Cerritos Advanced Conference 2020

Ad Hoc on Terrororism

Topic A: Cyberterrorism

Topic B: Narcoterrorism

Director: Paul Sherdsuriya

POSITION PAPERS DUE on October 17th by 11:59 pm to Committee Email

October 24-25, 2020

To Delegates of CHSMUN Advanced 2020

Dear Delegates,
Welcome to CHSMUN Advanced 2020!

It is our highest honor and pleasure to welcome you all to our 2020 online advanced conference here at Cerritos High School. On behalf of the Cerritos High School Model United Nations program, we are proud to host our very first advanced conference, where you will become more knowledgeable on international issues, participate in intellectually stimulating discussions, and create new and everlasting friendships.

The CHSMUN program continues to compete around the world as a nationally ranked MUN program. Our delegates utilize diplomacy in order to create complex solutions towards multilateral issues in the global community. Our head chairs are selected from only the best seniors of our program, undergoing a rigorous training process to ensure the highest quality of moderating and grading of debate. Furthermore, all the topic synopses have been reviewed and edited numerous times. We strongly believe that by providing each and every delegate with the necessary tools and understanding, he or she will have everything they need to thrive in all aspects of the committee. We thoroughly encourage each delegate to engage in all of the facets of their topic, in order to grow in their skills as a delegate and develop a greater knowledge of the world around them.

Although this wasn't what we expected, our advisors and staff have put in countless hours to ensure delegates have an amazing experience at the online conference. Our greatest hope is that from attending CHSMUN 2020, students are encouraged to continue on in Model United Nations and nevertheless, inspired to spark change in their surrounding communities. With this strong circuit consisting of 6 schools and over 500 delegates, CHSMUN Advanced 2020 will provide a quality experience for intermediate delegates to enhance their speaking and delegating skills.

If you have any questions, comments, or concerns, please contact us! We look forward to seeing you at CHSMUN Advanced 2020!

Sincerely,

Anjali Mani and Karishma Patel

sg.cerritosmun@gmail.com

Secretary-Generals

A Note From The Director

Delegates,

My name is Paul Sherdsuriya, and I'm the Head Chair or Director for ADHOC on Terror CHS 2020. I'm a senior at Cerritos and have been in MUN since I was in 8th grade, making this my 5th year in MUN. Through the Cerritos MUN program, I've gone through many different types of committees, from UNICEF to Security Council, and have gone to Nationals to represent the Cerritos Dons. Besides MUN, I love to sing and learn about the dynamics of singing. I'm more self-taught, but I've put countless hours into understanding the ins and outs of my voice and have learned to appreciate others'. Likewise, I also enjoy listening to all kinds of music. Ask anyone and they'll say that I can vibe with any kind of music, and my playlist is always all over the place in terms of genre and languages. However, if I had to choose my favorite song of 2020, I'd say it's Face to Face by Ruel. I'm looking towards creating a small band with my friends when quarantine ends and gain more experience as a singer. I'm also looking towards learning a new instrument, especially during this quarantine, and hope to hear many new ideas or recommendations regarding music or singing. You can also find me swimming at my favorite pool at the Cerritos Park East Community pool, where I've been learning and perfecting my swimming since I was 5. Although I've been taking a short break, I still hope to return to swimming healthily. I'm a very extroverted person, so if you ever feel the need to ask any questions regarding the committee or anything you may be curious about, ask away! I'm also actively looking for ways for delegates to improve with mental notes and I hope you are open to asking for feedback so you can become a better delegate. Remember to stay safe during this dire time, since I'm very excited to see all of you in the conference.

Sincerely,

Paul Sherdsuriya

Adhoc.CHSMUN@gmail.com

Director, Ad Hoc on Terrorism

Committee Introduction

The 1996 General Assembly brought about the creation of resolution 51/210 and the Ad Hoc Committee on the 17th of December. The roots of Ad Hoc on Terror can be traced to the adoption of the 1994 *Declaration on Meaures to Eliminate International Terrorism* and *1996 Declartation to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism*. Specifically, Ad Hoc on Terror was created to represent an international convention purposed with addressing and suppressing actions of terrorist bombings through the utilization of existing and new international instruments(international jurisdiction, other UN branches, etc) and the development of a legal framework organizing conventions related to the elimination of international terrorism. With its official mandate emphasizing the agenda of creating "Measures

to eliminate international terrorism", the Ad Hoc Committee is purposed to address the issue of terrorism with solutions revolving around the implimentation of defensive solutions and jurisdiction. The Ad Hoc Committee continues to supplement solutions through an annual session which lasts one to two weeks, working based on the idea that nothing is agreed until everything is agreed upon. Through Ad Hoc, the *International Convention for the Suppression of Terrorist Bombing*, the *International Convention for the Suppression of the Financing of Terrorism*, and the *International Convention for the Suppression of Acts of Nuclear Terrorism* were formed and adopted by the General Assembly.

TOPIC A: Cyberterrorism

Background:

Cyberterrorism, known as "the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society", has seen exponential growth with the rise of innovative and widespread use of accessible technological devices and the internet. The issues are emphasized by the infrastructural reliance on the internet (power utilities, water treatment services, and health and emergency systems), evolving cyber threats as a result of the development of sophisticated tools through the black market, and the risk of major corporations and the economy threatened by cyber attacks. With 40% of the world's population having access to the internet, 5 billion people owning a mobile device, and 90% of the world's data being generated within the past two years alone, a majority of the population is exposed to the fear raised through the possibility of cyber terrorist attacks. In addition, the use of cyberterrorism has grown to shift from focusing the use of cyber attacks on primary consumers to global politics and economic systems. This can result in the loss of revenue, expenses for restoring operations and improving cybersecurity defenses, regulatory fines and scrutiny, and reputational damage.

