



GA-1
DISARMAMENT AND INTERNATIONAL
SECURITY
STUDY GUIDE

Forum: GA1/Disarmament Committee

Issue: Drug Trafficking

Student Officer: Didem Yıldırım

Position: President Chair

Letter from the President Chair

Hey, guys! I'm Didem

I am a junior in Samsun Fen Bilimleri and I will be attending MPALMUN'19 as the President Chair of DISEC. I believe that we all will have marvelous time during the conference. See y'all soon!

Introduction:

The illegal drug trade or drug trafficking is a global black market dedicated to the cultivation, manufacture, distribution and sale 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. Drug trafficking presents a social evil that has refused to go away despite numerous interventions by governments and concerned stakeholders across the world. This problem is mostly prevalent in America. Latin America is among the major producers of illicit drugs in the world. Besides being a big producer, Americans are also among the biggest consumers of drugs.

The rise in organized crime organizations commonly known as cartels in America are in charge of drug trafficking. Research indicates that Americans spend over 150 billion dollars on illicit drugs. This money could alternatively be used constructively. Drug trafficking is an issue that has generated heated debates from policy makers, government officials as well as the members of the public. This is because of the associated negative effects associated with drug trafficking. The detrimental effects of drug trafficking includes increased crimes, national instability and other economic issues among others.

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 alone. 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 and remains very difficult for local authorities to thwart its popularity.

The beginning of the 21st century saw drug use increase in North America and Europe, with a particularly increased demand for marijuana and cocaine. As a result, international organized crime syndicates such as the Sinaloa Cartel and 'Ndrangheta have increased cooperation among each other in order to facilitate trans-Atlantic drug-trafficking. Use of another illicit drug, hashish, has also increased in Europe.



Definition of Key Terms:

DEA: The Drug Enforcement Administration (DEA) is a federal law enforcement agency responsible for enforcing controlled substance regulations in the United States. DEA agents are tasked with reducing the availability of illicit controlled substances by thwarting organizations and the people who grow, manufacture and distribute them.

2018 National Drug Threat Assessment (NDTA): The 2018 National Drug Threat Assessment (NDTA) is a comprehensive strategic assessment of the threat posed to the United States by domestic and international drug trafficking and the abuse of illicit drugs. The report combines federal, state, local, and tribal law enforcement reporting; public health data; open source reporting; and intelligence from other government agencies to determine which substances and criminal organizations represent the greatest threat to the United States.

Drug Addiction: Drug addiction is a complex neurobiological disease that requires integrated treatment of the mind, body, and spirit. It is considered a brain disease because drugs change the brain — they change its structure and how it works. Without treatment, these brain changes can be long-lasting. Addiction is chronic, it is progressive, and if left

untreated, it can be fatal. Individuals struggling with drug addiction often feel as though they cannot function normally without their drug of choice. This can lead to a wide range of issues that impact professional goals, personal relationships, and overall health. Over time, these serious side effects can be progressive, and if left untreated, fatal.

Drug Trade: The illegal drug trade or drug trafficking is a global black market dedicated to the cultivation, manufacture, distribution and sale 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.

Synthetic Drugs: Synthetic drugs are created using man-made chemicals rather than natural ingredients.

Drug Cultivation: Drug cultivation is a type of drug crime involving the growing of plants that are classified as controlled substances. This usually refers to the illegal growing of plants like marijuana, opium, and other types of intoxicants or hallucinogenic plants.

Drug cultivation laws are usually classified under or alongside with drug manufacturing laws. For example, most “drug cultivation and manufacturing laws” make it illegal to:

- Grow, produce, or possess plants with naturally occurring substances that are used in the production of illegal drugs and controlled substances; and
- Produce illegal substances such as cocaine which are derived from plants

Drug Cartel: A drug cartel is any criminal organization with the intention of supplying drug trafficking operations. They range from loosely managed agreements among various drug traffickers to formalized commercial enterprises. The term was applied when the largest trafficking organizations reached an agreement to coordinate the production and distribution of cocaine. Since that agreement was broken up, drug cartels are no longer actually cartels, but the term stuck and it is now popularly used to refer to any criminal narcotics related organization.

