan included training and mentoring components for the Afghan National Army(Afghanistan International Security Assistance Force: Mission). This revised operational plan, along with the ISAF led PRTs, contributed to a situation some 87 percent of the population will soon live in areas under Afghan control. Liaising with the Afghan government, civil society, and representatives of the international community and neighboring countries, the Afghan people have been afforded a level of organization and security, which should permit the stable transition into a functioning democracy and a strong and independent Afghanistan. With the launching of "Inteqal", the Afghan National Security Forces are expected to undertake full security responsibility for Afghanistan by 2014. This shift will allow the ISAF to proceed with a revised operational plan in which the ANSF leadership will generate a shift from combat based to training, advising and assisting role[21].

EVALUATING THE INTERNATIONAL ENGAGEMENT

NATO's main goal in Afghanistan is to ensure that the Afghan authorities are able to deliver effective security across the country and make sure that the country can never again be a safe harbour

[18] Un.org, (2015) *Resolutions adopted by the United Nations Security Council since 1946.* [online] Available at: http://www.un.org/en/sc/documents/resolutions/index.shtml
[19] Jones, W. (2015) *History | Resolute Support Mission.* [online] Rs.nato.int. Available at: http://www.rs.nato.int/history.html
[20] NATO, (2015) *ISAF's mission in Afghanistan (2001-2014).* [online] Available at: http://www.nato.int/cps/en/natolive/topics_69366.htm
[21] ISAF's mission in Afghanistan (2001-2014) *ISAF's mission in Afghanistan (2001-2014).* [online] Available at: http://www.nato.int/cps/en/natolive/topics_69366.htm

for terrorists[22]. This is done through population centric counterinsurgency operations in partnership with ANSF. Aimed to decrease the ability and the will of the extremist revival, while maintaining the growth in aptitude of the ANSF essential for the successful provision of a secure and stable Afghanistan, these operations target both military and socioeconomic development of the region[22].

The NTMA, created in 2009, is an example of successful ISAF development in Afghanistan. Sponsored by 38 member and partner countries, the training mission brings national forces and international forces into one[22]. NTMA's key objectives include assisting in training the Afghan national security forces, aiding the ANA's training base, and the ANP reorganization at the region level and below. It places emphasis on improving the ANA enabling capability underperformances (close air support, medical evacuation, intelligence through 'train the trainer' programmes)[22]. The institutional training capability, combined with the ISAF's Joint Command (IJC) field component responsible for facilitating the development of fielded ANSF units, are key ISAFled initiatives in the process of transition to a more enabling 'Security Force Assistance' role. In a joint effort of NATO's Training Mission Afghanistan (NTMA) and ISAF's Joint Command (IJC), with the European Police Mission in Afghanistan (EUPOL) and the European Gendarmerie Force (EGF), ISAF offers support through mentoring, and training of the Afghan National Army (ANA) and the Afghan National Police (ANP)[22].

The Afghan National Army (ANA) and the Afghan National Police (ANP) and the Afghan Air Force serve as perfect examples of military progress in Afghanistan. Since its creation in 2002, the ANA comprises an army with both combat elements and capabilities such as military police, intelligence, route clearance, combat support, medical, aviation, and logistics[22]. The objectives of the Afghan National Police (ANP) are changing from countering the insurgency towards a noncombatant policing role, by further increasing capabilities from criminal investigations to traffic control. In the meantime, the Afghan Air Force now has over 150 skilled pilots and 96 aircrafts, including gunship, attack and transport helicopters and light aircrafts[22].

Reconstruction and development as well as humanitarian support is generated through PRT's in joint effort with the Afghan government and the United Nations Assistance Mission in Afghanistan (UNAMA)[22].

Nevertheless, even after 11 years of operation, Afghanistan is faced with ongoing socio economic troubles that threaten to destabilize the country, if not the entire region itself. Stressing the need for regional cooperation, many Afghans have expressed concerns over the potential re-destabilization of the post 2014 Afghanistan. The potential Taliban takeover of the post ISAF Afghanistan remains a very real threat to many locals. The close cooperation with regional security organizations, such as the Shanghai Cooperation Organization, ASEAN and OSCE, as well as further engagement with regional partners, especially Russia and Pakistan, is often perceived as one of the real solutions to the potential destabilization of the region.