The complex topic of cyberterrorism can be separated into five categories: organized crime, hacktivism, non-state terror groups, lone wolves, and nation states. Organized cyber crimes are made up of hackers coming together because of functional skills that allow them to collaborate and commit specific crimes. This allows for expertise of certain aspects of cyberterrorism to coerce and create larger disruptions. On the political spectrum, hacktivists and the act of hacktivism, or the misuse of computer systems or networks for socially and politically motivated reasons, mainly focus on calling for the public's attention on a certain issue through exposing alarming information and data in attempts to inform and call for action from the populace. The most synonymous figure/group associated with the title of hacktivists is the infamous Anonymous group, which saw its creation in 2008 and their attacks on the government and ISIS in hopes of creating change in society. Methods used by hacktivists can include Geo-bombing, information leaking, Doxing, and DDoS/DoS attacks. Non-state terrorist groups,

such as Al-Qaede, who utilize cyberterrorism during a debate or conflict between sovereign states and international organizations. Nation-states cyberwarfare is when hackers target government agencies, critical infrastructure and industries known to contain sensitive data or property through cyberespionage. Its purpose is to obtain data that will benefit their own country's economy and strengthen both business and military strategies. Lastly, lone-wolfs are individual hackers attempting to crack and disrupt a system in hopes of individual gain. Although being different processes, ultimately each category owns the common motive that results in catastrophic economic and reputational damage to companies.

Among the most influential of the five categories, nation-state cyber warfare and non-state terror groups create the most impact on geopolitical positions. Through the utilization of cyber-espionage,"the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization", nation-state cyber warfare sponsor or co-opt indigenous cyber criminals, hacktivists, or semi-professional criminal hackers to either launch cyber operations with the cover of deniability. Due to the near impossibility of regulation of code and cyber actors are selling or sharing their capabilities and techniques without restraint. Because of the lack of regulation, automation and proliferation of sophisticated and "usable" cyber tools abound, nations have access to cyber-espionage, granting countries the ability to access highly sensitive information that would potentially grant a diplomatic or competitive advantage. A popular example of cyber-espionage can be traced to the controversy of the 2016 Donald Trump presidential campaign, with many insinuating that the Russian government utilized nation-state hacking to obtain a geopolitical and diplomatic influence through attempting to inflate the 2016 elections in Trump's favor. The threat-actors who often take advantage of technological innovations to expand or improve operations may not understand the geopolitical impact, creating potential consequences or the "domino effect" inherent in an interconnected environment. As a result of malpractice, this malicious code can also spread to other countries, disrupting the nation's critical infrastructure sector.

As stated, the number of cyber attacks have grown exponentially as a result of the alarming growth in the technological sector and interconnectivity. Greater interconnectivity creates a landscape for potential cyber threat actors. A major example can include the Internet of Things(IoT), conventionally referred to as the Internet, which hosts many different pathways for hackers to compromise a user device for operations, such as NotPetya, WannaCry, Destover, and Stuxnet, which resulted in large quantities of data destruction. In 2016, 758 million malicious attacks occurred according to KasperskyLab, with costs for damages reaching $5 trillion by 2020. Notable instances of cyberterrorism is Yahoo's 2014 report of suffering a cyber attack that affected 500 million user accounts, being named as the largest massive hacking of individual data directed against a single company. In addition, Yahoo! Confessed to being attacked for up to 32 million accounts, resulting in the firm being bought by Verizon in 2017 for $4.5 million instead of $4.8 million in 2016. Information, such as names, dates of birth, telephone numbers and passwords were leaked and sold for up to $1,900 for each password. Such cyber attacks have also been seen targeting critical infrastructure, with the Global State of Industrial Cybersecurity report finding 74% of IT security professionals globally being more concerned about a cyberattack on critical infrastructure than an enterprise. The lack of protection in critical infrastructures, with 51% of industry practitioners seeing a lack of safeguards and protection for industrial networks and 55% believing that the U.S. critical infrastructure is vulnerable to cyberattacks.

United Nations Involvement:

On December 27 of 2019, resolution 74/247 allowed for the General Assembly took note of Commission on Crime Prevention and Criminal Justice resolution 26/4 of 26 May 2017, where the Commission expressed appreciation for the work done by the Expert Group to Conduct a Comprehensive Study on Cybercrime, wanting to propose a new national and international legal response to cybercrime. This very resolution established an open-ended Ad Hoc intergovernmental committee of experts, representative of all regions, to elaborate an international convention on countering the use of information and communications technologies for criminal purposes. The General Assembly also called for an Ad Hoc committee to be hosted for a three day session in August 2020 in New York. Specifically, this committee is proposed with proposing an outline and modalities for the further activities of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

In addition, resolution 2341(2017), the security council called action from member states,"to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks." Additionally, the UNOCT, or the UN Office of Counter-Terrorism has intitiatives in the field of new technologies. For instance, the UNOCT has created a project on the use of social media in order to gather open source information and digital evidence to battle terrorism. The Cybersecurity and New Technologies programme aims to enhance capacities of Member States and private organizations in preventing cyber-attacks carried out by cyberterrorists against critical infrastructure. The Cybersecurity and New Technologies programme insists the Member States should consider reviewing national legislation to ensure that evidence collected through special investigative techniques or from countries of destination or evidence collected through ICT and social media, including through electronic surveillance, can be admitted as evidence in cases related to foreign terrorist fighters, while respecting international human rights law, including freedom of expression". The programme has also provided expertise in international fora on terrorist uses of unmanned aerial systems (UAS), proving successful. The UNODC's ability to prosecute hackers and collect data on hackers through a cybercrime respiratory database also allows for the UN to take legal action against hackers.