Types of Drugs: There are seven different drug types, and each has its own set of effects and risks:

- Stimulants
- Depressants
- Hallucinogens
- Dissociatives
- Opioids
- Inhalants
- Cannabis

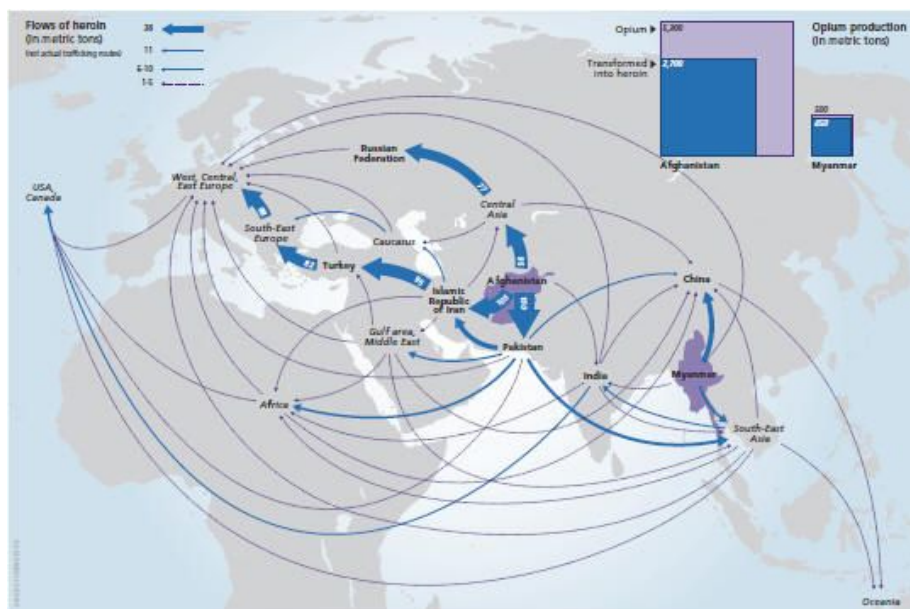
General Overview:

Drug trafficking is a global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws. UNODC is continuously monitoring and researching global illicit drug markets in order to gain a more comprehensive understanding of their dynamics. Drug trafficking is a key part of this research.

At current levels, world heroin consumption (340 tons) and seizures represent an annual flow of 430-450 tons of heroin into the global heroin market. Of that total, opium from Myanmar and the Lao People's Democratic Republic yields some 50 tons, while the rest, some 380 tons of heroin and morphine, is produced exclusively from Afghan opium. While approximately 5 tons are consumed and seized in Afghanistan, the remaining bulk of 375 tons is trafficked worldwide via routes flowing into and through the countries neighbouring

Afghanistan. The Balkan and northern routes are the main heroin trafficking corridors linking Afghanistan to the huge markets of the Russian Federation and Western Europe. The Balkan route traverses the Islamic Republic of Iran (often via Pakistan), Turkey, Greece and Bulgaria across South-East Europe to the Western European market, with an annual market value of some \$20 billion. The northern route runs mainly through Tajikistan and Kyrgyzstan (or Uzbekistan or Turkmenistan) to Kazakhstan and the Russian Federation. The size of that market is estimated to total \$13 billion per year.

Global heroin flows from Asian points of origin



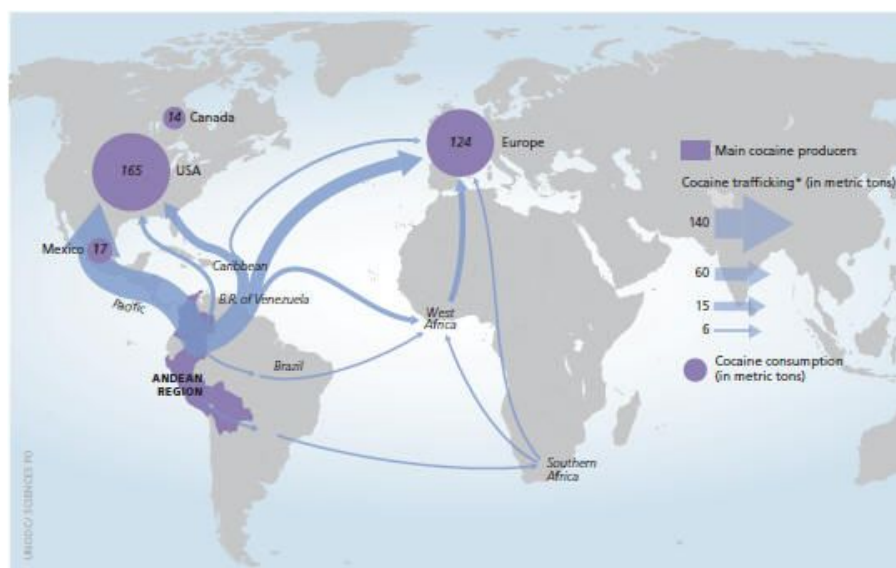
In 2008, global heroin seizures reached a record level of 73.7 metric tons. Most of the heroin was seized in the Near and Middle East and South-West Asia (39 per cent of the global total), South-East Europe (24 per cent) and Western and Central Europe (10 per cent). The global increase in heroin seizures over the period 2006-2008 was driven mainly by continued burgeoning seizures in the Islamic Republic of Iran and Turkey. In 2008, those two countries

accounted for more than half of global heroin seizures and registered, for the third consecutive year, the highest and second highest seizures worldwide, respectively.