[22] NATO, (2015) *ISAF's mission in Afghanistan (2001-2014).* [online] Available at: http://www.nato.int/cps/en/natolive/topics_69366.htm

PORSPECTIVE OUTLOOK FOR NATO

NATO led the International Security Assistance Force (ISAF) in Afghanistan from August 2003 to December 2014. Following a three-year transition process during which the Afghans gradually took the lead for security across the country, ISAF's mission was completed at the end of 2014. With that, Afghans assumed full responsibility for security. It is now fully in the hands of the country's 352,000 soldiers and police, which ISAF helped train over the past years. However, support for the continued development of the Afghan security forces and institutions and wider cooperation with Afghanistan continue.

The post ISAF Afghanistan will not be a NATO absent Afghanistan. The cooperation will occur along the previously reaffirmed Lisbon Declaration on Enduring Partnership. The enhanced capacity building and security sector reform cooperation between NATO and Afghanistan aims to promote the fight against corruption support the development of military and educational programs; support the Afghan civil aviation sector in meeting international standards; training in civil emergency planning and disaster preparedness; and public diplomacy efforts to promote a better understanding of NATO and its role in Afghanistan[23].

Successful transition to an independent, democratic and safe Afghanistan calls for a inclusive approach, comprising both civilian and military actors, directed not only at enhancing security but also at upholding good governance, the rule of law and long term progress. The importance of regional and international cooperation is crucial in understanding the complex nature of the transition[24]. Illustrative of this is NATO's close collaborative efforts numerous international partners, including the United Nations Assistance Mission to Afghanistan, the World Bank, the European Union etc. in regards to the ISAF mission[23]

Regional cooperation is probably the most important component of post ISAF transition. As NATO's ISAF forces will assume training and advisory roles, the insurance of pace, stability and security of Afghanistan is impossible without regional cooperation and coordination of efforts. Regional partners, such as Pakistan and Russia, share a mutual concern over the threat of extremism, drug trafficking and potential destabilizing effects of a weak and troubled Afghanistan. Illustrative of these are the contributions of these regional partners[25]. One of the major NATO supply routes into and out of Afghanistan lies south through Pakistan. Overflight rights and the leasing of military bases to individual Allies have been facilitated by NATO's regional partners including Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan. Kazakhstan and Uzbekistan (along with Russia, Belarus, and Ukraine) have facilitated rail systems for the transportation of non-lethal supplies along a northern Afghanistan[23]. Russia has been aiding the Afghan Armed Forces in the training, operation and maintenance of their helicopter fleet, and some 2000 Afghan, Central Asian and Pakistani counter narcotics personnel have been trained to date in counter narcotics initiatives. Russia remains a crucial partner in the expansion of the northern supply route as it permits for the transfer of nonmilitary equipment[23].

[23] NATO, (2015) *ISAF's mission in Afghanistan (2001-2014).* [online] Available at: http://www.nato.int/cps/en/natolive/topics_69366.htm

[24] ISAF's mission in Afghanistan (2001-2014) *ISAF's mission in Afghanistan (2001-2014).* [online] Available at: http://www.nato.int/cps/en/natolive/topics_69366.htm

[25] Jones, W. (2015) *History | Resolute Support Mission.* [online] Rs.nato.int. Available at: http://www.rs.nato.int/history.html

CONCLUSION

Afghanistan's transition to an independent, secure and stable government post 2014 is a challenging and complex topic to be explored. It necessitates a profound understanding of the contextual realities of the Afghan society. It is important to examine the historical, social and political impediments to a steady Afghan lead transition. One must ask what form should NATO's post ISAF mandate take? Should regional partnership be encouraged? Should NATO let other international organizations, such as the UN, take a lead in the post 2014 transitioning Afghanistan? How should NATO prepare for a potential threat posed by ISIS? Could cooperation with regional security organizations, such as the Shanghai Cooperation Organization, and OSCE, as well as further engagement with regional partners (such as Russia and Pakistan) contribute to NATO's follow on mission to support the development of ANSF capacity? In order to prevent a potential relapse of the Taliban influence in Afghanistan, should NATO mandate, promote or utilize Muslim assets for a steady and lasting transition to a democratic Afghanistan?

