CIMUN 2017

The Cathedral International Model United Nations, 2017

Interpol

Agenda A: Averting Global catastrophe arising from Cyber Terrorism.

Agenda B: Combating crimes related to the manufacture and sale of illicit drugs.

Table of Contents

Message from the Secretary General

Dear Delegates,

It is with immense pleasure that I welcome you to the 6th annual session of the Cathedral International Model United Nations. The Cathedral International Model United Nations is a CVSL student led event to be held from the 22nd of September to the 24th of the same month. This year in its 6th session CIMUN will be crossing boundaries it has never crossed before, and you, the delegates, shall be the ones to witness and enjoy a newer, grander CIMUN.

Four years ago, I was introduced to the concept of a simulated UN conference for students to engage in worldly affairs and rectify issues which challenge the existence of world peace. The UN, although it may be deemed by many as a failed organisation, has since its inception been an eminent peace keeper in the international scene as well as in many cases, the local scene. The UN plays an important role in our lives, whether we see it or not- ergo MUNs were started for students like you and me, to recognise the importance of the organisation and to understand the functioning of the same.

I proudly owe my enthusiasm about MUNs to my first MUN- which happens to be the second session of CIMUN. Since then My MUN career has soared through new heights and hasn't looked back ever since. It is a pleasure to head the same MUN which had launched me into the world of public speaking, internationalism and diplomacy, and I assure that this year's CIMUN will exceed the already high standards set by previous sessions of CIMUN.

I am glad to announce that CIMUN will be host to five UN committees as well as one external body. Whether you are a space geek, arms fanatic or a person like me who loves to engage in world trade policies and crises, CIMUN is the event you should keep your calendar reserved for. On the 22nd of September prepare to take the scenic drive to Lonavala, where for three days you would be stepping into the shoes of country leaders to "take the initiative and make the difference" and at night you would be partying away at the delegate ball hoping to create strong relations with other country representatives to aid you in moving forward your policies in committee sessions.

This will be my fifth CIMUN, and I could not be more honoured to serve on the secretariat with some of the most talented, hardworking and creative people I know. I hope to see an exciting, stimulating and productive conference this September.

I look forward to seeing you at CIMUN this fall!

Suraj Vijay Harjani,

Secretary General,

Cathedral International Model United Nations 2017.

Message from the Director of Interpol

Dear Delegates,

With rapid advancements in technology in the recent years, crimes across the internet and networks have increased. Also there have been an increase in crimes due to the manufacturing and selling of illicit drugs. And this is where this committee comes in, to combat and fight against these crimes. I welcome you to the International Police Committee. The purpose of this committee is to police the world.

My name is Kashish Dewnani, and am a 12th grade student at the Cathedral Vidya School Lonavala. I enjoy swimming and exploring the world of poets and I would love to travel the world. My favourite series are Harry Potter and Percy Jackson and I also love writing poems. Your deputy directors are Ronak Tanna and Arushi Dahiya. Ronak is an amazing footballer and enjoys travelling around the world. In his free time he enjoys watching Big Bang Theory. Arushi, an avid reader and film enthusiast is a division level basketball ball player intent on exploring the world. She can often be found engrossed in researching about things that fascinate her or tangled in the world of her favourite YouTubers.

We will be expecting intelligent, high quality debate from the delegates and solutions to the problems discussed in the committee based on their country's stand. Also, delegates are urged not to restrict themselves to only the study guide, but research from various sources, and understand the points of views and solutions which apply to the agendas.

I hope that the committee will be a positive and successful experience. Let us strive towards creating a peaceful and safer world, where not violence and crime but cooperation and understanding will lead to solutions.

Good luck, and have fun!

Kashish Dewnani

About Interpol

Interpol is the world's largest international police organisation. Its role is to enable police around the world to work together to make the world a safer place. Their high-tech infrastructure of technical and operational support helps meet the growing challenges of fighting crime in the 21st century. Interpol:

- Supports the police worldwide
- Aims to facilitate neutrality
- Connects the police worldwide
- Prevents and fights crime through cooperation and innovation.

