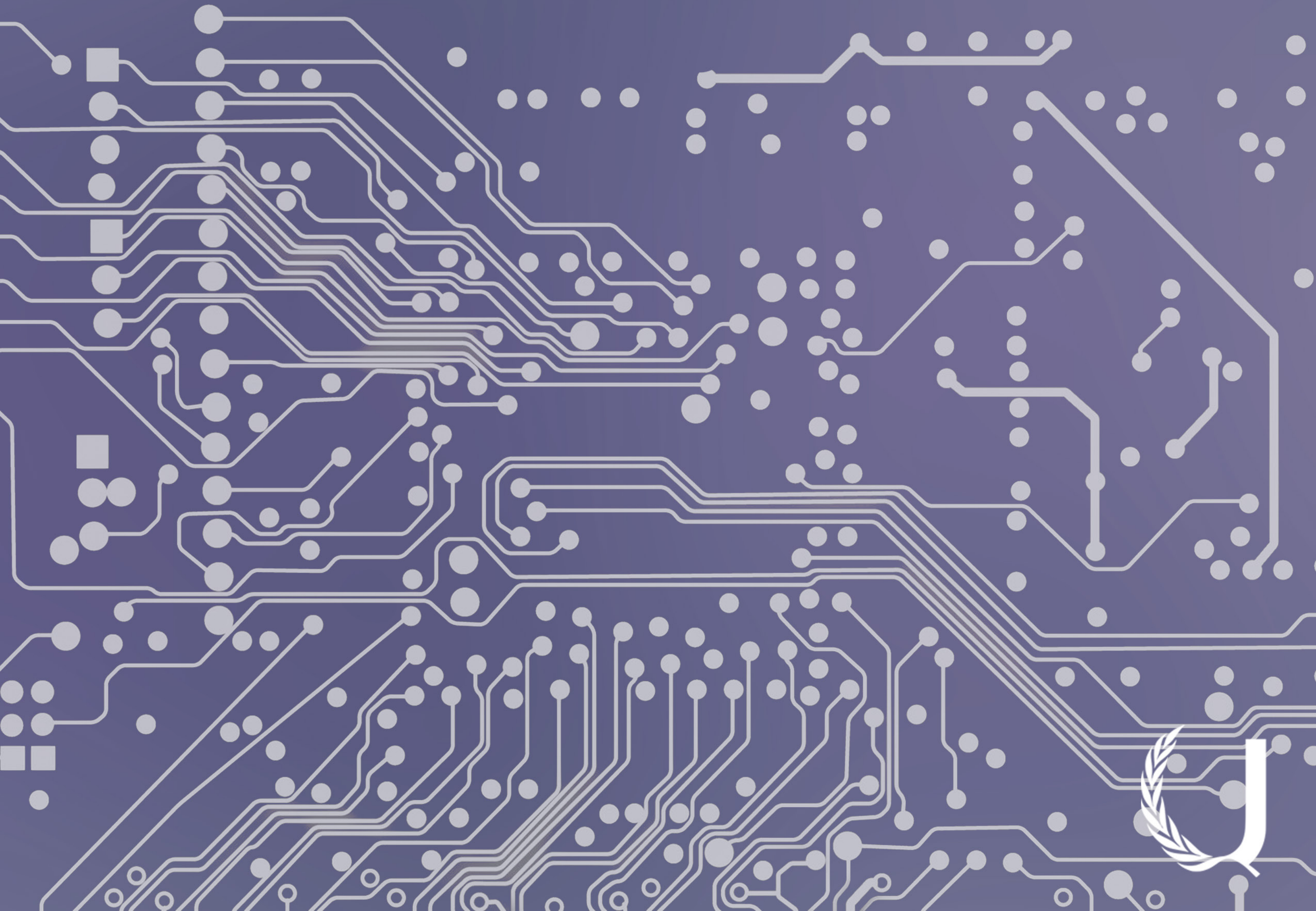
DISEC

DELEGATE BACKGROUND GUIDE



Staff

DIRECTOR:
Hasan Babar Matin

VICE-DIRECTORS:
Tasneem Gedi
Maya Mouilleron,
Michaella Ladha

MODERATOR:
Mattea Powell

A Letter From Your Director...

