Forum: Commission on Crime Prevention and Criminal Justice (CCPCJ)

Issue: Cybercrime prevention and other illicit uses of the internet in a changing world

Student Officer: Tanya Dwivedi and Shivom Dhamija

Position: Deputy President

Introduction

A recent and evolving form of transnational crime, one which can be committed anonymously, is expressed as cybercrime. The complex nature of the crime, as it occurs in the borderless realm of cyberspace constitutes the incline of parties involved in organized crime. Perpetrators involved in cybercrime and their victims can be located anywhere in the world, the two individuals/groups do not need to be in the same region. Correspondingly, this creates a ripple-effect throughout societies globally, and hence, the need for an urgent, dynamic and international response cannot be stressed enough.

Even though most cyber crimes are committed as a form of generating profit for cybercriminals, some are carried out against specific computers or devices, to directly damage (or disable) them. A primary impact that cybercrime entails is financial, and these include a variety of profit-driven attacks such as ransomware attacks, email and internet fraud, identity fraud, attempts to steal financial accounts; credit cards or other payment card information. Cybercriminals also target private and personal information, and this includes corporate data which is for theft and resale. Another aspect of cyber crime is its use in child abuse and exploitation.

However, due to increasing involvement in organized crime and general crime through the internet and its ambiguity because of the lack of regulations on international webspace is becoming a tremendous problem. There is a major deficiency of security on the internet and it is essential to consider the factors that play a role in maintaining the cybercrime world and finding ways to combat these attacks. As this has been a long-lasting issue with severe impacts, there have been previous attempts to resolve it and its significance has been recognized, though they have not eradicated the issue as a whole - it remains to be a matter that is affecting the world largely.
Definition of Key Terms

Cyberspace

Essentially the Internet; the online world on computers and other devices that use the Internet to function. The cyberspace is a requirement to be able to commit a cybercrime.

Organized crime

A group of individuals who are professional criminals, and work together to form a powerful and secret organization to engage in criminal activity.

Cyber-dependent crime

Cyber-dependent crimes or pure-cyber crimes are those crimes which occur exclusively via the internet. This includes the spread of viruses, malware, phishing, spam, etc. which are done using a computer on a network.

Cyber-enabled crime

A crime that can occur whilst people are offline, however, can also be facilitated through the means of information and communications technology. These crimes involve online frauds, purchases of drugs online and online money laundering.

Darknet

A generalized term used to describe the sections of the Internet that are deliberately concealed from the public or obscure networks whose layout (structure) seems to be superimposed on that of the Internet.

Hacking

An attempt to gain unauthorised access to or control over computer network security systems for the purpose of exploitation or extortion.

Copyright infringement

As per the federal U.S. Copyright Act, the infringement of copyright is a violation, piracy or theft of a rightful holder’s work or material.
Background Information

As cybercrime continues to expand as a covert means for criminals to resort to due to weak counter cyber terrorism measures in many parts of the world. It is a rapidly evolving, large impact for small groups of cybercriminals, and governments response to the changing nature of each cyber attack is slow. Essentially, it is important to realize that there are various forms of cybercrimes and cyberattacks. Each cybercrime-type has its effects on different areas within the society - such as identity theft having an impact on privacy security on the internet (and social media) - and to commit a cybercrime there must be a technique (cyberattack) implemented (i.e. password attack or phishing for identity thefts). Furthermore, there are severe impacts that businesses, individuals and nations are facing due to the existence of cybercrime, and most are negative impacts, especially towards national security and data breaches in companies, and child abuse.

Types of cybercrimes

There are several forms of committing cybercrimes and these involve different types of cyber attack strategies (discussed later). However, it is important to understand the types of cybercrimes taking place to manifest ways in which these the issue of cybercriminal activity can be resolved. This section looks into these types of crimes found within cyberspace and how they impact the general society; businesses, people and nations.

Identity theft

Identity theft is a type of cybercrime which involves pretending to be someone else in order to gain access to their personal information, including passwords and bank account information. According to a 2017 study by identity force, which is an American organization that provides Identity Theft protection software, about 1 in 15 people have been victims of identity theft, estimating to a shocking statistic of a new identity theft every 2 seconds. In recent years, there has been a constant increase in identity theft happening around the globe, leading to victims having huge financial losses and leak of their personal information. By far, the most severe consequence is the loss of personal funds and often involves the victim left financially devastated as it can take a long time for the person to even detect the fraud. Moreover, the stress and fear of financial security may have a detrimental impact on a person’s health and mental condition.