In 2007 and 2008, cocaine was used by some 16 to 17 million people worldwide, similar to the number of global opiate users. North America accounted for more than 40 percent of global cocaine consumption (the total was estimated at around 470 tons), while the 27 European Union and four European Free Trade Association countries accounted for more than a quarter of total consumption. These two regions account for more than 80 per cent of the total value of the global cocaine market, which was estimated at \$88 billion in 2008.

For the North American market, cocaine is typically transported from Colombia to Mexico or Central America by sea and then onwards by land to the United States and Canada. Cocaine is trafficked to Europe mostly by sea, often in container shipments. Colombia remains the main source of the cocaine found in Europe, but direct shipments from Peru and the Plurinational State of Bolivia are far more common than in the United States market.

Main global cocaine flows, 2008



Following a significant increase over the period 2002-2005, global cocaine seizure totals have recently followed a stable trend, amounting to 712 tons in 2007 and 711 tons in 2008. Seizures continued to be concentrated in the Americas and Europe. However, the transition

from 2007 to 2008 brought about a geographical shift in seizures towards the source countries for cocaine. Seizures in South America accounted for 59 per cent of the global total for 2008, compared with 45 per cent in 2007.

Major Parties Involved and Their Views:

United States: Marijuana was a popular drug seen through the Latin American trade route in the 1960s. Cocaine became a major drug product in the later decades. Much of the cocaine is smuggled from Colombia and Mexico via Jamaica. This led to several administrations combating the popularity of these drugs. Due to the influence of this development on the U.S. economy, the Reagan administration began "certifying" countries for their attempts at controlling drug trafficking. This allowed the United States to intervene in activities related to illegal drug transport in Latin America. Continuing into the 1980s, the United States instated stricter policy pertaining to drug transit through sea. As a result, there was an influx in drug-trafficking across the Mexico–U.S. border. This increased the drug cartel activity in Mexico. By the early 1990s, so much as 50% of the cocaine available in the United States market originated from Mexico, and by the 2000s, over 90% of the cocaine in the United States was imported from Mexico. In Colombia, however, there was a fall of the major drug cartels in the mid-1990s. Visible shifts occurred in the drug market in the United States. Between the 1996 and 2000, U.S. cocaine consumption dropped by 11%.

In 2008, the U.S. government initiated another program, known as the Merida Initiative, to help combat drug trafficking in Mexico. This program increased U.S. security assistance to \$1.4 billion over several years, which helped supply Mexican forces with "high-end equipment from helicopters to surveillance technology". Despite U.S. aid, Mexican "narcogangs" continue to outnumber and outgun the Mexican Army, allowing for continued activities of drug cartels across the U.S.–Mexico border

The top 5 districts for drug trafficking in last 3 years are:

- Western District of Texas.
- Southern District of Texas.
- District of Arizona.
- Southern District of California.
- District of New Mexico.

Mexico: Corruption in Mexico has contributed to the domination of Mexican cartels in the illicit drug trade. Since the beginning of the 20th century, Mexico's political environment allowed the growth of drug-related activity. The loose regulation over the transportation of illegal drugs and the failure to prosecute known drug traffickers and gangs increased the growth of the drug industry. Toleration of drug trafficking has undermined the authority of the Mexican government and has decreased the power of law enforcement officers in regulation over such activities. These policies of tolerance fostered the growing power of drug cartels in the Mexican economy and have made drug traders wealthier. Many states in Mexico lack policies that establish stability in governance. There also is a lack of local stability, as mayors cannot be re-elected. This requires electing a new mayor each term. Drug gangs have manipulated this, using vacuums in local leadership to their own advantage.