RESEARCH QUESTIONS

These are the questions that member States should address during their debate in the General Assembly:

1) In the light of the concluding ISAF mission, what should NATO's mandate regarding operation and presence post 2014 be?
2) Recognizing the need for efficient and integrated strategic planning and Smart Defense what should be NATO's minimum engagement in post 2014 Afghanistan?
3) Could cooperation with regional security organizations, such as the Shanghai Cooperation Organization, and OSCE, as well as further engagement with regional partners (such as Russia and Pakistan) contribute to NATO's follow-on mission to support the development of ANSF capacity?
4) Analyzing and assessing the newly posed threats by ISIS and the effect that they might have on the situation in Afghanistan post 2014.
5) In the interest of cultural significance, should the mandate promote the utilization of Muslim assets for a steady and lasting transition to a democratic Afghanistan?

III. TOPIC B: THE ROLE OF NATO IN THE BUILDING OF AN INTERNATIONAL CYBER WARFARE COMBAT SYSTEM

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."
Bruce Schneier
(American computer security specialist)

INTRODUCTION

In recent years, cyber attacks have become a matter of concern to State, because they can pose a serious threat to national security, as well as to foreign and military policies. It's generally acknowledged that the amount of these cyber attacks will continue to increase. In the mean time, the need of trillions of devices and petabytes of data to be processed and transferred worldwide means that we have to deal with new threats and vulnerabilities, plus facing the remaining old ones.
Nowadays, cyber warfare, cyber terrorism, cyber espionage and cyber activism challenge our technology. Consequently, effective cyber defence will be more and more important.

For the time being, cyber attacks have never provoked death of physical damage to anyone but the undertaken offensive and defensive strategies to combat cyber terrorism might cripple economies in the long run view. Instead, cyber crimes have a vast economic costs, estimated at between US$300 billion and US$1 trillion. It is causing huge losses for businesses and managing to steal sensitive data of government organizations, so it's worsen the economy as a whole.
Some cyber attacks have be economically driven (i.e. on the EU's carbon Emission Trading Scheme), while others have been directed to the military, such as the attack to the Estonian Ministry of Defence back in 2013. However, the most frequent cyber attacks were launched between China and the US, followed by North Korea targeting South Korea. [26]

This issue lacks of an universally accepted definition. A possible definition is provided by the CIA, which regards terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents."
Moreover, the definitions surrounding 'cyber war' and 'cyber defence' are still widely debated.
According to the common opinion, cyber warfare is the unauthorized conducting of a penetration by, on behalf of or in support of, a government into another nations' computer system with the aim of adding, altering or deleting data, or causing any other king of damage.[27]

The following general patterns of a Cyber War can be identified:

1) Cyber Espionage: hackers need to obtain as many secrets as possible from your opponent (i.e. social network analysis, sniffering, conventional spies) to gain control of the victim's resources for a financial, military, social or political advantage;
2) Preparation: attackers need to know the versions of the webservers and potential exploits in order to do the defacing of the web-site or any other useful information to reach their goals;

[26]Homeland Security, (2015) *Cyber security Overview* [online] Available at: http://www.dhs.gov/topic/cybersecurity
[27] Cyber Defense Magazine, (2015) *General updated information* [online] Available at: http://www.cyberdefensemagazine.com/

3) Cyber Attack: reach the targets. From the government agencies to news media, anything can fall under cyber attacks, especially small companies, which have recently become their preferred victims due to their rudimentary security measures. Even well protected security infrastructure such as the Pentagon seems to be vulnerable. When it comes to private sector, the main goal of attacks intellectual property (industrial espionage), whereas attacks against government agencies aim for strategic intelligence, sensitive security data or in general the disruption or destruction of private and public networks