Case Study: Cyberterrorism From China

Approximately 30 percent of all cyber-attacks worldwide are launched from China, which its largest military group of cyber experts execute. The country has been accused of perpetrating state-sponsored attacks against foreign governments and businesses. China, with its

outlook and goal of exceeding the United States in military strength, continues to look for advantages over the United States through asymmetrical warfare, which helps alleviate military shortcomings by electing to formulate and explore methods of countering an adversary's strength by attacking their weaknesses. China makes viable attempts to gain access to America's sensitive information. Referred to as a "red hackers", aim for the use of cyber-espionage with the intent of causing harm to the United States. China has been making large investments in new technology for the People's Liberation Army (PLA) and has established a special information-warfare group to coordinate national offense and defense. China experts in the Pentagon refer to these efforts as the creation of "The Great Firewall of China." Part of the reason for such aggressive action is China's belief that it is already under cyber-attack by the United States. Thus, within the year of 2015, the United States and China attempted to recuperate and communicate over the increase of cyber attacks by the Chinese government and their attempt to use cyber-espionage to gain an upper hand. The presidency of Obama saw a treaty between Xi and Obama in order to reduce the use of cyber-espionage, marking a more progressive action towards the reduction of the military policy of asymmetric warfare. Despite this, China continues to be the main user of cyber-attacks and espionage worldwide, with the current Trump agency creating accusations on Chinese applications and the use of spyware to gain highly-classified information.

Bloc Positions:

Western Bloc: The West has dealt with major damages to the economy as a result of the rise of the use of cyberattacks. Particularly, the United States has paid between $57 billion and $109 billion in 2016 in Cybercrime damage. Cyber attacks primarily targeted private and public entities with denial of service attacks, data and property destruction, business disruption(for the purpose of collecting ransoms) and theft of proprietary data. The US has also enlisted the use of the NIST Cybersecurity Framework, which recognizes five critical functions for managing cybersecurity risk, and the FBI Cyber Shield Alliance, which engages in partner partnerships with the U.S. State, local, territorial, and tribal law enforcement agencies to synchronize efforts against malicious cyber activity. The European Commission has created new rules and practical measures to make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists and support law enforcement authorities in overcoming challenges posed by encryption in the context of criminal investigations while respecting the strong encryption. Thus, various organizations like EUROPOL and EUROJUST will act in ways to mitigate risks and contain the damage of cybercrime and cyberterrorists.

Latin American and Carribean Bloc: Latin America is extremely susceptible to cyber attacks. In the Eset Latin American Security Report(2017) the number of reported ransomware cases grew 131% in 2016. Brazil has single handedly accounted for a 197% increase in 2015. This is a result of the few coordinated defense mechanisms, lack of public awareness, and disconnect between public and private industries. Although there are few coordinated defense mechanisms, Latin America has begun to create programs and teams such as the Cyber Emergency Response Teams(CERTs) and Computer Security Incident Response Teams (CSIRTS) to handle attacks.

However, these programs can only be found in a few countries, and are not widespread throughout Latin America. The public awareness in Latin America also suffers, as private companies believe they are not targets, resulting in having little to no preventative programs.

African Bloc: Last year, South Africa had the third-highest number of cybercrime victims of any country. Suffering from 577 malware attacks per hour, which was a 22% increase from last year, hackers easily targeted the trend found in the increase in the accessibility to banking apps . Fraud through the use of banking apps doubled, which has contributed to the billions in losses. Ransomware, being the most used cyberattack in South Africa, is easily accessible on the dark web for as low as $100, making it accessible to the most unskilled criminals. The *2019 KnowBe4 African Cybersecurity Awareness Report* which surveyed over 800 respondents from eight African countries, found that 64 percent of people in the continent do not know what ransomware is. The situation creates more concern as 525 million people in the region are connected to the internet, making up 40 percent of Africa's total population. As connectivity improves, users are more prone to the increasing cyberattacks.

Asian-Pacific Bloc: The Asian-Pacific is also susceptible to cyber threats. It Asian-Pacific is becoming the home to 40% of the world's data centers. More and more companies have begun to rely on APAC as a cloud service, allowing for users to become targetable by cybercriminals. Thus, the increase in the use of cloud services will collectively result in the growth of the insufficient protection and data breaches. Data breaches and the vulnerability of the cloud services that are currently trending in the Asian-Pacific are supported by the use of frequent IoT(Internet of Things) and DDoS(Denial of Service) attacks on the internet(through the use of attack drones). chinaThe Asian-Pacific is currently looking towards utilizing AI systems to counter cyber threats in the early stages. In addition to building on defensive capabiltiies, Asian-Pacific countries, such as China, North Korea, Pakistan, and India, have adopted offensive cyber abilities, reflecting Trump's decision to create offensive cyber operations.