Colombia: It was common for smugglers in Colombia to import liquor, alcohol, cigarettes and textiles, while exporting cocaine. Personnel with knowledge of the terrain were able to supply the local market while also exporting a large amount of product. The established trade that began in the 1960s involved Peru, Bolivia, Colombia, Venezuela and Cuba. Peasant farmers produced coca paste in Peru and Bolivia, while Colombian smugglers would process the coca paste into cocaine in Colombia, and trafficked product through Cuba. This trade route established ties between Cuban and Colombian organized crime. From Cuba, cocaine would be transported to Miami, Florida; and Union City, New Jersey. Quantities of the drug were then smuggled throughout the US. The international drug trade created political ties between the involved countries, encouraging the governments of the countries involved to collaborate and instate common policies to eradicate drug cartels. Cuba stopped being a center for transport of cocaine following the establishment of a communist government in 1959. As a result, Miami and Union City became the sole locations for trafficking.¹ The relations between Cuban and Colombian organized crime remained strong until the 1970s, when Colombian cartels began to vie for power. In the 1980s and 90s,

Colombia emerged as a key contributor of the drug trade industry in the Western Hemisphere. While the smuggling of drugs such as marijuana, poppy, opium and heroin became more ubiquitous during this time period, the activity of cocaine cartels drove the development of the Latin American drug trade. The trade emerged as a multinational effort as supplies (i.e. coca plant substances) were imported from countries such as Bolivia and Peru, were refined in Colombian cocaine labs and smuggled through Colombia, and exported to countries such as the US.

Timeline of Events:

1800s	During the mid-1800s, Chinese immigrants arriving in California introduced Americans to opium smoking.
1970s	In the late 1970s, the illegal cocaine trade became a major moneymaking opportunity throughout the world.
1975	In 1975, Colombian police seized 600 kilos of cocaine from a plane. Drug traffickers retaliated by killing 40 people during one weekend in what became known as the “Medellin Massacre.” The event triggered years of violence that led to assassinations, kidnappings and raids.
1982	Panamanian General Manuel Noriega allowed Medellin drug lord Pablo Escobar to ship cocaine through Panama.
1995	In 1995, top Cali cartel members were captured and arrested. A year later, all of the Cali kingpins were behind bars.
2013	In 2013, six substances accounted for nearly all drug trafficking offenses: powder cocaine, methamphetamine, marijuana, crack cocaine, heroin, and oxycodone.
2014	A 2014 report revealed Americans spent about \$100 billion a year over the previous decade on illicit drugs.

Recent Statistics on Drug Trafficking

- The DEA puts much of its focus on trafficking from Mexican drug cartels because not only do they control a large share of the drug smuggling into the U.S., they are also responsible for much of the drug distribution within the U.S.⁴
- Another emerging threat is Africa, as it is often used as a transit shipping point for South American and Asian drug organizations.
- Between 2011 and 2015, there was an almost 50% increase in the number of people sentenced for crimes related to heroin trafficking in the U.S.¹
- In 2015, the DEA made 6,353 arrests for heroin-related offenses. Conspiracy, distribution, and possession with intent to sell account for 84% of these arrests

6 drug types accounted for nearly all drug trafficking offenses:

- Methamphetamine: 33.6%
- Cocaine: 19.8%
- Marijuana: 17.6%
- Heroin: 14.4%
- Crack: 8.1%
- Oxycodone: 2.8%
- Other: 3.7%

Possible Solutions:

Decriminalisation of drugs: The artificially high profits of the illicit drug market provide a great incentive for drug cartels, which lead to gang wars and crime in order to gain or retain

a share of the black market for drugs. For this reason countries, and even sub national territories and cities have expressed a desire for decriminalisation in the past. These countries emphasize on the rehabilitation of the offenders and the promotion of drug-related education and awareness campaigns rather than prosecution. As such, they hope to spend fewer resources on tracking down criminals and incarcerating them, by concentrating instead on public health and education initiatives, which would be tackling the roots of the problem. Decriminalisation of drugs could be achieved by subjecting the production, trade and consumption of drugs to international regulations, which would mean that certain limits and conditions would be imposed and monitored.

Rehabilitation: Countries could provide rehabilitation to drug users and prevent the consumption of drugs by strengthening their systems of public health and social services. By ensuring that treatment is widely accessible, these countries would be able to undermine the illicit drug market and reduce the negative effects that widespread drug abuse causes on society. Another measure which will prove useful is the provision of psychological treatment to abusers in order to tackle to the underlying reasons for their addiction.

Education and Employment: By ensuring a proper education and a good work environment, states can ensure that people pursue other activities than drug cultivation. Training, internships and vocational skills can be offered to the young, unemployed or rehabilitated. Better education will also prove necessary to prevent the rise in the number of drug users, by making people understand the consequences of drug abuse and hence limit the demand for drugs. Education initiatives concerning drugs can be reinforced, along with the spreading the knowledge of the dangers of sharing hypodermic needles.