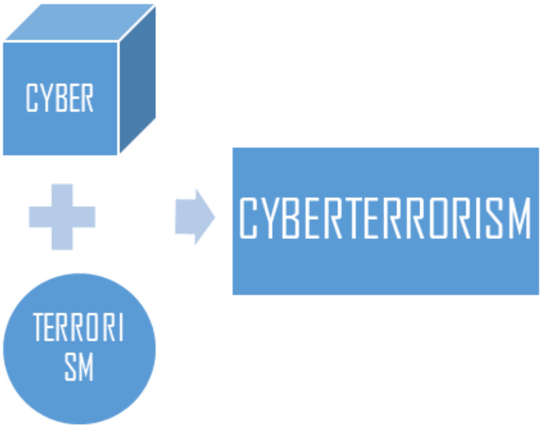
Agenda A: Averting Global catastrophe arising from Cyber-Terrorism.

Cyber-Crime Vs. Cyber-Terrorism:

Cyber-crime is a term for any illegal activity that uses a computer, phone, digital notepads, or any other technological device that stores data or uses modern telecommunication networks, to commit offences against individuals or groups of individuals. Cyber-crime usually involves a criminal motive to intentionally harm the reputation of the victim or cause physical, financial, mental harm, or loss, to the victim for the criminals own personal gain.

Cyber-terrorism is a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society for an ideological goal. A cyberterrorist attack can often be designed to cause extreme financial harm.

Cyber describes something relating to or characteristic of the culture of computers, information technology etc.



Terrorism is a term used to describe the use of intentional indiscriminate violence to create or fear, to achieve a political, religious, or ideological aims

terror

The difference between the two is the reason for committing the crime. For example: A criminal may take over the entire system of a nuclear power-plant and hold it for ransom while a terrorist may use the access to the system for destructive purposes

Beginning of cyber-terrorism:

In recent times, human lives have become highly technology oriented. Due to technological advancements, people have switched from the traditional payment method of using cash to making online transactions and online payments through their bank account. This can be accredited to the numerous advantages that online transactions convey. With this convenience granted, there remains the opportunity cost of security. Hackers utilize the cyber world to get unguarded information.

If a crime has been committed in the cyber world, it may most likely be unknown to the victim which makes it dangerous and unsafe for the victim. Cyber-crime is very difficult to stop and control and as a result it has extended to the degree of cyber-terrorism.

Cyber terrorism started in the late 20th century but has become a more drastic issue since 2006. For example: in December 2006, NASA was forced to block emails with attachments as they were afraid that they would be hacked and, at the same time, it was reported that the plans for the US space launch were obtained by foreign intruders.

History of cyber-terrorism:

Some of the earlier examples of cyber terrorism attacks are in 1996, when a computer hacker, who claimed to be linked with the White Supremacist movement, temporarily disabled and damaged a Massachusetts Internet Service Provider (ISP) while sending out worldwide racist messages under the ISP's name.

In 2000, someone hacked into Maroochy Shire, Australia waste management control system and released millions of gallons of raw sewage on the town.

As technology improved and became more common and popular worldwide, terrorists' trends shifted and they started using cyberspace to aid terrorism. They use the cyber world for recruitments, to attain money illegally or to spread false rumours. They may use web sites to coordinate with members and recruit young supporters to expand their attacks.

For example: In October 2010, there were malwares that disrupted the Siemens industrial control systems, discovered in Iran and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear programme.

Citigroup, one of the largest financial giants in the world, provides an ample incentive for hackers to organize an attack due to the vast amount of wealth and sensitive information that flows through the company daily. In 2011, over 200,000 customer information from contact details to account numbers were compromised, which resulted in $2.7 million loss for the company.

