Cerritos Novice Conference 2020

Ad Hoc on Terrororism

Topic : Cyberterrorism

Director: Paul Sherdsuriya

October 10th, 2020

To Delegates of CHSMUN Novice 2020

Dear Delegates,
Welcome to CHSMUN Novice 2020!

It is our highest honor and pleasure to welcome you all to our 2020 online novice 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 virtual novice 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. CHSMUN Novice 2020 will provide a quality experience for beginner delegates to develop their speaking and delegating skills.

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

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: 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.

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/.