Alternative Development: Alternative development initiatives work on the assumption that reductions in opium and coca cultivation are conditional upon the general social and economic development of source areas and their integration into the nation state. As such the elimination of drug crop cultivation is often a positive externality of the process of enhancing food security, increasing household incomes and an improvement in the quality of life.

Alternative development via the introduction of substitute crops and diversified cropping patterns has disproved the myth that coca and opium offer the highest returns to small farmers. Substitution efforts in Northern Thailand have illustrated that annual profits per square metre can be increased by over 50 times by replacing opium with flowers. In the Chapare rubber has been found to accrue four times that of coca per hectare. In Buner, Pakistan household incomes were more than doubled through development efforts between 1976 and 1991 whilst opium cultivation had been all but eliminated since 1983. Moreover, Thailand's success in reducing the level of opium production has proved what development efforts can achieve where decades of coercion have failed. Current levels of production are half that produced in 1984 and only a quarter of that produced in the mid 1960's. Consequently, Thailand's programme is considered as one of the most effective in the world.

Bibliography:

<https://www.unodc.org/unodc/en/drug-trafficking/index.html>

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

<https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/drug-trafficking>

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&cad=rja&uact=8&ved=2ahUKewi62rT_zZXhAhXlxIUKHY6LC9IQFiAKeqQIBhAB&url=https%3A%2F%2Fdrugabuse.com%2Fstatistics-data%2Fdrug-trafficking%2F&usq=AOvVaw3Sh-hi6U4wv7JcN7I657wI

https://www.druglibrary.org/schaffer/history/drug_law_timeline.htm

<http://www.drugpolicy.org/issues/brief-history-drug-war>

<http://www.drugpolicy.org/issues/brief-history-drug-war>

<https://www.therecoveryvillage.com/drug-addiction/types-of-drugs/#gref>

Forum : Ga-1/ Disarmament and International Security(DISEC)

Issue: Future of Cyber Security

Committee Director: Eymen Ata Dursunoğlu

Position: Deputy Chair

Letter from the Deputy Chair

Hi everyone, My name is Eymen. I am a Junior in Samsun Fen Bilimleri High School. I am very much honored to be Chair of the DISEC committee of MPALMUN'19. When I was the freshman, I joined MUN club in my own school and I am saying that with no doubt It was the best decision of my life. Mun has been my passion for my high school life. I attended 9 conferences before and MPALMUN'19 will be my last conference and first charing experience.

In the upcoming days, we will discuss 2 crucial topics in our committee. I wrote a study guide about cyber security for you. I expect all of you to work hard and searching well. Please don't forget to look at the notes from the chair. They can be very essential and useful for you. If you have any question and concern, Please don't hesitate to send me a mail(eymenata2555@icloud.com). I am very excited to meet you all. I hope it will be amazing and delightful 3 days. See you soon!!

Introduction

Currently, we are living in the Cyber-age where Internet & computers have foremost impacts on our way of living and social life. The usage of information technology has posed great safety challenges and moral questions in front of us.

Cybercrime is a global problem that's been dominating the news cycle. It poses a threat to individual security and an even bigger threat to large international companies, banks, and governments. Today's organized cybercrimes far out shadow lone hackers of the past now large organized crime rings function like start-ups and often employ highly-trained developers who are constantly innovating online attacks.

With the expansion of the internet, network security has also become big anxiety. Cyber crimes have emerged quickly in the last few years.

Cyber-criminals are practicing day by day from stealing money and intellectual property, hacking into others computers, spreading viruses & worms to damage computers connected to the internet and with so much data to exploit out computers, Cybersecurity has become essential.

Definition of Key Terms

Cyber Attack: Although there is no internationally adopted definition, cyber attacks can be defined as all acts in cyberspace intended to cause harm.

Cybercrime: United Nations Office on Drugs and Crime (UNODC) Global Programme on Cybercrime defines cybercrime broadly as “having cyber-dependent offenses, cyber-enabled offenses and, as a specific crime-type, online child sexual exploitation and abuse.” This means that all crimes committed on cyberspace, or via the cyberspace are considered cybercrime.

Hacker: Someone who violates computer security for malicious reasons, kudos or personal gain.

Encryption: The transformation of data to hide its information content.

Virus: Malware that is loaded onto a computer and then run without the user’s knowledge or knowledge of its full effects.