Dear delegates,

Welcome to UTMUN! Whether this is your first committee, or your tenth, I hope that you get everything you're looking for out of a MUN experience.

My name is Hasan and I'll be your director. I'm currently in my 2nd year of study at university, pursuing a degree in Financial Economics. I am a passionate member of the MUN community here at the University of Toronto and hope to create a dynamic and engaging committee for all of you.

Of course, I can't run a committee on my own. A dedicated team is behind every committee and we've been working hard to create an inclusive environment for you to improve your debate skills. However, you MUN experience is ultimately what you make of it. Bring your ideas to the table, research your position and speak to your fellow delegates. If you have any questions, please get in touch and I'd be happy to help.

It's going to be a fantastic conference and my team and I look forward to meeting you all this February!

Best Regards,

Hasan Babar Matin
hasan.matin@mail.utoronto.ca

CYBER SECURITY

Photo: NBC

Background

The emergence of the internet in the early 1990's has progressed from an obscure concept of computers being linked through a network in 'cyber-space', to today, being an entire way of life, a seemingly boundless and increasingly complex medium. The telecommunications revolution is believed to be one of the most powerful changes in the rise of non-state actors. "Instantaneous access to information and the ability to put it to use multiplies the number of players who matter," and in turn, breaks down governments' monopoly. This has given rise to far-reaching cybersecurity issues and questions regarding cybercrime and online freedom; protecting nations from attacks and building ethical frameworks of right and wrong. The Internet remains essentially borderless, meaning an actor can take actions in one country that could have potential outcomes in another without crossing any actual territory. Cybersecurity is the collection of policies, safeguards and security concepts to help mitigate the risks of exploiting national and international jurisdictions. The need for international co-operation (international recognized procedures, regimes) is therefore very pertinent since cybersecurity is a global threat.

Cybersecurity is separated into two principle streams adopted by the United Nations. The first is politico-military, which includes defending against cyber-warfare, and the unauthorized penetration of a government into another nation's network. DISEC is the primary UN body where these acts are discussed. The second stream is economic, including acts of cyber-crime and the criminal misuse of information technologies, and is generally not under the purview of DISEC.

Certain nations play a crucial role in how the international community handles cyber-warfare. The United States is pushing for broader cooperation on the crime-fighting level, in hopes of limiting Russia's capabilities, whereas Russia is calling for cyber arms control. Germany, Canada, and the United Kingdom have also played an active role funding various research projects and expert groups.

ROLE OF THE UN

Information security has been on the UN agenda since the Russian Federation in 1998 first introduced a draft resolution. The General Assembly has seen a lot of activity in the development of norms to govern behaviour of member states. Significant work is done by a multitude of UN organizations regarding cyber-security. DISEC has primarily dealt with the politico-military stream (cyber-warfare) and the following organizational platforms:

The United Nations Institute for Disarmament Research (UNIDIR)

- Raising awareness of the issue among diplomats and sparking further multilateral discussion
- Internet governance
- Cyber-terrorism
- Critical infrastructure protection and information assurance
- Legal issues
- Military aspects

The International Telecommunications Union (ITU)

- Responsible for practical aspects of cyber-security such as treaty organization
- The use of a matrix to compare the legal provisions of laws in various countries in regard to the development of cyber-crime legislation to harmonize cyber-crime laws.
- Sets technical standards around smart grid infrastructure

- Autonomous norm entrepreneur
- "International framework for cyber-security"

Proposals include:

1) Developing model legislation for member states to adopt
2) Creation of a "Cyber-Security Readiness Index"
3) Framework for national infrastructure protection, conceptualization of culture of cyber-security

The ITU is in collaboration with The World Federation of Scientists on the advancement of cyber-peace with the "elimination of the restrictions of free-flow of information, ideas and people," that of which add suspicion and animosity in the world.