Cyber terrorism, or more general cyber attacks, might be pursued by private groups to gain visibility and media resonance, targeting a focused objective and advancing political or social claims through violence and fear. Also a state may make use of cyber terrorist attacks to advance its interests.
Moreover, cyber attacks might come in the form of so-called hacktivism (i.e. Anonymous), the new way of protest and "civil disobedience".
Cyber attacks have been labelled as the war in the "fifth dimension" or "fifth domain".[28]

HISTORICAL DEVELOPMENTS

It is essential that information does not fall into the wrong hands of those who want to use for destruction, which some claim to cross the line into warfare. [29]

Here's a list of the *major cyber-incidents* in the past few years:

- (2007) DDoS attacks against the Estonian government led to paralysis of public services in Estonia for three weeks.
- (2008) Media and government websites in Georgia came under attack from hackers.
- (2010) The 'Stuxnet' computer worm, one of the most sophisticated cyber weapons, damaged uranium enrichment centrifuges at Iran's Natanz nuclear site.
- (2012) A DDoS campaign against the US financial sector, claimed by the group 'Izz ad-Din Al Qassam', but it is suspected that Iran was behind it
-

Although these incidents **have not been attributed to any particular State**, analysts believed that State actors sponsored them. Even in the conflict in Ukraine or against NATO (2014), cyber attacks might have been used.

However, there are examples of **non-state sponsored** cyberterrorist attacks:

- (1982) A computer control system stolen from a Canadian company by Soviet spies caused a Soviet gas pipeline to explode. It's considered a logic bomb, that is a piece of code that changes the workings of a system, which changed the pump speeds to cause the explosion.
- (1996) A computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts Internet Service Provider (ISP) and damaged part of the ISP's record keeping system in order to send out worldwide racist messages under the ISP's name.
- (1997-1998) An e-mail bombing campaign was launched against the Institute for Global Communications (IGC), a San Francisco–based ISP that hosted the web pages of *Euskal Herria* (in English, the *Basque Country Journa*l), a publication edited by supporters of the Basque separatist group ETA. The attackers bombarded the website with thousands of e-mails.

[28] NATO, (2015) *Cyber Security* [online] Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm
[29] Hackmageddon.com, (2015) *1-15 April 2015 Timeline cyber attacks* [online] Available at: http://hackmageddon.com/category/security/cyber-attacks-timeline/

- (1998) Ethnic Tamil guerrillas attempted to disrupt Sri Lankan embassies by sending large volumes of e-mail to disrupt their communications.
- (1999) Business, public entities, and academic institutes in NATO member states received virus-laden e-mails from computers located in Eastern European countries.
- (2013) Media companies, such as The New York Times, Twitter and The Huffington Post lost control of some of their websites Tuesday after Syrian hackers breached the Australian Internet company that manages many major site addresses.
- (2015) at least three official German websites, including the chancellor's and the website of the Bundestag, were inaccessible due to a cyber attack performed by a Russian-speaking group based in Eastern Ukraine, Cyber Berkut, They demanded that Germany addressed financial and political support for the Kiev government.
- (2015) Hackers claiming allegiance with the Islamic State took control of the Twitter account of the United States military's central command to post threatening messages and propaganda videos, as well as military documents.

On the other hand, about 100 countries have been sponsoring both offensive and defensive cyber attacks. Sadly, always more often States use the new cyber tools to attack other States or non-state actors (i.e. terrorist organizations).[30] It's more than predictable the usually States deny direct involvement but there are several examples of **state-led attacks**:

- (2003) The Titan Rain, coordinated attacks on American computer systems both sensitive private and public networks, which were infiltrated by the hackers, such as those at Lockheed Martin and NASA. Military intel and classified data were stolen, but also thousands of "zombified" machines, i.e. computers infiltrated by malicious software that can be activated later. It is believed that it has been organized or supported by the Chinese government
- (2012) Experts discovered a computer virus dubbed Flame, active in the Middle East-targeting Iran in particular - like Stuxnet, but used as an espionage tool.
- (2013) The New York Times reported a set of cyber attacks against U.S. financial institutions (JPMorgan Chase, Wells Fargo, American Express), performed by an Islamic non-governmental group, but investigations claim that the Iran might be behind it.
- (2013) Up to 32,000 computers of South Korean financial institutions. North Korea was called responsible for the attack, after it openly declared that it was targeting its neighbor to the south to cause economic damage.
- (2014) The North Korean hackers attacked Sony.