Software piracy
Software piracy involves illegally duplicating original content and making it available to billions of people via the internet. This content usually include books, music, movies, software, etc. which are rapidly pirated on a large scale and made available using torrents. Due to this copyright infringement, creators who create original content suffer significantly on their income as their content gets illegally mass-produced. Some notable examples include using cracked versions of software like MS Office and even unofficial system software such as Windows. This leads to getting the software for free due to illegal pirated copies online while giving no credit to the owner of them leading to significant financial loses.

**Hacking**

Hacking refers to the partial or complete control of the computer or a network. It is usually used to breach privacy and get access to sensitive data. It is often done on a large scale to huge businesses and governments. A notable example includes Sony, in April 2011, whose servers got hacked leading to leaking of personal data of over 77 million users of the Sony Playstation Network, including banking details which were also compromised. Sony suffered significant losses and had to close down for a month and pay for all the loses the users faced leading to significant financial loss. Hacking involves identifying weaknesses in computer networks and then exploiting them to the advantage of the hacker. Hacking is very commonly used to commit cybercrimes such as fraud, privacy invasion, extracting essential personal data, and lead to a loss of billions in revenue to huge businesses.

**Cyber espionage**

Cyber Espionage or commonly called cyber spying is a cybercrime involving stealing of sensitive date and property via the internet without the knowledge of the user it is being stolen from. Cyber espionage is carried out by the highly skilled hackers from around the globe who use cyber warfare to gain access and take control of military and government secrets, which are highly confidential.

**Cyber extortion**

Cyber extortion is the method through which criminals threaten victims by holding onto one’s data, website, computer system, or other sensitive information, in order to ensure the victim meets their demand for payment. This type of cybercrime typically involves the use of ransomware and distributed denial-of-service (DDoS) attacks, both of which have disastrous effects. An example of how ransomware is employed to implement cyber extortion would be, a hacker tricking one of the employees at a firm into clicking into an attachment within an email. Hence initiating the ransomware that infects the network, thereby encrypting the firm’s servers,
which does not permit anyone’s access except for the hacker - the only way to gain access to this information is through paying the hacker for the encryption key.

**Cryptojacking**

The illegal use of an individual's device (computer) to mine cryptocurrency is also known as cryptojacking. Essentially, this is a method that hackers use to convince the victim to either, enter a malicious web page via an email which loads the crypto-mining (mining for cryptocurrency) code onto the computer system, or by creating an online advertisement with Javascript code that automatically loads the code in the victim's browser. As cryptocurrencies are a recent exploration many individuals have delved into; a noticeable increase of 8500 per cent of attacks involving cryptojacking occurred in 2017, as per Symantec.

**Credit card frauds**

A credit card fraud occurs when someone makes a purchase or payment via the victim’s credit card without authorization. However, the cybercrime version of this fraud would be when a criminal steals one’s credit card account number, PIN and security code, and then makes these unauthorized transactions, and all of this can be implemented without needing the physical credit card (also known as card-not-present frauds). According to Varonis Systems, 41 per cent of companies have more than 1000 sensitive files including credit card numbers and health records left unprotected. Due to this form of irresponsibility and carelessness of companies, there are multiple ways for hackers to conduct a form of credit card fraud, and these are impacting people and businesses every day.

**Child abuse and exploitation**

Child exploitation is the commercial exploitation of children, perpetrated by adults for the financial benefit of individuals or criminal organisations. This can be done by exchanging pictures, videos and other forms of child sex abuse material. Children who's images are being exchanged are subject to severe psychological, physical and sexual abuse by their abusers. A more sinister level child trafficking on the darknet market. Children, particularly girl children, from vulnerable communities such as a refugee, migrant, and children in extreme poverty are especially vulnerable to trafficking.