THE COUNTER-TERRORISM IMPLEMENTATION TASK FORCE (CTITF)

The Working Group on Countering the Use of the Internet for Terrorist Purposes focuses on state's perception of cyber-security threats and understanding how the Internet can be used by terrorists.

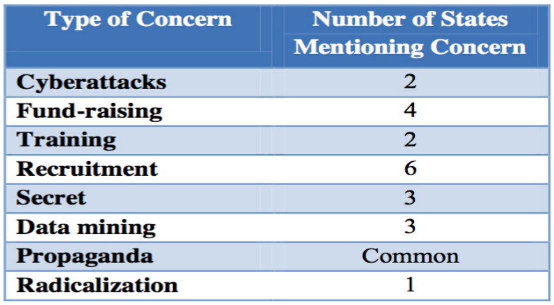
The CTITF has established the following four goals:

I. Identify and bring together stakeholders and partners on the abuse of the Internet for terrorist purposes, including using the web for radicalization, recruitment, training, operational planning, fundraising and other means

II. Explore ways in which terrorists use the Internet

- E.g. Removing or altering information on computer systems, disrupting flow of data, the stealing of information, disseminating content relevant to advancement of terrorist purposes

III. Quantify the threat that this poses and examine options for addressing it at national, regional and global levels



Type of Concern	Number of States Mentioning Concern
Cyberattacks	2
Fund-raising	4
Training	2
Recruitment	6
Secret	3
Data mining	3
Propaganda	Common
Radicalization	1

Data collected by the UN in February 2009 from 31 anonymous member states

IV. Examine what role the United Nations might play.

Current Conditions

UN's position:

Each year, the UN appoints members to the Group of Governmental Experts (GGE) to examine the existing and potential threats from the cyber-sphere and then reports to the UN General Assembly (GA). Each year the Secretary-General of the UN submits a report to the GA, which provides the views of UN Member States on the issue.

Experts from the following 20 member states participated in the GGE in 2015:

- Belarus
- Brazil
- China
- Colombia
- Egypt
- Estonia
- France
- Germany
- Ghana
- Israel
- Japan
- Kenya
- Malaysia
- Mexico
- Pakistan
- Russian Federation
- Spain

- U.K.
- U.S.A.

The 2015 GGE Report is considered significant because it achieved consensus on key aspects of cyber security including recommendations from major players on norms of behaviour, thus highlighting aspects of international law.

Key findings:

- In their use of information and communication technologies (ICTs), States must observe, amongst other principles of international law, state sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.
- Existing obligations under international law are applicable to state use of ICTs and states must comply with their obligations to respect and protect human rights and fundamental freedoms.
- States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts.
- The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible state behaviour.

The UN GA unanimously adopted the resolution of the outcome of 2014/2015 GGE, and in 2016, a new GGE was established that would report to the General Assembly in 2017.

OTHER IGOs

The North Atlantic Treaty Organization (NATO) runs the NATO Cyber Defense Centre of Excellence. Its mission is "to enhance the cooperation and capability of information sharing among NATO, NATO nations and partners in cyber-defense by virtue of education, research and development, lessons and consultation."

The key objectives of the European Union's policies on cyber-security include increasing cybersecurity capabilities and cooperation among all EU members, making EU a stronger player in cybersecurity, and mainstreaming cybersecurity in EU policies.

Case Study

A Cyber-Attack on Deutsche Telekom. This attack is one of cyber-crime nature, thus falling under the politico-military stream that DISEC deals with.

> In September 2012, Deutsche Telekom AG, a large German Internet Service Provider (ISP) was attacked by unknown adversaries. The attack was a Denial-of-Service (DoS), meaning that it was an attempt to block the Domain Name System (DNS) of the provider. There are several DoS attacks reported daily, worldwide. These attacks can last from as long as 1 hour to several months. The criminals carrying out the attacks do so for reasons such as political involvement, patriotic reasons, personal attacks against governments, organizations, companies, protest movements, extortion etc. DoS attacks lead to loss in revenue, tarnishing of reputation and infrastructure, and disruption of supply of essential goods and services to a state's population.
>
> Outcome:
>
> The German Federal Crime Office became involved in the response to the attack and they were able to recognize that the attack was targeting a critical infrastructure. The final remark to take away is that every single provider worldwide should be made aware of the threats to their DNS and prepare the necessary counter measures as well as establishing national and international contact points between ISPs and government agencies who may be able to stop an ongoing attack. Taken from their report, the German Federal Crime Office stated, "The Internet is a critical infrastructure. Its availability is essential for the functioning of a society and economy. Its outage can cause serious negative effects on almost all areas of life and can even inflict real damage in the physical world. Therefore, its protection should be an important goal for governments in every country."