Basic Solutions:

When considering solutions for the issue of Cyberterrorism, it is important to research and address issues revolving around the judicial aspect of the UN to punish cyberterrorists, find innovative solutions revolving around cyber security, and spread awareness in countries with a lack of knowledge in regards to cybersecurity. The judicial prosecution of cyber criminals through the ICC(International Criminal Court) is often overlooked as a result of the lack of solid evidence that can be collected and used against cyber criminals and legal guidelines revolving around cybercrimes can be interpreted as loose. Thus, defining a legal guideline for the prosecution and acts of cybercrimes is essential in tackling cyberterrorism. Cybersecurity can also be seen as an essential solution to research, as the use white-hat hackers and safe databases can be used to improve sustainability within companies that are susceptible to cyberattack. White-Hat hackers use hacking in order to find vulnerabilities in the cybersecurity system, allowing for these short-comings to be fixed. Lastly, solutions revolving around spreading awareness, especially in countries in Latin America, can significantly reduce the threat of cyber

attacks and data breaches. For instance, the NCSAM, or National Cybersecurity Awareness Month, continues to raise awareness about the importance of cybersecurity and ensure that all Americans have the resources they need to be safer and more secure online. A similar action can be implemented globally, but must be organized in order to successfully be efficient in educating the public. A major focus of this committee is dealing with controversial and impactful effects of nation state and non-state terror groups, who create huge influxes and damages to critical infrastructure, the geopolitical platform, and diplomatic relations. Thus, solutions regarding diplomatic relations among nation-states can decrease the usage of cyberespionage. Such as the agreement between the United States and China in 2015 regarding the reduction of cyber-espionage. Delegates also look towards increasing the amount of cyber-warfare defense measures and assist other developing-countries and worn-torn countries under attack by non-state terror groups, creating and encouraging the use of innovative databases, such as blockchain, that can store valuable information and maintain critical databases.

Questions to Consider:

1. What countries have utilized nation-state cyberterrorism for their own benefit and how can they contribute to the reduction of cyberterrorism?
2. How can the U.N. reduce the use of cyber terrorism caused by non-state terrorist groups like Al-Qaeda?
3. What is the importance of the black market in the apprehension of cyber terrorism?
4. What can companies do in conjunction with the U.N.'s actions to reduce the risk of cyber threats and attacks like ransomware and DDos?
5. How can countries address the issue and risks having a critical infrastructure and economy?

Sources:

1. *Hackers on the Dark Web Love South Africa - Here's Why We Suffer 577 Attacks per Hour*, www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6.
2. 03.Dec.2018 Outpost24, and Outpost24. "TOP 10 of the World's Largest Cyberattacks, and How to Prevent Them." *Outpost 24 Blog*, outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks.
3. "Globalization's Bastards: Illegitimate Non-State Actors in International Law." *Taylor & Francis*, www.tandfonline.com/doi/abs/10.1080/09662840420002790 09?journalCode=flic20.
4. "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar", *Public-Private Analytic Exchange Program,* 2019
5. "Critical Infrastructure Cyberattacks a Greater Concern than Enterprise Data Breaches." *Security Magazine RSS*, Security Magazine, 26 Mar. 2020, www.securitymagazine.com/articles/91992-critical-infrastructure-cyberattacks-a-greater-concern-than-enterprise-data-breaches.

6. "Cybercrime Ad Hoc Committee." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html.
7. "Cybercrime Ad Hoc Committee." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html.
8. "Cybersecurity Could Be Better If African Businesses Knew These Things." *WeeTracker*, 13 Apr. 2020, weetracker.com/2020/01/13/african-cybersecurity-challenges/.
9. Anonymous. "Cybercrime." *Migration and Home Affairs - European Commission*, 6 Dec. 2016, ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en
10. "Cybercrime Top 10 countries where attacks originate", https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf
11. "Cybersecurity | Office of Counter-Terrorism." *United Nations*, United Nations, www.un.org/counterterrorism/cybersecurity.
12. "Cybersecurity | Office of Counter-Terrorism." *United Nations*, United Nations, www.un.org/counterterrorism/cct/programme-projects/cybersecurity.
13. LCDR Lonnie Pope, "Cyber-Terrorism and China", *Master of Military Studies,* April 2002
14. Dyer, Geoff. "Obama and Xi in Deal on Cyber Espionage." *Register to Read | Financial Times*, Financial Times, 25 Sept. 2015, www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644.
15. Lynkova, Darina. "How Fast Is Technology Growing Statistics [Updated May 2020]." *Tech Jobs*, 4 May 2020, leftronic.com/how-fast-is-technology-growing-statistics/.
16. "National Cybersecurity Awareness Month (NCSAM)." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/national-cyber-security-awareness-month.
17. O'Malley, Mike. "Concerned about Nation State Cyberattacks? Here's How to Protect Your Organization." *Security Magazine RSS*, Security Magazine, 26 Mar. 2020, www.securitymagazine.com/articles/91889-concerned-about-nation-state-cyberattacks-heres-how-to-protect-your-organization.
18. "Organized Cybercrime -- Not Your Average Mafia." *ScienceDaily*, ScienceDaily, 16 Jan. 2020, www.sciencedaily.com/releases/2020/01/200116123805.htm.
19. Rouse, Margaret. "What Is Hacktivism? - Definition from WhatIs.com." *SearchSecurity*, TechTarget, 31 July 2018, searchsecurity.techtarget.com/definition/hacktivism.
20. "Secretary-General Calls Cyberterrorism Using Social Media, Dark Web, 'New Frontier' in Security Council Ministerial Debate | Meetings Coverage and Press Releases." *United Nations*, United Nations, www.un.org/press/en/2019/sgsm19768.doc.htm.
21. Security, Penta. "3 Cyber Attack Trends to Hit Asia-Pacific in 2020." *Penta Security Systems Inc.*, 17 Dec. 2019, www.pentasecurity.com/blog/3-cyber-attack-trends-hit-asia-pacific-2020/.
22. "Three Reasons Why Latin America Is Under Cyber Attack." *IEEE Innovation at Work*, 28 June 2017, innovationatwork.ieee.org/latin-america-is-under-cyber-attack/.
23. "Webinar 65/2018 Cyber – Terrorism: A Threat for the European Union and Its Response." *CEPOL*, 7 Nov.2018, www.cepol.europa.eu/education-training/what-we-teach/webinars/webinar-652018-cyber-–-terrorism-threat-european-union-its.