**Types of cyberattacks**

...
Cyberattacks are the means by which the above mentioned cyber crimes are committed. They are usually done by hackers for unethical use and can be used to extract information from every different source possible using targeted techniques. The most common of these cyberattacks are:

**Phishing**

Phishing is a cybercrime attempting to get sensitive information through means such as email and other mass media. Phishers act like a legitimate company or organization and trick the victims into giving out their personal details to them. These are done in multiple thousands at a time, carrying links to illegitimate websites which contain harmful viruses that scan your computer drive. For example, phishers send out emails claiming that they notice unexpected activity in their account and then ask the users to login, however, this usually detects to a website which looks very much like the actual website but its not, and that's how passwords are easily stolen. Moreover, spear phishing is a very targeted form of phishing in which phishers do research about their targets and therefore generate relevant and personal emails which tend to be extremely effective. Due to this reason, spear phishing is very hard to detect, causing damage to personal details and property to targets.

**DDoS and botnets**

One of the most common methods of hacking in today’s world is Distributed Denial of Service (DDoS) attacks. DDoS attacks are used to interrupt servers and networks to compromise certain functions leading to malfunctioning of the servers making them vulnerable to further hacks. Unlike other attacks, DDoS attacks do not give any access to the hacker, however, they do make the system vulnerable due to service denial.

Botnets, meanwhile, are networks of computers controlled by hackers in a remote location, without the knowledge of the owner. They are used to attack computers by sending spam and malware and are usually targeted towards huge businesses and governments. Botnets are very common and effective methods to trigger DDoS attacks and they are often used simultaneously. They affect the system of computers directly thus leading to harmful viruses and leak of data along with full system crashes on big networks causing huge loss of essential data. A notable incident involves GitHub, a developer platform which was hit with a massive DDoS attack on February 28th, 2018, which made their traffic shoot straight up to 1.35 terabytes per second resulting in crashing their server and making it vulnerable to further attacks.

**Malware**


Malware or malicious software is harmful software installed on the user’s computer without their consent. Malware often replicates itself and spreads throughout the system and even the network of computers causing damage to important information and files. Malware can be of various types such as macro viruses, stealth viruses, trojans, worms, ransomware, etc.

Macro viruses are the viruses that infect major applications. They attach to the initialization protocol of the application, therefore executing and transferring harmful information before passing on the control to the application opened by the user. All of this happens in the background, and therefore the users do not get an idea about it until it has reached a stage where the computer starts malfunctioning.

Stealth viruses are those viruses which firstly affect the malware detection software, thereby reducing their chances of being detected by the computer and completely conceal themselves. They can be very harmful and are usually almost impossible to detect by the user unless the hard drive is thoroughly scanned by unaffected software.

Trojans are programs that hide inside other programs to serve a malicious function. Trojans, as opposed to viruses, do not self replicate and spread. However, trojans are used to create backdoors into confidential systems which allow the hacker to get unrestricted access to concealed data.

Worms are programs that self-propagate through networks without attaching to a host program. They are commonly spread through email attachments, an opening which triggers worms. These worm exploits once opened send a copy of themselves to every contact on the infected user’s computer thus spreading exponentially at a time.

Ransomware is a type of malware that restricts the user from viewing their data and threatens to publicize sensitive personal information about the user until a ransom is paid. Usually, they are very complex with their encryption and tend to leave the user with no choice other than paying the ransom amount.

The best example is WannaCry, one of the biggest malware attacks in history, which spread out in 2017 in over 150 countries affecting over 230,000 users. This ransomware software encrypted important files which led it to generate over 130,000 US dollars just before a kill switch was found to terminate it for once.

**SQL injections**
This type of attack has become very common on database-driven websites. An SQL injection takes place when a criminal initiates an SQL query to some database in the form of input data from the client to a specific server. When the SQL query is executed, some commands are added to a data-plane input (i.e. instead of the login or password) in order to run the query. Hence, a successful SQL injection attack is capable of reading sensitive data from a particular database, then modify (insert, update or delete) data from the database, carry out administrative operations, such as the shutdown of the database. recover the content on a file in the database, not always, but can issue commands to the database.

**Man-in-the-middle**

A man-in-the-middle (MitM) attack occurs when the hacker intervenes between the communications of the victim and the server. This form of attack has 3 common ways of appearing: session hijacking, IP spoofing, and replay.

Essentially, session hijacking entails the criminal hijacking a session between a trusted victim and their server. Thus, the attacker substitutes their IP address with the trusted client, while the computer system continues to believe that it is communicating with the client. This can be used to gain control of the client, disconnect the client from the server, replace the client’s IP address for the attacker IP and then spoof the client’s sequence numbers, etc.