Questions

1) Are "warfare" or "crime" adequate terms to describe certain actions in cyber-space?
2) How can you use the expertise and efforts of the various initiatives best while trying to avoid pitfalls of the past? Can you potentially adopt more network like structures given the small number of staff and geographic disparity?
3) What right do nations have to perform espionage through the internet, and other covert activities?
4) What may be some unanticipated consequences of UN organization's missions?
5) How are activities at the UN linked to activities at the EU, NATO, OECD, ASEAN?

Bibliography

Fischer, Eric. “Cybersecurity Issues and Challenges: In Brief.” Congressional Research Service. August 12, 2016.

“Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations General Assembly. July 22, 2015.

Maurer, Tim. “Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security.” Belfer Center for Science and International Affairs Harvard Kennedy School. September, 2011.

“Developments in the field of information and telecommunications in the context of international security.” UNODA. 2015.

“Cybersecurity” European Commission – Digital Single Market, Digital Economy and Soceity. June 7, 2016.

“ International Case Report on Cyber Security Incidents – Reflections on 3 cyber incidients in the Netherlands, Germany and Sweden.” Federal Office for Information Security, Germany. November, 2014.

Mathews, Jessica. “Power Shift.” Council on Foreign Relations. February 1997. https://www.foreignaffairs.com/articles/1997-01-01/power-shift

INTRODUCTION TO ISSUE

Drones are unmanned aerial vehicles (UAVS), which can be controlled remotely by pilots, or autonomously from a pre-programmed mission. There are many different drones (approximately a dozen) but they mainly fall into two categories: those that are used for surveillance purposes and those that are armed with missiles and bombs.

Drone warfare has become an important aspect of modern day warfare. Putting soldiers directly in combat zones has become far less common, and nations can establish their superiority from above with these drones. Nations choose to use drones because their enhanced surveillance capabilities reduce the likelihood of harming anyone than the intended target.

The first drone strike occurred in February 2002, when the CIA launched a Predator drone towards Paktia, a province near the city of Khost in Afghanistan targeted at Osama Bin Laden, leaving many civilian casualties. Nevertheless, drone warfare has dramatically increased, as it is a low-cost and low-risk form of defense. Drone warfare has continued to expand, but remains widely controversial because it raises humanitarian, legal, and other concerns.

86 countries have some level of drone capability, but the main ones are:

1) USA
2) Israel
3) The United Kingdom
4) Russia
5) Pakistan
6) Iraq
7) Nigeria

8) Iran

9) Turkey

10) Hezbollah (nonstate actor)

CURRENT CONDITIONS

Drone warfare has recently increased due to the transnational terrorist threat. Recently, countries like the United States have targeted drones at suspected ISIS occupied locations, but with a limited ability to avoid civilian deaths. For instance, the Syrian town of Aleppo was recently severely bombed; the initial target was military bunkers but there were still a lot of causalities from these drone strikes. Furthermore, Europe has recently taken a larger role in drone warfare. It used to mainly concern the USA, but now it has expanded to countries like Germany and France as these European countries now also want drone technology. They have requested the US to share their resources.

The problem with drone warfare is its regards to international law. Indeed, drone warfare doesn't actually fit a clear categorisation so it cannot be punished by international rule of law. Technically, they are not 'rule breaking', which makes their abuse even more problematic. There can be many surrounding factors (like self-defence), which makes their deployment defendable. Thus, any framework a government desires can justify drone strikes.