It is clear that the difference between non-State-led and State-sponsored cyber attacks is very slight because the attacks basically follow the same techniques. Moreover, some non-State actors act on behalf of a Sate. It is the international community should also decide when a government becomes responsible for the actions of private actors.

CURRENT DEVELOPMENTS

Cyber security

Cyber attacks are designed so that it's difficult to trace and uncover them, while attackers can easily disrupting or stealing from systems. Hackers use a variety of methods to distort the track back to their IP address.

[30] Nato Parliamentary Assembly, (2014) *Cyber Space and Euro-Atlantic Security* [online] Available at: http://www.nato-pa.int/default.asp?SHORTCUT=3528

Unfortunately, antivirus software, such as McAfee, Kaspersky and Symantec, may not be 100% able to eradicate all possible viruses. [31]

One of systems created with the purpose of protecting state and non-state actors from cyber terroristic attacks is **Early Warning System**. Its vision is to protect national security through responsible information sharing so organizations and States can learn, prepare, and hopefully defend themselves against similar attacks
However, the mission of this system goes beyond the advance responsible information sharing to further counterterrorism and homeland security and cybersecurity missions. Indeed, it aims to improve nationwide decision making by transforming information ownership to stewardship and promote partnerships across federal, state, local, and tribal governments, the private sector, and internationally.

Basically, the entire Early Warning System might be summarized as follow:
DETECT → MITIGATE AND RESPOND → RECOVER → PROTECT AND PREVENT →
back to DETECT as an endless lifecycle.

Currently, besides this system, two fundamental techniques are used for network-based intrusion detection: misuse detection and anomaly detection.

1) The first one includes the *signature based group* of systems and it's the most common type of intrusion detection system (IDS) and widely in use.
2) The second one is based on *anomaly detection* and it is realized by the measurement of the current state of the system and the comparison to the values gained from the model.

Also combinations are possible, for example the application of Evolutionary Algorithms in Data Mining Systems. This type of IDS is also called Network Behavioral Analysis (NBA). An enhancement of NBA systems is called Network Situation Awareness (NSA), where visualization and high-level data management are included to the process of network monitoring.

Due to increasing number of technological progress, it's very difficult to keep the current systems updated and it's unlikely that further systems will not be manageable.
Cyber defence has been defined as 'the application of security measures to protect against, and react to cyber attacks against communications and command systems infrastructure.'
Many new measures regarding cyber defence have been included in national defence planning and budgets, including the development of offensive cyber capabilities.
47 States give a role to the armed forces, while 67 states only have civilian programmes. [32]
The US, UK, China, Russia and France are the most advanced in terms of cyber power and cyber capabilities. [33]

NATO Cyber Defence Management Authority (CDMA)

The new Cyber Defence Management Authority in Brussels represents the way to centralise cyber defence operational capabilities among the Allies, providing a centralised procedures for coordinating member responses. This authority's precise capabilities are still not that clear, but it surely contains advanced electronic monitoring capabilities for sharing critical cyber intelligence in real-time. It is

[31] NATO, (2015) *Cyberspace Security: Official Texts* [online] Available at: http://www.natolibguides.info/cybersecurity/documents
[32] U.S. DoD News, (2015) *Cybercom Chief Discusses Importance of Cyber Operations* [online] Available at: http://www.defense.gov/news/newsarticle.aspx?id=128583
[33] New York Times, (2015) *U.S. Demands China Block Cyberattacks and Agree to Rules* [online] Available at: http://www.nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set-cyber-rules.html?pagewanted=all&_r=2

expected to evolve into a war-room operation for NATO to improve e a 'coalition of the willing' among the member States. [34]

International and national laws

As article 2.4 of the Charter of the United Nations states "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.", The use of any kind of force to settle international disputes is condemned.
States may also be responsible for attacks carried out by private agents within them.
However, the existing body of international law concerning cyberterrorism and cyber-security specifically is limited. So far, only national laws have cyber-attacks and they differ from one another.