However, a replay attack takes place when the hacker stops and saves old messages sent by the victim and then, later sends them in order to impersonate the victim. This type of a MitM attack can easily be opposed by implementing session timestamps and/or nonce (a string or random number that changes over time). Though there are ways to counter a replay attack most people are not aware of being secure from other MitM attacks as they have not discovered a technology for it.

**Password**

Password attacks are usually correlated to data breaches in the cyber world, and according to Uber, over 57 million drivers and riders have had their information stolen in 2017. Obtaining an individual’s password is a common method to attack, due to the fact that passwords are typically used to authenticate users to an information system. There are several ways through which one’s password can be acquired: physically searching for it, “sniffing” the connection to the network to gain unencrypted passwords, implementing social engineering, accessing a password database or merely guessing. However, the last approach (outright guessing) to acquire one’s password can be done through two means: brute force and/or a dictionary attack.
The random method of obtaining one’s password is through brute force, which involves trying
different passwords and hope that one of these work. These ransomware attacks are growing by
350 per cent annually, according to Cisco’s annual reports on cybercrime. However, there can be
some logic applied to the brute-force, such as using the victim’s personal information (name, job
title, hobbies, etc.) in the password attempts. Likewise, another and a more systematic way of
implementing a password attack is by employing a dictionary attack where a dictionary of
common passwords is used to gain access to a user’s computer and network. Hence, an
approach to accomplish this is to copy an encrypted file which includes the passwords, and then
use the same encryption in a dictionary of commonly used passwords to compare the results.
However, there is a link between ransomware detections and countries with higher numbers of
internet-connected populations, and according to Symantec, the United States ranks the highest
with 18.2 percent of all global ransomware attacks.

**Impacts of cybercriminal activity on businesses**

McAfee (an internet security organisation), in 2018, published a report regarding the economic
impacts of cybercrime, and this equated to an estimated annual cost of $600 million to the global
economy, compared to $45 million in 2014. Thus, when the economic impacts are increasing,
businesses are at a great loss too, and therefore cybercriminal activity has a great stake over business
activity.

In the case of a security breach creates damage to investor perception of a business, as they
lead to a drop in the financial value of a company. Correspondingly, when potential share price reduces,
businesses face the challenge of increased costs as they have usually borrowed money and thus there
are issues regarding raising capital. Hackers usually attempt to control the company servers to steal
information and for these reasons, businesses maintain high security and update software regularly to
avoid such situations. According to EWeek, when surveying a group of large companies, an average of
$8.9 million p.a. was spent on cybersecurity systems, this was due to a 100% of the companies
experiencing at least one malware incident in the last year and others reporting a hijack of the company
computers.

Other effects on a business include loss of sensitive customer data and damaged brand identity
(loss of reputation). Essentially, the prior can result in penalties to the company as they fail to protect
their consumers’ data, which could be further escalated by suing the business due to data breach.
However, the latter can occur after a cyberattack and leads to lower the trust customers have in a
company and its ability to protect their financial data. Therefore, followed by a cyberattack, businesses
do not simply lose their current customers but also their potential to gain any other customer.
Impacts of cybercriminal activity on national defence

With the increase in the rate of cybercrimes happening every day, their threat to the national security of countries also increases. National defence, being the most confidential data of governments, is also the most attacked data by hackers. Organized crime, hackers and cyber espionage can pose a great threat to national security. Getting access to national defence strategies of countries can affect politics and economy of the world drastically, as defence secrets, which are so confidential that only certain people at the highest posts have access to them, are leaked and made available to everyone on-demand via the internet.

Increasing uncertainty due to cybercrimes can lead to chaos, as people struggle to understand and deduce what is true and what is not. With cyberattacks getting access to governmental information, the public opinion can be drastically altered and manipulated resulting in distrust between citizens and governments, therefore breaking the social contract of the country. Furthermore, targeted advertising and deep fakes can be made using sensitive government data on the citizens of the country. Nowadays, it is due to these reasons we see countries heavily investing in cybersecurity to prevent confidential information from getting available to hackers.