Examples of cyber-terrorism:

Terrorism can occur over the public internet, over private computer servers, or even through secured government networks. There are many ways in which a criminal could use electronic means to incite fear and violence. It's far less expensive to purchase a computer than to access guns or bombs, making this approach appealing for many potential criminals worldwide. It can be anonymous and conducted from a great distance away from the target. For a few examples, consider these situations:

- Foreign governments may use hackers to spy on U.S. intelligence communications in order to learn about where their troops are located or otherwise gain a tactical advantage at war.
- Domestic terrorists may break into the private servers of a corporation in order to learn trade secrets, steal banking information, or perhaps violate the private data of their employees.
- Global terror networks may disrupt a major website in order to create a public nuisance or inconvenience, or even more seriously, try to stop traffic to a website publishing content with which they disagree.
- International terrorists could try to access and disable signals which fly drones or otherwise control military technology.

Viruses and Malware:

Viruses, malware, adware, and Trojans are a nuisance for everyday computer users. These can be used to steal personal information from users. Methods of deployment include: infected documents, virus attachments in emails and when a website is hacked so that when a user visits it, it can inject a

malicious code into computers. Not only do hackers, criminals and terrorists use viruses and malware to get information, but so do governments and their agencies in order to get information from other states.

The infrastructure of networks:

Anything that is interconnected electronically is vulnerable to cyber-terrorism. For example: in a banking system that has many branches, there has to be communication and connections and what cyber-terrorists do is that they find the weak spots in these connections and utilise them to destroy or cause havoc in the network system.

Effects of cyber-terrorism:

Cyber terrorist causes disruptions in systems and can cause financial chaos or be utilised along with physical attacks to cause confusion and delays to response. Effects can be:

- Disruption of peace between countries.
- Loss of sales during disruption.
- Increased costs
- Loss of trust between different states.

Cyber-terrorism doesn’t cause physical damage or pain but affects people psychologically. In a simulation-based study, the research team provides the first glimpse of how cyber terrorism affects the psychological and physiological well-being of its victims.

Dozens of test subjects were asked to sit in front of a computer and answer a series of random questions. As they filled out the questionnaire, their computer was “hacked” by “Anonymous” without the test subjects realizing that the attack was part of the experiment. Suddenly, the frightening mask of Anonymous appeared with a warning that their site would crash and sensitive personal data would be publicized to the world at large.

After a few more moments, a split Skype screen captured the computer showing a hooded, masked figure typing an unseen message on one side and a live feed of the test subject/victim on the other.

Finally, in the third stage of the experiment, the test subjects received a private text message on their personal cell phones: “You’ve been hacked,” and “Anonymous has acquired your contact list.”

Immediately before and after the simulated cyber-attacks, respondents gave the researchers a saliva sample to test the level of the hormone cortisol, a well-known physiological indicator of stress.

The results of the experiment were striking and pointed to a significant increase in psychological and physiological stress among those who experienced the simulated cyber-attack by Anonymous.

The same subjects also described how their sense of personal security was undermined and how they worried about future cyber-attacks significantly far more than the control group, which did not experience the simulated attacks.

"It is important to see how individuals who had previously waved off the threat of cyber terrorism were now significantly more attuned to the danger," noted Canetti.[1]

This is a small test to show the effects of cyber-terrorism. Cyber-terrorists do not intend to cause physical harm but instead intend to cause psychological distress. Terrorists can use the cyber-world to inflict fear amongst people so much so they listen to the terrorist's demands even if it leads to their death.

Terrorism has spread rapidly in the 21st century. Terrorists can use the internet to persuade people to commit crimes they don't want to do. These terrorists may persuade them by threatening them or encouraging them through their religious beliefs.

Cyber-terrorism does not on its own create substantial damage or cause extensive chaos to the world but accompanied with physical attacks, it can bring out the fear in civilians.