International laws consist in both *ius ad bellum* (the rules governing international armed conflict) and *ius in bello* (the way in which war is waged, namely international humanitarian law).
The Tallinn Manual process was a step towards governing cyber warfare. It defines state responsibility in cyber operations contrary to International Law, according to the principle of prohibition of the use of force, potential self-defence, etc. Cyber operations alone might cross the limit of international armed conflict, as a cyber operation can be considered as in self-defence only if the conditions of a cyber armed attack ('use of force' resulting in serious physical injury and damage) are met.
These rules remain open to interpretation.
Finally, there is an ongoing debate whether it is possible for a state to violate the cyber-space of another country in order to attack a non-state actor. Someone claims that the violation of a state's cyber-space is acceptable when that state is really unable or unwilling to combat an international cyber-terrorist organization. On the other hand, many others think that any foreign intervention in a country's cyber-space is only a violation of the basic principles of sovereignty and non-intervention.

POTENTIAL FUTURE DEVELOPMENTS:

Although cyber security is a priority in the European internal security strategy, EU action has been limited, due to the reluctance of Member States to cooperate with each other. It is moving forwards a comprehensive approach to cyber security, focusing on defining the legal and operational framework of this cooperation. A huge number of strategic priorities in this field is included the Common Security and Defence Policy (CSDP) with the purpose of building cyber defence capabilities in the MS, promoting civil-military dialogue, as well as dialogue with international partners, including NATO. [35]

According to the *EU Concept for Cyber defence in EU-led military operations*, member States are supposed to maintain situational cyber awareness.
Experts believe that military cyber defence at European level is not properly developed yet so a series of actions should be taken at EU level. This means that enhancing network protection, strengthening intelligence and incident response capabilities, creating a culture of cyber-security, and reinforcing links between NATO and the EU must be at the top of the agenda of member States.
Other similar key areas are the development of cyber-defence training and education initiatives; information exchange, as well as sharing facilities.

[34] Department of Defense, (2015) *DoD's Three Primary Cyber Missions* [online] Available at: http://www.defense.gov/home/features/2015/0415_cyber-strategy/
[35] Global Research, (2015) *Pentagon Partners With NATO To Create Global Cyber Warfare System* [online] Available at: http://www.globalresearch.ca/pentagon-partners-with-nato-to-create-global-cyber-warfare-system/21366

When it comes to training and awareness, EDA, the *European Defence Agency*, is currently working on specific projects to reach solutions against malwares and for cryptography and protection of information.

The role of the European Council [36]

The European Council called for an *EU Cyber Defence Policy Framework* to be set up in 2014. This would include concrete projects focused research and technologies, reinforced protection of communication networks, mainstreaming of cyber security into EU crisis management.
The key points of this document are the following:

1) Supporting the development of Member States cyber defence capabilities related to CSDP. MS should act as a security providers both at the international level and the neighbourhood. Therefore, they need to enhance their own security and their global strategic role by cooperating against cyber attacks.
2) Enhancing the protection of CSDP communication networks used by EU entities
3) Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector.
4) Improve training, education and exercises opportunities, which also contribute to jobs, growth and innovation across the EU and can enhance Europe's strategic autonomy.
5) Enhancing cooperation with relevant international partners, such as NATO, who share with the EU common values and principles and are able and willing to support EU crisis management efforts. This is highly relevant due to the institutional framework and decision-making autonomy of the EU. It notes that priority should be given to cooperation with partners.

This policy should take into account the competences of Member States and their shared needs assessments and risk analyses. This initiative has a flexible geographical scope of the initiative, as the cases on Mali and Somalia show (early 2015) as well as the follow up on the Conclusions of the European Council of March 2014 to strengthen the African Peace and Security Architecture;
There the challenge, though, to find and retain high-quality cyber specialists for the armed forces.
Finally, the basic premise of cooperation in cyber defence is that MS trust each other and are aware of their shared interests in cooperating in this matter.