One major way cybercrimes and lack of cybersecurity can affect countries are by cyberterrorism. The linking of hackers and cybercriminals to those of terrorist is, unfortunately, not a new phenomenon. Terrorist groups often take advantage of the vulnerability of the cybersecurity of countries and further exploit it to their needs. Cyberterrorism is becoming more and more prominent on the internet today. Cyberterrorism can put a great threat to a country’s economy and political situations. Cyberterrorist often use emails, social media and other forms of media available on the internet to spread terrorist propaganda and influence the youth by altering their beliefs. This further poses the threat to the future generations of the country, involving the youth of today.

Impacts of cybercrimes on people

As cyber-attacks become more and more common in society, the more people become a victim of it. According to a study by the University of Maryland, a person is hacked every 39 seconds. Moreover, the 2019 Official Annual Cybercrime Report (ACR) estimates that there is a ransomware attack every 14 seconds. Moreover, with the current technologies, it takes over half a year to even detect data breaches, due to which people don’t even realise that their data is being stolen. Such extreme statistics only lead to worse situations for the common people as
Cybercriminals often target individuals as they are more easy to attack and eventually gain access to and misuse information. The types of cybercrimes on people ranges from malware to cybertheft to ransomware. Therefore, individuals can lose a lot of data and financial assets due to cybercrimes, mostly due to cyber theft. This often leads to loss of livelihood and life-savings as it is almost impossible to recognize cybertheft in its initial stages. Moreover, people usually don’t have protection against viruses and malware online which leads to unwanted software like spyware and trojan horses on their systems getting access to their storage drives and leaving no information private to the user.

Furthermore, with specifically targeted cyberattacks such as spear phishing today, the rates of people falling for cyberattacks have also been increasing, despite measures being taken to spread awareness about preventing cybercrimes. Therefore, cybercrimes tend to affect the people drastically from the very sense of “threat” people have in their minds.

**Major Countries and Organizations Involved**

**United States of America (USA)**

Cybercrime is the fastest-growing crime-form in the United States of America and is gradually affecting more and more people as every year passes. The annual number of data breaches and exposed records are 1244 and 446.5 billion, respectively. Also known as, cyberwarfare, citizens in the United States are constantly in the midst of credit card frauds, identity thefts, email hacking, ransomware, password attacks, etc. The frequency of cyberattacks within the U.S. is because as large of a country it is, they have free access to most elements of the cyberspace and restrictions are minimized, thus attempting to commit a cybercrime is simplified. Due to the extremity of cybercrimes in the USA, billions of dollars are spent on preventing and combating cybercrime, however, the number of cyberattacks merely increase year by year. Hence, they have established multiple initiatives and partnerships such as cyber action team, national cyber forensics and training alliance - and these have been affiliated with the Federal Bureau of Investigation (FBI).

However, as cyber warfare is very common in the United States - a country that possesses an abundant military budget - the government has implemented various strategies to prevent cybercriminal activity. There are five pillars of preventing such malicious activity established in 2015 by the US Department of Defense Cyber Strategy. The main purpose of the pillars is to advance in research and development to form technical capabilities that can provide the U.S. with enhanced security and defence. The Defense Department published a document in September 2018, which announced that this strategy would “defend forward” U.S. networks by disrupting “malicious cyber activity at its source” and endeavour
to “ensure there are consequences for irresponsible cyber behaviour by “preserving peace through strength”. Though the Cyber Strategy is the first extensive one the U.S. has prepared, it has also received much criticism as the cyber networks and activity of the U.S. is still ambiguous to its citizens and the rest of the world. Nonetheless, the United States consists of a U.S. Cyber Command which is responsible for planning, coordinating, integrating, synchronizing and conducting activities which defend Department of Defence Information networks and prepare to conduct “full-spectrum military cyberspace operations” that can US (or allies) a sense of freedom of action within the cyberspace and can deny the same to adversaries. Hence, the United States has allegedly been responsible for cyberattacks on China, Iran, Russia, and other countries across the globe. For example, the most recent attack was in June 2019, as Russia accused the United States of attacking its electrical grid. Later, the New York Times released a report that this was indeed true, as American hackers (from the United States Cyber Command) had planted malware which was capable of disrupting the process of Russia’s electrical grids.