Cyber-terrorism and security measures:

How can we deal with terrorist activities in cyberspace? We can deal with it passively by defending ourselves and not causing harm to the attacker. Governments, banking companies and other businesses can utilize firewalls, cryptography, and intrusion detection to protect their information. It can also be dealt with by imposing huge penalties on cyber attackers such as exposure, prosecution, and counter attacks.

How can we prevent cyber-attacks? A system should be designed to protect itself from an attack. Attacks should be prevented before they occur and vulnerabilities should be found and fixed so that terrorists do not exploit them. With improved security and detections of cyber-attacks, it will be easier to protect information. Another way to prevent attacks is to take measures to ban them. Since people are law abiding, as they don't want to suffer consequences, there could be comparatively less malicious attacks and the fewer the attacks, the easier it will be to locate other perpetrators. Interception of an attack which is stopping the attack before it reaches the target can also help prevent cyber-attacks. This may be either cyber or physical. Information can be protected through passwords and firewalls but since these are easy to pass if access is given, the system should be protected physically too so that no damage occurs. There should be protection against attempts to cut cables or from electromagnetic pulses. This can be done through fences and biometrics. Since there are possibilities of catastrophic terrorism, it is important to prevent attacks and identify these attackers.

A short video for further reference - https://www.youtube.com/watch?v=L78r7YD-kNw

[1] SIEGEL-ITZKOVICH, JUDY. "Cyber Terrorism Triggers Severe Psychological, Physical Stress, Haifa Researchers Shows." *The Jerusalem Post | JPost.com*. N.p., 06 Apr. 2015. Web. 02 July 2017.

Agenda B: Combating crimes related to the manufacture and sale of illicit drugs.

Manufacture of Illicit Drugs:

The illegal drug trade is often described as a global black market that revolves around the cultivation, distribution and most importantly manufacture of drugs that are subject to drug prohibition laws. Most jurisdictions prohibit trade, except under license, of many types of drugs through the use of drug prohibition laws.

The United Nations Office on Drugs and Crime's *World Drug Report 2005* estimates the size of the global illicit drug market at US$321.6 billion in 2003. With a world, GDP of US$36 trillion in the same year, the illegal drug trade may be estimated as nearly 1% of total global trade. Consumption of illegal drugs is widespread globally.

Conviction/Circumstances

To be convicted of manufacturing (or intending to manufacture) illicit drugs, prosecutors are required to attest or verify both the possession and intent to manufacture. For instance, while possession of common cold medicines (often used in methamphetamine production) may not be enough to charge an individual with drug production, possession of these medicines in tandem with other methamphetamine chemicals, can result in a charge of drug manufacturing. Similarly, a man who is found in possession of marijuana may be subject only to a charge of drug possession. However, if he is also found to have multiple plants, or grow lights, on his property, he may be charged with drug manufacturing instead.

Drug Manufacturing Penalties

Punishment for the crime of drug manufacturing can be quite significant. Drug manufacturing is typically prosecuted as a felony, and often results in at least one year of prison, although sentences can be as high as ten years. Defendants may also face substantial fines, up to $25,000 or more. Under federal laws, punishment for the cultivation of marijuana plants can range from five years in prison for 50 plants to more than 25 years for 1,000 or more plants.

One common defense to drug manufacturing is that the defendant was a permit or license holder who is authorized to be in possession of certain precursor chemicals. Thus, for instance, many factories and businesses that use industrial chemicals common in drug production may be protected from a drug manufacturing charge because they possess permits allowing them to purchase and use these chemicals.

Types of Crimes Related to the Manufacture and Sale of Illicit Drugs:

Drug related crimes can involve crime against the person such as a robbery or sexual assault. Problematic crimes associated include shoplifting, property crime, drug dealing, violence and aggression and driving whilst intoxicated.