24. Wyman, Oliver. “Global Cyber Terrorism Incidents on the Rise.” *Marsh & McLennan Companies*, www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.
25. “International Law, Codification, Legal Affairs, Legal, Committee, Terrorism, Charter, Criminal Accountability, Administration of Justice, Jurisdictional Immunities, Cloning, Safety of United Nations and Associated Personnel, Ad Hoc.” *United Nations*, United Nations, legal.un.org/committees/terrorism/.

TOPIC B: Narcoterrorism

Background:

Narco-terrorism can be defined as “terrorism associated with trade in illicit drugs” or “terrorist tactics employed by dealers in illicit drugs, as against competitors or government agents”. However, the definition of narco-terrorism can also be interpretted as a ambigious, and thus, opens the topic up to many different issues. The term was first used to describe campaigns by drug traffickers using terrorist methods, such as car bombings, assassinations, and kidnappings against anti-narcotics police in Colombia and Peru. The literal action of narco-terrorism can range from input of terrorist groups utilizing illicit drug trade to fund their terrorist intentions to drug trafficking groups resorting to terrorist activity to maintain their interests. Narco-terrorism may draw in many participants as a result of many issues within the social constructs of a country, with poverty being the number one reason for the increase in participation in narco-terrorism. Narco-terrorism creates an opportunity to escape the confines of poverty, especially within third world countries where the cultivation of narcotics thrive. Narco-terrorists in the context of drug traffickers using terrorist methods refers to individuals such as the drug lord Pablo Escobar from the Medellin cartel in Colombia and other members of drug cartels, mafia, or other criminal organisations, whose actions were defined as “the attempts of narcotics traffickers to influence the policies of government by the systematic threat or use of violence”. On the other hand, narco-terrorism can also focus primarily on the “terrorism” aspect. The DEA, or the United States Drug Enforcement Agency, has described narco-terrorism “narco-terrorism may be characterized by the participation of groups or associated individuals in taxing, providing security for, or otherwise aiding or abetting drug trafficking endeavours in an effort to further, or fund, terrorist activities”. Thus, the DEA’s definition of narco-terrorism emphasizes the terrorist organization aspect of the topic and the use of narcotics to create a different source of income. The complexity of the topic of narco-terrorism is due to the duality of its definition, where the emphasis can be shifted between narcotics organizations or terrorists organizations. The many terrorist groups, such as the Taliban, have influences over drug sales in the hopes of generating a secondary source of income to fund terrorists intent. Primarily, terrorist groups will employ the trading and selling of Opium, a highly addictive non-synthetic narcotic that is extracted from the poppy plant, Papaver somniferum. Additionally, Opium is the key source of many other narcotics, including morphine, codeine, and heroin. Through the sale of opium, narco-terrorists are capable of retrieving income in many different environments. On the other hand, drug cartels and criminal organizations can be extremely influential in areas such as Latin America or with instances that instate Russian gangs. Latin America has also invested into the widely cultivated coca, which is later synthesized for the use of cocaine. Thousands of peasant families grow coca leaves while drug barons direct much of the production, processing and trafficking of cocaine, earnings wield enormous economic, social and political influence in Latin America. Apart from the corrupting power of such huge sums of narcodollars on police and judicial systems, Congressmen are elected with cocaine funds, banks are sustained or broken by trafficking groups and exchange rates fluctuate in sympathy with the state of the trade. Peru is considered the biggest coca leaf producer, with about 60,000 tons, followed by Bolivia with about 50,000 tons. However, Colombia leads the world of cocaine with 15,000 tons. Experts