The People’s Republic of China

As a rapidly growing economy, China is pressured to maintain solid and secure cyberspace due to the other nation’s hacking capabilities for the intention of gaining access to their national data. An example would be the attack in 2013, a member of the Central Intelligence Agency (CIA) and one at the Defense Intelligence Agency (DIA) revealed that the U.S. government had attempted to hack into Chinese mobile phone companies to gather evidence on text messages and spy on Tsinghua University - a world-renowned research institution, along with six major backbone networks in China, the China Education and Research Network (CERNET), which is a network that contains internet data of millions of Chinese citizens. Hence, it leads to the creation of further intensified cybersecurity within the nation, as a hack like this could have left devastating consequences on China and its economy.

Therefore, due to the many cyber threats, China has seen over the years, they have established legislation that tackles the needs to be fulfilled for secure cyberspace. China does not have a national law that specifically addresses the collection, storage, transmission and use of personal information. Rather, a gradual and steady approach is adopted, which is found within the Constitution, the Cybersecurity Law, telecommunications regulations, criminal law, tort law, consumer rights law, etc. The cybersecurity law came into existence in June 2017, with its main objective being the regulation of the collection, storage, transmission and use of personal information by network operators and critical information infrastructure operators. However, this is unlike the other regulatory practices in Asia-Pacific countries as China’s Cybersecurity Law imposes strict data localisation requirements and many cross-border movement restrictions on personal and important information/data.
The Islamic Republic of Iran

Iran is known to be one of the greatest cyber threats to the Middle Eastern countries and is repeatedly accused of launching state-sponsored cyber espionage attacks. As Iran continues to seek geographical prominence, the United Arab Emirates (UAE) and Saudi Arabian government and defence sectors are main targets due to their extensive economies, according to CrowdStrike, a cybersecurity technology company based in California. The regional head of CrowdStrike at UAE said that Iran continues to be a destructive threat to countries within the Middle East as well as, companies based in western nations that could have business relations with the Middle East. This report revealed that countries such as Russia, China and North Korea are also involved with Iran and maintain a professional and experienced cyber-crime capability, and mainly include eCrime and state-sponsored cyberattacks in the world. Thus, Iran is not greatly affected by cybercrime and does not have any major involvement in the prevention of this issue, however, it is currently still viewed as a cyber threat to many nations.

UN Office on Drugs and Crime (UNODC)

UNODC is an organization that has constantly worked towards achieving sustainable and long-term solutions to cybercrimes in the status-quo today. The UNODC uses the justice system to raise awareness, resources and provide research and analysis on cybercrimes. In 2017, UNODC started the cybercrime program, which aimed to increase the efficiency and effectiveness in investigations of cybercrime. This has resulted in a positive impact as more countries tend to support and join the programme. Another main aspect of this programme focus on strengthening communication between governments and finding out effective long term governmental measures to prevent cybercrimes. However, it has not achieved its goal as of yet, as stronger communication between governments requires constant support of an impartial mediator such as the UN, which hasn't received lately. Apart from this, the UNODC has also launched various other initiatives and even established a cybercrime repository in 2015. This repository aims to assist countries in informing strategies to combat cybercrime. It has had a great start and is very useful as it contains evidence on cybercrimes that have happened in the past.

International Criminal Police Organization (INTERPOL)

The INTERPOL has played a major role surrounding cybercrimes. The INTERPOL is an inter-governmental organization having 194 member countries as of date. With the increasing cybercrime rates of today, it is crucial for a global organization like INTERPOL to provide a platform for cooperation between different nations. INTERPOL fights cybercrimes by previous research and also using advice
from cyber intelligence experts from around the world. In 2014 INTERPOL opened the IGCI (Interpol Global Complex for Innovation), a facility dedicated to research and find more effective ways to tackle issues. This initiative has especially helped the countries in Latin America and the Caribbean in tackling cybercrime by assisting them. Furthermore, INTERPOL also carries out a variety of activities to support its member countries to fight cybercrime, including sessions on cases of cybercrime investigation, workshops and sessions on reviewing a country’s cyber fight capacities, and sharing new technologies to prevent cybercrimes. This has served to be very useful and effective, especially when we consider cybercrimes as transnational crimes. It is through such programmes and activities that awareness is spreading on how to prevent different forms of cybercrimes and generating support for bigger programmes such as the UNODC’s cybercrime programme.