Vulnerability: A flaw or weakness that can be used to attack a system or organization.

General Overview

At the same pace as our society is becoming more and more digitalized, there are also more and more ways to exploit this. We have everything from individuals and organizations looking to earn money illegally, to those who want to spy on countries/businesses/individuals, those who want to injure countries/businesses/organizations/individuals and those who just want to show that they can. The more serious threats can briefly be divided into groups:

- Hacking is a major cybercrime which is committed today. A hacker makes loopholes in operating systems to destroy the secure data and steal important details from the computer of the victim. Cracking or Hacking is normally done through the use of a ‘backdoor’ program

installed on your machine. A lot of hackers also try to get access to resources through the usage of password-cracking software.

- Viruses & worms are a large threat to normal users and business companies. Viruses are normally computer programs that are designed to damage the computer system. It is named “virus” because it spreads from one computer to another computer like a biological virus. A worm usually creates loopholes in the operating system.
- Kidnapping information is encrypting information and then demanding a ransom for its release. The trend is targeting businesses and organizations that have important information, such as hospitals and their patient records.
- Selling information found through espionage, such as credit card details, hospital records, accounts or passwords. This type of information is often attained by searching far and wide via the Internet for vulnerabilities that can be exploited.
- Espionage can also be employed to gain access to confidential information. The difference between this and when the goal is to acquire money is that the attacks are directed towards accessing specific information.
- Phishing, i.e. false email used to trick people into providing information, can either be utilized to steal money or be sold. The trend here is focusing on directed attacks, so-called spear phishing, against selected persons that can produce a high yield.
- DDoS, where a large number of computers are instructed to overload services and websites so that others cannot access them. This is most often done to injure the owner of a service or website.

- Intrusion for the purpose of causing general or more specific damage by breaking into a system to spread disinformation.
- Attacks designed to alter or knock out all or parts of systems. The final points are common ingredients in extreme scenarios such as cyber wars and terrorism but are also methods employed by activists and bored hackers. The threats are increasing on all these fronts, but the same applies to awareness and technical aids.

Solutions and Technologies to Avoid Cyber Crime

This is an important question arises about how these cyber crimes can be prevented. A variety of techniques & solutions have been used but the problems still exist and are increasing day by day.

Antivirus and Antispyware Software:

antivirus software is a computer program that attempts to identify and prevent computer viruses and other malicious software. Anti-spy wares are used to block backdoor program, Trojans & other spy wares to be installed on the computer system.

Firewalls:

A firewall protects from unauthorized access to a computer network. Firewalls may be hardware devices, software program or a combination of both hardware & software. A network firewall typically protects an internal computer system against malicious access from outside the network.

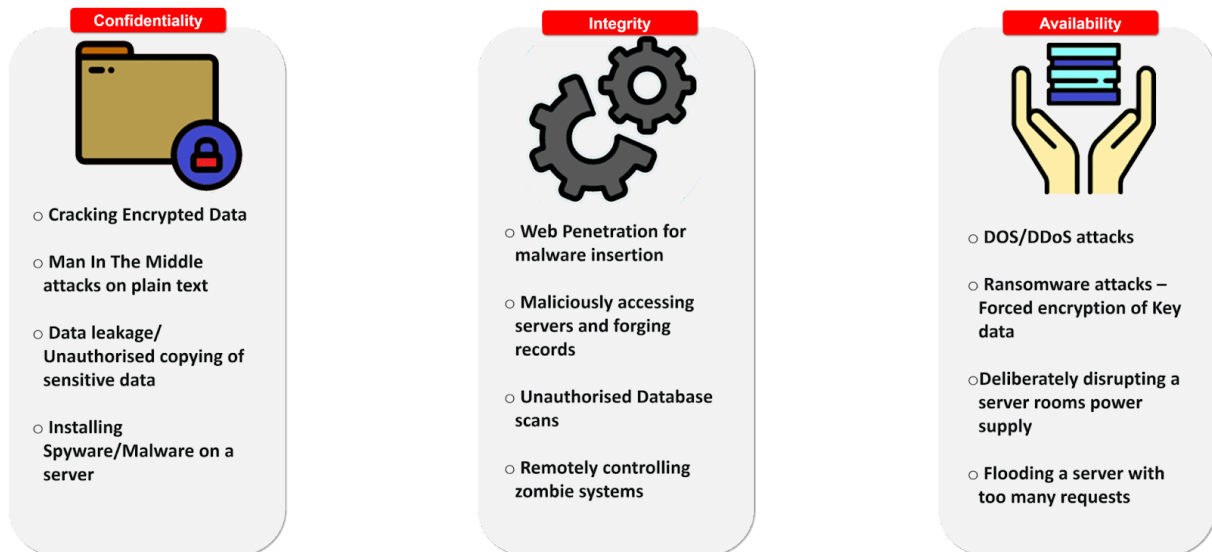
Cryptography:

Cryptography is the method of encrypting & decrypting of secure information. Encryption is like sending a postal mail to another party with secure lock code on the envelope which is known only to the sender & the recipient. There are a number of cryptography methods that have been developed and many of them still have not been cracked.