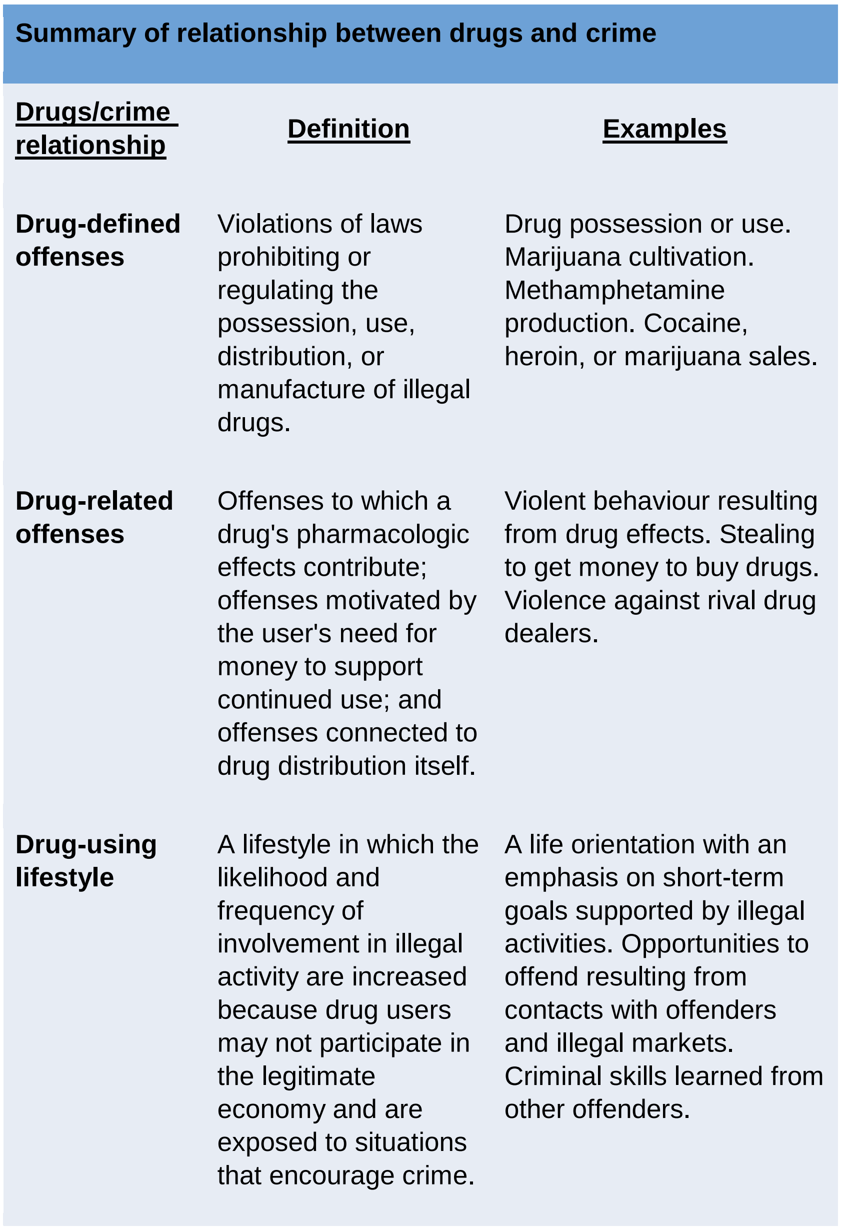
In 2002, in the U.S. about a quarter of convicted property and drug offenders in local jails had committed their crimes to get money for drugs

- Use-Related crime: These are crimes that result from or involve individuals who ingest drugs, and who commit crimes because of the effect the drug has on their thought processes and behaviour

  - Economic-Related crime: These are crimes where an individual commits a crime to fund a drug habit. These include theft and prostitution.

  - System-Related crime: These are crimes that result from the structure of the drug system. They include production, manufacture, transportation, and sale of drugs, as well as violence related to the production or sale of drugs, such as a turf war.

- Trafficking
- Benzodiazepines
- According to the National Drug Intelligence Centre, it's against the law for anyone to sell, import, or export any drug paraphernalia.