The Council of Europe

The Council of Europe is an international organization that fights against Human Rights violations and maintain peace among its 47 member states, 28 of which are from the European Union. It has taken up a constant role in the prevention of cybercrime over the past two decades. It established the Budapest Convention in 2001 (also known as the Convention on Cybercrime), which was the first international treaty addressing cyber crimes as a major issue, and developed guidelines to help nations develop strong national legislation against cybercrime while also establishing a framework for international cooperation. It focussed particularly on copyright infringement, cyber fraud, and violation of national security and laid down guidelines to act against the aforementioned. Furthermore, being the first international treaty against cybercrimes, it laid down the foundation of later conventions which enabled cybercrime justice systems today.

Timeline of Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td>Launch and start of the World Wide Web</td>
</tr>
<tr>
<td>1997</td>
<td>The G8 countries meet in Washington D.C. to adopt 10 principles in combating cybercrimes</td>
</tr>
<tr>
<td>1998</td>
<td>The first major attack on national security in the USA, where 2 teenagers hacked into the air force’s database and gained access to national defense secrets</td>
</tr>
</tbody>
</table>

2001 The Council of Europe drafts the Budapest convention establishing the framework for international cooperation

2004 The Europe Convention on Cybercrime came into effect

2015 UNODC launches its cybercrime repository storing electronic evidence of past cybercrimes

2017 UNODC starts its cybercrime combating programme spreading awareness on cybercrime prevention and also sharing available technology on the same

Relevant UN Treaties and Events

- Combatting the criminal misuse of information technologies, 22 January 2001 (A/55/593)
- Creation of a global culture of cybersecurity, 31 January 2003 (A/57/529/Add.3)
- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 17 March 2010 (A/64/422/Add.3)
- Advancing responsible State behaviour in cyberspace in the context of international security, 22 December 2018 (A/RES/73/266)
- The right to privacy in the digital age, 14 November 2018 (A/C.3/73/L.49/Rev.1)

Previous Attempts to solve the Issue

As a rapidly growing international concern, cybercrime is, many organizations including the United Nations have been searching for viable solutions to eradicate such forms of criminal activity. Essentially, there have been a few methods to resolve this matter at hand. A major organ of the UN is the United Nations Office on Drugs and Crime (UNOD) is heavily involved in the improvement of the situation of cybercrime in many nations.

UNODC training for combating child exploitation via the internet
Therefore, they have been working in more than 50 countries and providing the required training to enhance investigative skills (amongst the police and other authorities), trace cryptocurrencies as a part of financial-related investigations, and use software to find online abuse sources and hunt predators. However, as they cooperate with the Internet Watch Foundation (an organization that works on making the internet a safer place, globally), they have released child exploitation reporting portals, in Belize, in order to raise awareness of the issues and make citizens take the initiative to report this content as viewing them, thus protecting boys and girls from such online exploitation. This has lead to the arrest and conviction of a high-risk paedophile with over 80 victims This training was delivered in partnership with the International Centre for Missing and Exploited Children and Facebook. Furthermore, the UNODC has made solid partnerships with Thorn and Pantallas Amigas, and manage to strengthen online protection whilst educating parents, guardians and children about cyber risks via presentations in schools and local communities - emphasizing the fact that prevention is key.

**UNODC training against the use of cyberspace for criminal purposes**

Thus, the UNODC training came into play, mainly focusing on Central America, the Middle East and North and Eastern Africa, along with SouthEast Asia. This training looks into online drug trafficking and identifying digital evidence, battling the use of the darknet to terrorist/criminal purposes, and advancing data collection to improve address threats. It is specifically targeted to the aforementioned nations due to the vulnerability of their national securities noticed in the past, as they have consistently been victims of cyberattacks that occurred in the past. However, international cooperation is a critical foundation for the work being done by the organization. The UNODC’s work has been funded by donor governments, thus exhibiting the fact that even though political differences exist, countries do manage to unite and counter the threats of cybercrime. At the moment, the organ is seeking to find means through which they can further strengthen international cooperation via the Intergovernmental Expert Group, which meets at UNODC headquarters in Vienna.