There are also many blurred lines on what determines this type of warfare. For example, the USA does not provide evidence to their strategy in drone proportions or what they consider necessary. In addition, they supposedly claim to only attack sovereign states (when they are facing an internal threat) but the consent of those states remains, to this day, quite ambiguous.

ROLE OF THE UN

- The UN Charter states to agree to "settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered" and to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state".
- The Security Council identifies that if "any threat to the peace, breach of the peace

or act of aggression" may make a state legitimately able to "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security" (member states can then pass a resolution to carry out force).

- Article 51 of the Charter gives importance to self-defence if a member state feels threatened.
- The Security Council also authorizes that any act of international terrorism gives rise to a right of self-defence and calls upon UN member states to collaborate "to prevent and suppress terrorist acts".

ISSUES AND QUESTIONS TO CONSIDER

Drone warfare is a challenge because there is no adequate law that can judge it. These weapons are not unlawful in themselves but their use is dependent on a very limited international law. It also takes into account a moral dilemma, where no human rights law can judge their use.

- Are the statements from the UN a sufficient legal basis to justify air strikes
- Do terrorist attacks impact the right to use force in a self-defence context?

•To what extent can drone strikes be lawful?

•Does the UN's have a sufficient international rule of law?

•What other laws could be implemented in order to prevent civilian deaths?

•Should there be a specific legislature regarding drone transparency?

•What makes drone strikes ethical and necessary?

•What is the ratio between a terrorist attack and a subsequent mass drone attack?

•Does UN law apply to drones set against a non-state actor?

•Does the Security Council have a proper judicial system regarding drone warfare?

•With the current ruling of drone warfare, are states free to engage in drone warfare as they please?

•How does drone warfare legislation fit into collective security?

Bibliography

"Drones and the International Rule of Law", Rosa Brooks 2013 Georgetown University Law Center (http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2296&context=facpub)

"A Brief History of Drones" by John Sifton (advocacy director for Asia at Human Rights Watch, February 7th 2012 (https://www.thenation.com/article/brief-history-drones/)

International Committee of the Red Cross, Interview of the president of the committee Peter Maurer, 10th of May 2013 (https://www.icrc.org/eng/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm)

The United Nation's Charter, Chapter 1, Purposes and Principles, signed on the 26th of June 1945 (http://www.un.org/en/sections/un-charter/chapter-i/)

The Economist – "the Agony of Aleppo", September 29th 2016 (http://www.economist.com/news/middle-east-and-africa/21707937-americas-ceasefire-deal-russia-never-stood-chance-agony-aleppo

"What are Drones?" written by Chris Cole and Jim Wright, January 2010 (https://dronewars.net/aboutdrone/)

Terrorism

Terrorism is one of the most pressing issues facing us on the international stage today. The increased frequency of attacks over the past few decades have pushed terrorism, and the development of feasible counter-terrorism measures, to the forefront of the United Nation's agenda. The development of a holistic international counter-terrorism strategy that benefits all member states is an overarching aim of the UN.

WHAT IS TERRORISM?

In 1994, in the United Nation's Declaration on Measures to Eliminate International Terrorism, the General Assembly defined "terrorism" as "criminal acts intended or calculated to provoke a state of terror in the general public by a group of persons, or particular persons for political purposes." It is the use of violence and intimidation to achieve political aims. The declaration further asserted that any attempt by persons to invoke terrorism as a legitimate tool was "unjustifiable" regardless of the philosophical, ideological, ethnic, religious or racial considerations that may be used. Today, most terrorism is carried out by non-state actors, with examples including ISIS, Al Qaeda, and Boko Haram. These groups are often ideologically strong and militarily weak, and use terror as a tool to gain more power.

However, occasionally, individuals have also been responsible for terrorism identified as "lone wolf" terrorism. It is an offshoot of more conventional terrorism, and is used to describe a person who prepares and commits violent acts alone, outside of a command structure and without material assistance from any group. Despite this, they may be influenced or motivated by the ideology and beliefs of an external group, and may act in support of such a group. Lone wolf terrorism is therefore difficult to both detect and prevent. Counter-terrorism measures aimed at stopping lone wolf terrorism are often aimed at ideologies seen to be the main motivator behind these attacks.