believe about 60 percent of South America's exported cocaine is refined in Colombia, with Brazil and Ecuador expanding very rapidly in the last three years, and minimum estimates run at 11,000 and 6,000 respectively. Small plantations in other countries such as Venezuela and Argentina raise the total number of tons to at least 145,000. Additionally, organizations like FARC play a huge contribution to the growth of narcotics within the South American terrain. The Revolutionary Armed Forces of Colombia, a Marxist-Leninist guerrilla group, began trafficking cocaine in the late 1970s to fund its activities, a practice that facilitated its rapid growth throughout the 1980s. The FARC's wealth from kidnappings and the drug trade, and its provision of social services, attracted a large number of new members who sought to escape the increasing poverty levels in Colombia. Together, the increase in profit and new members marked the beginning of the FARC's exponential growth and rise in power. South American and Caribbean waters have seen a rise in piracy and narcotics trafficking, with Colombian maritime territory being a huge host for maritime narcoterrorism. Thus, the narcotics produced in Colombia, can be transported across the world, creating influences across the globe Although, traditionally a concept connected with Latin America, narco-terrorism is seeing an exponential increase in activity within the regions of Central and Southeast Asia. Specifically, narco-terrorist trafficking occurs within the Golden Crescent and the Golden Triangle. The Golden Crescent and the Golden Triangle are known as Asia's two principal areas for illicit opium production, with the Golden Crescent being located between Central, South, and Western Asian and overlapping over Afghanistan, Iran, and Pakistan and the Golden Triangle being located along the borders of Thailand, Laos, and Myanmar. Afghanistan, located in the Golden Crescent, is widely acknowledged to be the world center of opium cultivation, hosting up to 160,000 hectares of poppies and yielding 6,700 pure metric tons of opium within 2019 alone, seeing an extreme of 328,000 hectares and 9,000 yield between 2016 and 2017. As a result, Afghanistan can be considered a narco-state, with 90% of the world's opium coming from Afghanistan. This plays a large role in the topic of narco-terrorism, as many terrorist groups rely on the Golden Cresecent and Golden Triangle to generate opium and create elaborate drug traffick chains. This results in the over running and manual destruction of crops in order to create more arridable land for the production of opium. Terrorist groups, as stated earlier, have become reliant on drug trafficking as a principal funding source as result of the significant decline in funding of guerilla and terrorist groups by ideologically motivated state sponsors since the end of the Cold War. This relationship with narcotics allows for not only having a source of income, but allows for the exchange of drugs, weapons, use of the same smuggling routes, use of similar methods to conceal profits and fund-raising, informal transfer systems such as the Black Market Peso Exchange(BMPE), use of the same resources for laundering money, and the use of the same corrupt government officials. The cartels and the drug-trafficking organizations normally seek financial enrichment while the extremist groups and terrorist groups seek political and religious influence. This is primarily seen within Islamic fundamentalist groups who have become known to be involved with drug trafficking to fund their operations and degrade the western society. In addition, all narco-terrorists have been seen to have some involvement with al Qaeda, an active narco-terrorist group.``Charitable" and other non-governmental front organizations, such as the Saudi-based International Islamic Relief Organization (IIRO), are used by worldwide terrorist organizations to channel funds to their affiliated terrorist groups. Together, the drug-traffickers and terrorists share a pragmatic relationship.

United Nations Involvement:

The UN has tackled the issue of narco-terrorism through trying to limit the trafficking of narcots and influences of terrorists on the international community. For instance, the United Nations Office on Drugs and Crime (UNODC) has created the Commission on Narcotic Drugs (CND), a committee that emphasizes solutions that stop narcotics. Besides AdHoc On Terror, the UNODC has had large contributions towards stopping the issues of terrorism. The UNODC has created the a 19 part system for actions against terrorism, regarding with the topics of financing terrorism, terrorist bombings, nuclear material, and other topics. This is also backed by the UN Global Counter-Terrorism Strategy, outlining the common set of strategies for countries to follow while dealing with the issue of narcotics. In addition, the CND creates strategies to stop the drug cartels, recommending governments information on how to combat the exportation of narcotics. Within resolution A/RES/S-30/1, CND worked to negotiate the outcome document from the Special Session on the World Drug Problem. Overall the UN has passed over 65 resolutions in accordance to terrorism, such as A/RES/72/824, which institutes the use of the UN Global Counter-Terrorism Strategy, A/RES/72/246, and A/RES/62/194, which implemented counter-terrorist strategies and referencing the Ad Hoc Open-ended Working Group. Additionally, the UN, within the 19 part system, has initiated a series of UN resolutions imposing sanctions- such as the freezing of assets, a travel ban and an arms embargo, on members of the Taliban, Al-Qaeda, and their associates(up to 124 entities and 226 individuals). This is especially prevalent, as the Taliban and Al-Qaeda have been seen to harbor a large amount of narcotics for their intents and purposes. The FATF, or the Financial Action Task Force, was also appointed by the UN to update the FATF/GIABA report on *Terrorist Financing in West Africa* (October 2013) and to extend the study to the Central African Region. The report considers the possible funding sources, particularly in relation to Boko Haram and groups linked to Al-Quaeda, including Al-Qaeda in the Lands of the Islamic Maghreb (AQIM) and its affiliates, and also considers potential means to finance terrorism and other vulnerabiulities. This report reveals the number of threats and vulnerabilities that are specific to the region.

Case Study: Narcoterrorism In Columbia

Narcoterrorism became an issue within the country of Colombia in the early 2002, the final days of Colombian President Andres Pastrana's administration were taken back by an unending internal war against right wing and leftist narco-terrorists and criminal cartels, which was a time when narco-terrorists reached their apex of power. The two major leftist groups,the Fuerzas Armadas Revolucionarias de Colombia (FARC) and the Ejército de Liberación Nacional (ELN), threatened the capital and were able to operate in every region of Colombia. These groups were well armed due to the immense sums of narco-dollars, which maintain them in the field to this day. In a desperate bid for peace, President Pastrana ceded to the FARC a vast safe-haven ,Zona del Despeje, in exchange for participation in peace talks. Regardless, the

FARC continued illicit trafficking and even engaged in terrorist acts while “talking peace.” A similar offer was under consideration for dealing with the ELN. Another instance involves Pablo Escobar, who was a Colombian criminal and head of the Medellin cartel. Eventually Pablo Escobar controlled over 80 percent of the cocaine shipped to the U.S., but had his start in the cocaine trade in the early 1970s by collaborating with other criminals to form the Medellin Cartel. He later utilized his platform for terror campaigns that resulted in the murder of thousands and having relations with terrorists groups. In 2000, the United States began funding for Plan Colombia, intending to rid of drug crops and to act against drug lords accused of engaging in narcoterrorism, primarily groups like the FARC. The U.S. government, in order to assist the Colombian government and military operations, started funding large-scale drug eradication campaigns.