The CIA Triad:

The CIA triad which stands for Confidentiality, Integrity, and Availability is a design model to guide companies and organizations to form their security policies. It is also known as the AIC triad to avoid confusion with the Central

Intelligence Agency(CIA). The components of the triad are considered to be the most important and fundamental components of security. These are the briefs about this triad:



Confidentiality

Confidentiality is the protection of personal information. Confidentiality means keeping a client's information between you and the client, and not telling others including co-workers, friends, family, etc.

Integrity

Integrity, in the context of computer systems, refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification.

Availability

Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format.

QUANTUM TECHNOLOGY:

One of our most important technical aids for protecting information is encryption. Using encryption, information can be hidden, fidelity proven and personal identity verified. A challenge that many are presently studying is how encryption should be adapted for a world where we have many connected devices that may not have all that much calculative capacity, memory and

electrical power. This is a major challenge but many have taken it on and the technology will be developed in the near future.

An interesting development that has to be considered if we look 10 to 20 years into the future is how quantum technology will affect the encryption methods we use. There are two different encryption methods, symmetric and asymmetric. Symmetric encryption will be weakened by quantum computers, but with longer encryption keys, it can still be used. The algorithms presently used for asymmetric encryption will, however, lose all their security and it is these asymmetric encryption algorithms that much of today's e-commerce, e-identities and certification management are based on. Here it is important to follow development so that these algorithms can be replaced before quantum computers become reality.

Major Parties and Organizations Involved

Russia

Britain, Australia and New Zealand have accused the Russian military intelligence of carrying out cyber attacks. "British Foreign Secretary Jeremy Hunt said in a statement Thursday that the country's National Cyber Security Centre (NCSC) had found out that Russian GRU intelligence service operations were behind cyber attacks believed to have cost the global economy millions of dollars" (CNN). The alleged state-sponsored attacks included the aforementioned DNC attack, as well as hackings of global agencies. Russia has not commented on any alleged involvement.

China

China has also been accused by other countries of hacking global agencies and exposing sensitive information. Chinese hackers were found to expose the European Union's communication systems. The US also has accused them of stealing documents from the US Navy, including missile plans. The Norwegian software firm Visma also revealed that hackers from the Chinese Ministry of State Security had targeted the company to steal trade secrets from the firm's clients" (CSIS). China has also not commented on their involvement in these attacks

India

India has focused on cyber-crime and terrorism in their foreign policy last year. As most of the stated countries, India has invested a large amount of money (500 million dollars) into the development of software, defense, and the slow development of a military branch dealing with cyber terrorism. Furthermore, India holds an annual conference to monitor the advances of this military unit.

Africa

Africa along with Latin America hasn't been the subject to many major cyber attacks, however along with Latin America, Africa's economy is growing significantly and is becoming a major player in the economic sector. This makes it a target for cyber attacks and has next to none major policies regarding this issue. The continent of Africa needs a collective agreement like the EU however putting something like that into place as the same reasons as Latin America.

European Union

All of Europe combined invests 734 million dollars in defense and new software and officially hosts an annual conference in which all the state officials and EU members meet and discuss the technological advances.

United States

While speaking at a press conference in G20 summit in China, the former President Barack Obama said: "the nation he leads has the world's foremost cyber arsenal in the world." This might be actually true given the sophistication of cyber attacks allegedly carried out by the US. In fact, 17.12% of cyber attacks are initiated by the US. As per various estimates, the US accounts for nearly 10% of the world's malicious digital traffic. It is home to many famous and infamous hackers.

Brazil

It was last year's hacking attempt at the Rio Olympics that brought Brazilian hackers into the limelight. In fact, Brazil has the highest cyber attack traffic not only in South-America but the entire southern hemisphere. Approximately, 8.60% of cyber attacks are initiated by Brazilians. The reason behind the growing numbers of cybercriminals in Brazil is the cashless nature of its economy.