**Possible Solutions**

CCPCJ Resolutions work differently in that, as opposed to voting on a resolution, the member states must come to a consensus. One resolution is written for each issue, and the house goes through the resolution line-by-line. All delegates must agree on a clause before they move on. If there are delegates who disagree with the clause, it is debated upon, and changes on the clause are considered. At the end, a change is made to a clause so that all delegates agree, and then the next clause is debated upon. Even if only one delegate disagrees, debate will have to happen to form a new clause that all delegates, that delegate included, can agree with, or to simply remove that clause completely. We must keep this in mind as we move on to consider possible solutions, as different countries may have different views on which solution will work better.
Spreading awareness

The first and foremost step taken towards the prevention of cybercrime must be educating the people on how to safely use the internet. This can be done internationally with the help of experts from various organizations such as INTERPOL and UNODC. This will give a global understanding of cybercrimes which will make common people and their data on the internet security to at least a major extent. Furthermore, they could express and emphasize the use of antivirus software and firewalls to provide another cushion of protection before falling for cyberattacks. Apart from this, basic knowledge and guidelines on using the internet can be added as part of education in school to protect the growing youth as well and also make them understand what morally correct hacking is. An example of this is Hackathons held at schools and institutions.

Problems with this is that 93% of computer users have long graduated school and college, making it harder to engage them in national educational programs on awareness of counter cyberterrorism measures.

Regulation of data

On a much wider scale, cybercrime is a transnational crime and must be tackled on an international scale. The problem, however, is to find the perfect balance between security and privacy. For this, the UN must take measures to ensure proper regulation of digital networks which can help a large number of citizens at once while preserving their privacy. Programs such as the “Cyber surge” programme of INTERPOL, which focuses on filtering out data rather than mass-surveilling and compromising someone’s privacy can be further expanded to the rest of the world and the UN can help get this support. These will further ensure the protection of citizens at a large scale, as they will be supported by experts from all around the world. On top of this, encouraging countries to expand their research into detecting cyber crimes can serve as a massive boon to prevent them as well as it can help in developing stronger data filtering algorithms as well as improve existing ones. The only issue is to not compromise privacy while being able to filter out data as privacy is a person’s inalienable right.

Merging cybersecurity with national security

The hacking of government databases destroys any sort of privacy in society and is unfortunately not very uncommon in the status-quo. Recent examples include malware WannaCry attacking the United Kingdom’s NHS and also the US Voter Database leak back in 2015 where all data of 191 million registered voters in 50 states were openly available on the internet for a while. Therefore, as cybercrimes have drastically affected nations in the past, governments must also treat cybersecurity as an important aspect of national security and must allocate resources to strengthen their cybersecurity in order to
prevent it from getting compromised by data breaches from hackers. They may form separate units just to take care of the cybersecurity and invest in further research and education in the same. Furthermore, all databases and networks involving sensitive information of either businesses or governments must be regularly updated with security patches and logs to further prevent them from being breached. This would prevent hackers from getting even a small insight into the encryption of the data and would make hacking the servers, combined with the other efforts, almost impossible.

Guiding Questions

1. How can nations work together in combating cybercrimes?
2. How can national security become less susceptible to cyber crimes?
3. How can the citizens be educated on the cybercrimes?
4. Can a perfect balance between monitoring and privacy be attained?
5. How can global coordination on cybercrimes be achieved?

Bibliography


Appendices

This website presents information and statistics regarding the state of cybercrime currently and further details regarding the ways in which new attacking-styles can be implemented, thus in this case, how we can prevent these attacks from occurring.


One of the major cybercrime prevention acts, this is the basis of the regulations we have against cyber criminal activity and this can be read to further understand the previous attempts to solve this issue.

III. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ (Most Common Types of Cyber Attacks)

Even though a diverse range of cyberattack types have been included within the report, it can be very useful to understand how other cyberattacks take place when trying to build resolutions against their existence.


There are multiple organizations and individuals that are at major losses/risks due to the occurrence of cybercrimes and it is imperative to delve further into the magnitude of their effects.


This source displays information in regards to the ways in which specific cyberattacks can be prevented and how security-related markets have been established due to the growth of cybercriminal activity.

VI. https://www.varonis.com/blog/cybersecurity-statistics/ (Key Cybercrime Statistics of 2019)

A solid source, which includes key figures that display the significance and urgency to resolve the issue. Furthermore, it includes more information regarding the current state of cybercriminal activity everywhere.