HISTORY OF TERRORISM

The word terrorism is derived from the Latin word "terreo" which means to frighten. In English, the first use of the word terrorism was during the French Revolution's Reign of Terror, where the Jacobins enacted violent measures as a policy of the state, designed to compel obedience and quell resistance from enemies.

In the 20th century, terrorism was linked to a variety of political groups including anarchist, fascist, and socialist groups in third world countries that fought against colonialism. Towards the end of the 20th century, radical Islamic terrorism became the most prevalent form of terrorism, and has continued acting as such until present day. The 2001 attacks on World

Trade Center and Pentagon symbolized a shift in the international approach to counter-terrorism measures, and brought them to the forefront of global attention.

ROLE OF THE UN

One of the major roles of the UN in the development of a counter-terrorism strategy is to ensure that measures follow the rule of the international law, and that they protect and promote universal human rights. Furthermore, the UN must ensure that any counter-terrorism measures do not breach the sovereignty of states. Territorial integrity, political independence, and equality are all inalienable rights of states, and counterterrorism measures must respect that. For example, during the United State's War on Terror, the question of how to deal with the sovereignty of the invaded state vs the security of the United States was a topic of extreme importance.

Lastly, to destroy the capacities of international terrorist organizations while simultaneously building up capacities of states to combat terrorism.

Since 1963, there have been nineteen universal instruments against terrorism.

In September 2001, after the attacks on the WTC, the General Assembly developed resolution 1373, which for the first time established the Counter Terrorism Committee. The CTC has taken steps to criminalize the financing of terrorism, freeze any funds related to persons involved in acts of terrorism, and deny all forms of financial support for terrorist groups. It also included measures to suppress the provision of safe haven, sustenance or support for terrorists, and increase cooperation between governments in the investigation, detection, arrest, extradition and prosecution of those involved in such acts and criminalize active.

In 2006, the United Nations General Assembly adopted the Global Counter-Terrorism Strategy. This was a milestone in the development of an international response to global terrorism. The Strategy, which is reviewed every two years, was agreed to by member states in order to develop a "global, comprehensive and strategic" counter-terrorism protocol. It was designed to bring together all of the United Nation's counter-terrorism activities under a common framework. It has four pillars:

1. Addressing the conditions conducive to the spread of terrorism
2. Measures to prevent and combat terrorism
3. Measures to build states' capacity to prevent and combat terrorism, and to strengthen the role of the United Nations system in that regard
4. Measures to ensure respect for human rights for all, and the rule of law as the fun-

damental basis for the fight against terrorism.

Questions to consider:

- What steps can the United Nations take to engage intergovernmental organizations and highly developed countries to assist in the development of counter-terrorism measures in countries with poor counter-terrorism infrastructure?
- What are the roots of inefficient counter-terrorism strategies in countries with poor counter-terrorism strategies?
- In what ways can the UN resolve the security versus sovereignty dilemma while developing efficient counter-terrorism measures?

- How can the UN intensify cooperation between states in the exchange of timely and accurate information concerning the prevention and combating of terrorism?
- How can the UN assist in the development of counter-terrorism strategies that target lone wolf terrorism?

Bibliography

"The United Nations Global Counter-Terrorism Strategy". 2008. Resolution adopted at 120th Plenary Meeting of the United Nations General Assembly, New York, 5th September

United Nations General Assembly. 1996. Measures to Eliminate International Terrorism. [Available at: http://www.un.org/documents/ga/res/51/a51r210.htm [Accessed: Nov 7 2016]

UN.org. n.d. General Assembly Actions to Counter Terrorism - United Nations Action to Counter Terrorism. [online] Available at: http://www.un.org/en/terrorism/ ga.shtml [Accessed: Nov 6 2016].

Nunn, Samuel. "Incidents of Terrorism in the United States, 1997-2005." Geographical Review, vol. 97, no. 1, 2007, pp. 89–111.

UTMUN'17

CELEBRATING TEN YEARS

University of Toronto
Model United Nations

utmun.org | info@utmun.org