Bloc Positions:

Western Bloc: The Western Bloc, especially the United States, has taken a firm stance against narco-terrorism since the Cold War, with president Reagan tailoring the term to describe the relationship between narcotics traffickers, political terrorists, and leftist guerrilla movements. Specifically, Reagan used this term to accuse Cuba and Nicaragua of smuggling drugs into the United States to destabilize American society and then using the profits to finance the Marxist revolution in the Western Hemisphere. Furthermore, the United State's relationship with terrorists reached its peak after the events of September 11, 2009 and the start of the “War on Terror”. Thus, the United States has been the forefront of the battle against terrorism and has had involvement in Afghanistan and the Afghanistan War, the international narco-state. The United States has even planned Operation Reciprocity, an operation focused on ending the narcotics held within the which ultimately failed to pass as an action. On the other hand, the European Union has also followed the footsteps of the United States, with 129 failed foiled terrorist attacks and 1056 terrorists arrested in 2018. To add on, in May 2015 and July 2016, the Council and the European Parliament adopted new rules to prevent money laundering and terrorist financing and the European Commission released a proposal to amend the existing rules to further strengthen the fight against terrorism financing. The Council and the European Parliament are currently reviewing the proposal.

Latin American and Carribean Bloc: Narco-terrorism primarily targets Latin America through the drug cartel and drug orgnaizations. The concept of “narcoterrorism” emerged in the highly politicized context of the Cold War. The Reagan administration accused Cuba and Nicaragua, the two avowedly Marxist-Leninist regimes in Latin America, of smuggling drugs into the United States to destabilize American society and then using the profits to finance Marxist revolution in the Western Hemisphere. Circumstantial evidence of the involvement of corrupt Cuban and Nicaraguan officials in the drug trade did emerge, but there was no evidence to suggest that it was systematic or pursued as a matter of policy. Thus, the term was basically tailored as a result of Latin America’s concrete relation to narcotics and narco-terrorim. As a result of this strained relationship, Latin America has seen escalating crime levels, which have negatively impacted the economic growth and democratic development. The current state of

Latin America's relation to narcotics trafficking needs to be led through judicial reform and root out political corruption that has already allowed for narco-traffic to flourish.

African Bloc: West and Central Africa are particularly vulnerable to terrorism. The continuing violence and conflict in this area since 2010 has caused concerns that the threats from terrorism, especially funding-related terrorism, would cause disfunction to economic gains, contribute to political instability and stall future developments. Communities within the West and Central have already experienced the impact of extremist violence from multiple terrorist groups. Sources of funding can easily be seen within the borders of Western and Central Africa. Historically, it is unlikely that terrorist groups operating in Western and Central Africa have been responsible for providing the entire infrastructure necessary to maintain international drug-trafficking. Contrary to this belief, it is more likely that major international cartels have employed terrorists at various stages of the trafficking process to ensure the delivery of drugs to their destinations and are paid compensation for their services, thereby apply to both definitions of narco-terrorism. Additionally, it has been traced that illicit drugs have also been seen to start manufacturing within West and Central Africa. The US Drug Enforcement Administration has reported
Mexican cartels setting up clandestine drug labs in Nigeria and drug trafficking and money laundering organisations in West Africa may be led by Lebanese nationals with ties to Hezbollah.

Asian-Pacific Bloc: Within Asia, Thailand, Laos, China, and Myanmar currently make up the Golden Triangle, one of the two centers for opium production. Thus, Asia plays a major role in Narco-terrorism. Acting as both a source and consumer, the Golden Triangle has yielded $16.3 billion dollars worth of opium production and illegal drugs trade in 2006 and has 762 tonnes of opium in 2014, making up 76 tonnes of heroin. The policy regarding opium production and narco-terrorism is also controversal, especially as it has its roots tied to political corruption. Since operations began in January, Thailand, Myanmar, Laos, and China have reported nearly 600 arrests along with solving 590 drug-related cases as a result of over 5,000 law enforcement officers participating in 840 operations. Through these arrests, 71kg of heroin, 38kg of methamphetamine, 1.2 kg of opium, and 4.12 m amphetamine tablets were seized in 2015.