Summary of relationship between drugs and crime

Drugs/crime relationship	**Definition**	**Examples**
Drug-defined offenses	Violations of laws prohibiting or regulating the possession, use, distribution, or manufacture of illegal drugs.	Drug possession or use. Marijuana cultivation. Methamphetamine production. Cocaine, heroin, or marijuana sales.
Drug-related offenses	Offenses to which a drug's pharmacologic effects contribute; offenses motivated by the user's need for money to support continued use; and offenses connected to drug distribution itself.	Violent behaviour resulting from drug effects. Stealing to get money to buy drugs. Violence against rival drug dealers.
Drug-using lifestyle	A lifestyle in which the likelihood and frequency of involvement in illegal activity are increased because drug users may not participate in the legitimate economy and are exposed to situations that encourage crime.	A life orientation with an emphasis on short-term goals supported by illegal activities. Opportunities to offend resulting from contacts with offenders and illegal markets. Criminal skills learned from other offenders.

The annual Bureau of Justice Statistics (BJS) National Crime Victimization Survey (NCVS) asks victims of violent crimes who reported seeing the offender whether they perceived the offender to be under the influence of drugs or alcohol. According to the 1998 survey, 30 percent of victims could not determine whether the offender was under the influence of a substance. Of those who could decide, about 31 percent reported that the offender was under the influence of alcohol and/or drugs.

Related Problems:

The internet and the manufacture and sale of illicit drugs –

Among the many well-known criminal activities involving the Internet, drug trafficking has reached major dimensions. Internet-based drug trafficking includes the sale of illicit drugs and, increasingly, the illegal sale of pharmaceuticals containing narcotic drugs and psychotropic substances in recent years, the volume of illicit sales of narcotic drugs and psychotropic substances through websites has risen, making the Internet a major source of drugs for drug abusers. Many of the drugs are addictive; some are highly potent and their abuse can have fatal consequences. Concern has been expressed about the ease with which children and adolescents can obtain such drugs, using the anonymity afforded to them by the Internet. In addition, the quality of medicines purchased illegally through Internet pharmacies and other websites

Research Guidance

Do not stick to only the study guide. Please do your own research about your country and the agendas. Here are some helpful tips for the delegates for agenda A:

- Know your country's stance against cyber-attacks.
- Discuss ways to protect your civilians from a cyber-attack and thus global catastrophe.
- Ensure that you understand how Cyber-Terrorism is/has affecting/affected your country negatively.
- What measures can/will your country adopt to put an end to Cyber-terrorism?

Tips to delegates for Agenda B:

- Find out solutions to problems that your countries can implement.
- What type of drugs are illegally manufactured in your country?
- What drug related criminal activity has adversely affected your country?

Bibliography

Agenda A: Averting Global catastrophe arising from Cyber-Terrorism

https://www.linkedin.com/pulse/cyber-crime-v-cyber-terrorism-what-difference-matthew-kurnava

http://www.jpost.com/Israel-News/Health/cyber-terrorism-triggers-severe-psychological-physical-stress-Haifa-researchers-shows-396277

https://www.techopedia.com/definition/6712/cyberterrorism

Agenda B: Combating crimes related to the manufacturing and sale of illicit drugs.

https://www.incb.org/documents/Narcotic-Drugs/Guidelines/internet/NAR_guide_Internet_guidelines_English.pdf

https://en.wikipedia.org/wiki/Illegal_drug_trade

https://en.wikipedia.org/wiki/United_Nations_Convention_Against_Illicit_Traffic_in_Narcotic_Drugs_and_Psychotropic_Substances

https://www.unodc.org/documents/commissions/CND/Drug_Resolutions/2000-2009/2008/CND_Res-2008-11e.pdf

http://criminal.findlaw.com/criminal-charges/types-of-drug-crimes.html

https://www.justia.com/criminal/offenses/drug-crimes/drug-manufacturing/

http://www.policyalmanac.org/crime/archive/drug_related_crime.shtml