International Telecommunication Union (ITU)

The International Telecommunication Union is a specialized agency of the United Nations (UN) that is responsible for issues that concern information and communication technologies. The ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world, and assists in the development and coordination of worldwide technical standards. The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in a fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks. The agency also organizes worldwide and regional exhibitions and forums, such as ITU Telecom World, bringing together representatives of government and the telecommunications and ICT industry to exchange ideas, knowledge and technology. ITU, based in Geneva, Switzerland, is a member of the United Nations Development Group and has 12 regional and area offices in the world. ITU has been an intergovernmental public-private partnership organization since its inception. Its membership includes 193 Member States and around 800 public and private sector companies, and academic institutions as well as international and regional telecommunication entities, known as Sector Members and Associates, which undertake most of the work of each Sector.

Timeline of Events and UN Involvement

6 August 1991	The Invention of the Internet
22 January 2001	The UN General Assembly debated Resolution 55/63, the first resolution on cybersecurity and information technologies.
3 April 2012	The UN General Assembly passed Resolution 65/230, requesting the Commission on Crime Prevention and Criminal Justice to establish an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States
February 2013	The draft of the study requested by 65/230 was published with the help of the UNODC.
17–18 June 2013	The attending countries agreed to cooperate on cybersecurity in the 39th G8 Summit.
2013	The Global Programme on Cybercrime was established with the mandate of helping countries tackle cybercrime in a holistic manner.

United Nations Office on Drugs and Crime (UNODC) is the UN body that tackles this issue. As stated on their mandate, “UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness-raising, international cooperation, and data collection, research and analysis on cybercrime.” The body oversees the Global Programme on Cybercrime as well as the Open-ended Intergovernmental Expert Group on Cybercrime.

Relevant UN Documents

Combating the criminal misuse of information technologies, January 2001 (A/55/63)

United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) Resolution on Cybercrime (Vienna, 12 -19 May 2010)

United Nations Congress on Crime Prevention and Criminal Justice Resolution on Cybercrime (Brazil, 12-19 April 2010)

Twelfth United Nations Congress on Crime Prevention and Criminal Justice, April 2011 (A/65/230)

Treaties and Events

It should be stated that there is no international convention on cybercrime, the regional ones are demonstrated on the map above. (UNODC Study on Cybercrime,2013)

According to the 2013 Comprehensive Study on Cybercrime, globally, 82 countries have signed and/or ratified a binding cybercrime instrument.

The Council of Europe Convention on Cybercrime is the most used multilateral instrument for the development of cybercrime legislation.

Evaluation of Previous Attempts to Resolve the Issue

All past attempts at solving the issue have been limited in region and scope. The UN resolutions have focused primarily on forming expert groups to prepare a report on the issue. However, the time to act is now. With the data collected, solid action should be taken, as will be discussed below.

Possible Solutions

The most significant necessary steps are legal measures to prevent and combat cybercrime. Criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability are all issues that need to be solved.

At the national level, cybercrime tends to focus on criminalization. The need for legislation in investigative measures, a jurisdiction of police forces and collecting evidence is evident. Furthermore, the perpetrators of cyber attacks should be penalized internationally.

With the issue of cybercrime and cyber attacks being so broad, the measures are taken to prevent them have to be focused yet all-encompassing to be effective. One of the most important measures that need to be taken is to establish global definitions of these terms, as one does not exist already. Establishment of a convention and criminalization are other necessary steps that need to be taken.

Notes from the Chair

Although this issue may seem abstract as there is no clear chronological development, please take a look at the UNODC report ([linked here](#)) to grasp the issue in its entirety.

Also, you can find more information in Global CyberSecurity Index([linked here](#)) published by ITU(International Telecommunication Union)

Bibliography

<https://www.edureka.co/blog/what-is-cybersecurity/>

<https://www.quora.com/What-is-cyber-security>

<https://combitech.com/news-inspiration/stories/the-future-of-cyber-security/>

<https://securitytoday.com/Articles/2017/03/03/Top-5-Countries-Where-Cyber-Attacks-Originate.aspx?m=1&Page=1>

https://www.nato.int/cps/en/natohq/topics_78170.htm

https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf

www.unsystem.org/content/action-cybersecuritycybercrime

<https://www.bbc.com/news/topics/cp3mvdpd1r2t/cyber-attacks>

<https://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Glossary-of-cyber-security-terms/>

https://www.researchgate.net/publication/50273874_Privacy_and_Data_Protection_in_Cyberspace_in_Indian_Environment