Basic Solutions:

Delegates should consider solutions on how to directly stop terrorist groups and their sources of income, treat the citizens of target countries, and attack the roots of narco-terrorism. For instance, delegates should look for solutions, such as heroin assisted treatment(HAT) to treat the targeted citizens and reduce the sales of narcotics. HAT treatment was found to have 2 major benefits over methadone treatments, with 67% retention rates and 6000 euros cheaper than conventional treatments. In addition, delegates should utilize solutions such as anti-money laundering (AML) monitoring technologies to ensure money can not be transferred from "legal" operations. This helps to sever the relationship between the drug cartel and criminal organizations and terrorists who assist in transferring of drugs between stations. Banks create systematic integrity risk analyses (SIRA), which provide guidelines on suspicious activity that

banks have to be wary of. This allows for banks to use the AML technologies in order to identify transactions that have violated the terms set by SIRA. Banks will be able to report any alerts to their nation's anti -money laundering branch and reduce further complications. This can be utilized in countries to harbor a large number of banks, such as the Netherlands, in order to increase the amount of presence the country has in scanning for narco-terrorists activities. Lastly, delegates should attack the roots of narco-terrorism, such as political corruption through the use of solutions such as anti-corruption kits and establishing a proper judiciary system within countries that fail to maintain a stable government. However, it is important for the delegates to maintain sovereignty for the respective countries while working around the unshakable corruption found in countries such as Myanmar or Thailand.

Questions to Consider:

1. What allows for countries to harbor drug cartels and opium reduction without the international communities involvement?
2. What definition does the Ad Hoc Committee follow and how should the solutions be focused to best target the issue of narco-terrorism?
3. How has the relationship between narco-terrorists and drug cartels changed from the last 40 years?
4. What terrorist groups hold the most influence over the narco-terrorist and drug-trafficking chains?
5. How have organizations, such as the FATF, helped the United Nations in stopping the funding of terrorists groups and, specifically, narco-terrorism?
6. How can the United Nations intervene into major opium production countries and areas, such as the Golden Triangle and Golden Crescent?

Sources:

1. "A GLOBAL OVERVIEW OF NARCOTICS-FUNDED TERRORIST AND OTHER EXTREMIST GROUP ", *The Library of Congress,* May. 2002, https://www.loc.gov/rr/frd/pdf-files/NarcsFundedTerrs_Extrems.pdf
2. *A/RES/72/246 - E - A/RES/72/246*, undocs.org/en/A/RES/72/246.
3. *A/RES/62/194 - E - A/RES/62/194*, undocs.org/en/A/RES/62/194.
4. Author Kendall Sarita. "South American Cocaine Production." *Cultural Survival*, 1 Dec. 1985, www.culturalsurvival.org/publications/cultural-survival-quarterly/south-american-cocaine-production.
5. "The Commission on Narcotic Drugs." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/commissions/CND/index.html.
6. "Drug Trafficking and the Financing of Terrorism." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/frontpage/drug-trafficking-and-the-financing-of-terrorism.html .

7. “EU Fight against Terrorism.” *Consilium*, 16 June 2020, www.consilium.europa.eu/en/policies/fight-against-terrorism/.
8. “Narco-Terrorism: The Merger of the War on Drugs and the War on Terror.” *Emma Bjornehed,* August 2004*,* https://www.diplomatie.gouv.fr/IMG/pdf/drogue-terreur.pdf
9. “The Enduring Legacy of Reagan's Drug War in Latin America.” *War on the Rocks*, 20 Dec. 2018, warontherocks.com/2018/12/the-enduring-legacy-of-reagans-drug-war-in-latin-america/.
10. Felbab-Brown, Vanda. “Afghanistan's Opium Production Is through the Roof-Why Washington Shouldn't Overreact.” *Brookings*, Brookings, 21 Nov. 2017, www.brookings.edu/blog/order-from-chaos/2017/11/21/afghanistans-opium-production-is-through-the-roof-why-washington-shouldnt-overreact/.
11. Kiran Moodley @kirancmoodley. “Welcome to the Centre of the World's Drug Trafficking.” *The Independent*, Independent Digital News and Media, 11 Mar. 2015, www.independent.co.uk/news/world/asia/welcome-to-the-golden-triangle-the-centre-of-the-worlds-drug-trafficking-10100420.html.
12. “MMP: Revolutionary Armed Forces of Colombia (FARC).” *FSI*, cisac.fsi.stanford.edu/mappingmilitants/profiles/revolutionary-armed-forces-colombia-farc.
13. “Making Bad Economies: The Poverty of Mexican Drug Cartels.” *Oxford Research Group*, 16 Sept. 2019, www.oxfordresearchgroup.org.uk/blog/making-bad-economies-the-poverty-of-mexican-drug-cartels.
14. “ONDCP Releases Data on Poppy Cultivation and Potential Opium Production in Afghanistan.” *The White House*, The United States Government, www.whitehouse.gov/briefings-statements/ondcp-releases-data-poppy-cultivation-potential-opium-production-afghanistan/.
15. “Opium”, *Department of Justice/Drug Enforcement Administration*, June 2020, https://www.diplomatie.gouv.fr/IMG/pdf/drogue-terreur.pdf
16. “Terrorist Financing in West And Central Africa” *FATF,* Oct. 2016, https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-West-Central-Africa.pdf
17. Commander Dario E. Teicher, “The Decisive Phase of Colombia’s War on Narco-Terrorism”, US Air Force Counterproliferation Center ,https://media.defense.gov/2019/Apr/11/2002115494/-1/-1/0/28THEDECISIVE.PDF
18. “Pablo Escobar.” *Biography.com*, A&E Networks Television, 29 Aug. 2019, www.biography.com/crime-figure/pablo-escobar.
19. “Terrorism Prevention.” *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/terrorism/index.html.
20. “UN, United Nations, UN Treaties, Treaties.” *United Nations*, United Nations, treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&lang=en.