Today, the Council is working on the adopted *Policy Framework for Systematic and Long-Term Defence Cooperation*, which is in line with the European Council Conclusions. It puts forward in full coherence with existing NATO planning processes, which provides an assessment of the critical military deficits with the aim of supporting national capability planning, identify the abilities required and look for collaborative opportunities.
Another priority is a more structured approach to cooperation between the CSDP missions and operations other actors, notably the EU Agencies (EUROPOL, FRONTEX and CEPOL) and with INTERPOL as well as the European Gendarmerie Force. This will cover other relevant issues such as illegal migration, organised crime, terrorism, foreign fighters and cyber security and it will help to identify gaps to establish a list of generic civilian CSDP tasks.
In May 2015, the Council will discuss upon CSDP in order to enable the European Council to take stock of progress and provide further guidance in June 2015.

[36] Council of European Union, (2015) *Outcome of Proceedings* [online] Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

The future of Early Warning System

To respond to the disruptive e-market, which is taking shape on an international scale, an efficient and cooperative *Early Warning System* for potential future networks.
Nowadays, security actions between private system providers is very marginal, which means that no encryption is done or mostly only partial when it comes to heterogeneous networks.
Anomaly detection, which is a very powerful instrument for intrusion detection, is only possible for subnetworks, while current Early Warning Systems are based on the analysis of log-files, flow-information or packet counting.

To overcome these deficits, an efficient EWS needs to be based on network virtualization and on the use of virtual sensors, new reasoning models, new developed learning algorithms and a sophisticated correlation of data, also taking into account security management aspects.
These systems are crucial for an effective risk management in firms and for national homeland security systems. The priority for the new Early Warning System is to overcome those gaps that make State-of-the-Art Intrusion Detection Systems possible. [37]

WHY IS NATO INVOLVED?

NATO put cyber defence on its agenda following the 1999 cyber attacks against NATO during the Kosovo war. Its main mission remains securing its own networks, although it aims also to ensure a minimum level of cyber defence to all Allies and reduce vulnerabilities in their critical infrastructure.
At the NATO Summit in Wales, in September 2014, the Allies claimed an enhanced cyber defence policy to create partnerships with industry, help individual States to improve their capabilities in the cyber world and focus more on training and education.
NATO's political power remains focused on its own networks as any agreement has been signed yet to allow NATO to deploy to help member States.

Many multinational projects have been undertaken to advance MSs' cyber defence capabilities on multinational basis, that is for all NATO members, sharing technical information and awareness of threats and attacks and advanced cyber-defence sensors.
Moreover, cooperation and information-sharing have been recognised as very helpful.
In June 2014, the creation of a new NATO military cyber warfare training centre in Estonia was approved. The importance of cooperation on cyber defence, such as joint exercises, exchange of best practices and mapping the extent of cyber attacks is essential.

The cyber world has become a new hot-spot for a variety of conflicts between companies and between governments. It is called "the new cold war" for either the vast potential for serious arguments between specific countries (i.e. China and the U.S.) or the deliberate missions to explicitly declare the States responsible for cyber attacks to avoid legal and diplomatic issues.
In short, there remains the urgent need to reach a solution on a multilateral level in order to find international agreements to face the issue in a fast and proper way and to provide the necessary legally binding framework for everyone in the global cyberspace.

[37] BBC news, (2015) *Web War II: What a future cyberwar will look like* [online] Available at: http://www.bbc.com/news/magazine-17868789

RESEARCH QUESTIONS

These are the questions that member States should address during their debate in the General Assembly:

1) Should cyber terrorism be considered as an act of armed conflict? If yes, should it be treated as every other terrorist attack?

2) Considering the worst scenario, should State actors allow humanitarian organizations to govern cyberspace?

3) Is it possible to build a legal binding framework to govern cyberspace upon which every State actors agree?

4) Should the UN establish a new committee with the purpose of dealing with the peaceful use of the cyber world as well as coordinating States' action and resources against cyber-terrorism?

5) What are the steps to follow in order to regulate the activity of governments to ensure international information security and avoid the violation of international peace and security, while guaranteeing the free exchange of technology and the respect of the sovereignty of States?

6) Is it possible to find an alternative to offensive operations, which can potentially cripple economies, change political views, instigate conflicts?

7) Is it possible to equalize technological capacities of nations?

8) Can a state take action in the cyber world of another country for the sake of protecting itself? Would it be a violation of state's sovereignty?