ITKMUN'25

International Criminal Police Organization (INTERPOL)

Study Guide

Toprak Buluttekin
Gülse Öz

Table of Contents

Letter from Secretary General

Letter from Under Secretary General

Dear Delegates,

I would like to welcome you all to The International Criminal Police Organization.I am Toprak Buluttekin and I will serve as your under secretary general for these 3 days.

Throughout these 3 days,Interpol will focus on cybercrime attacks.Our committee will follow semi-crisis procedure which means that we will be facing some conflicts and operations.

I prepared a study guide for you to read and come to the committee well prepared.I am expecting all of my delegates to understand the study guide and think about possible solutions to these cybercrime attacks.

I want you to consider this conference as an opportunity to enhance your knowledge on global politics and diplomacy but also as a chance to make unforgettable memories and socialize.

Sincerely,

Toprak Buluttekin
Under Secretary General

Letter from the Academic Assistant

Introduction to the Committee

Interpol, intergovernmental organization that facilitates cooperation between the criminal police forces of more than 180 countries. Interpol aims to promote the widest-possible mutual assistance between criminal police forces and to establish and develop institutions likely to contribute to the prevention and suppression of international crime. Headquartered in Lyon, France, it is the only police organization that spans the entire globe.

Interpol organization and functions

Interpol concentrates on three broad categories of international criminal activity: terrorism and crimes against people and property, including crimes against children, trafficking in human beings, illegal immigration, automobile theft, and art theft; economic, financial, and computer crimes, including banking fraud, money laundering, corruption, and counterfeiting; and illegal drugs and criminal organizations, including organized crime. Interpol's day-to-day operation is managed by a General Secretariat under the direction of a secretary general, who is appointed for a five-year term by the General Assembly. The General Assembly, consisting of one delegate from each member country, is Interpol's supreme decision-making body. An Executive Committee of 13 members, each representing a different region of the world, is appointed by the General Assembly at its annual meeting. The Executive Committee oversees the implementation of decisions made by the General Assembly and supervises the work of the secretary general.
Each member country has a domestic clearinghouse—called the National Central Bureau, or NCB—through which its individual police forces may communicate with the General Secretariat or with the police forces of other member countries. Interpol relies on an extensive telecommunications system and a unique database of international police intelligence. Each year, Interpol's telecommunications staff handles millions of messages in the organization's four official languages: Arabic, English, French, and Spanish. An automatic search facility, introduced in 1992, allows specially equipped NCBs to search a large database of information; search results are automatically sent in the language of the query. A system known as I-24/7, introduced in 2003, provides

NCBs with quick access to a wide variety of data, including fingerprints, DNA records, watch lists of criminal suspects and persons wanted for questioning, and lists of stolen identification documents.

In contrast to the image occasionally conveyed on television and in the movies, Interpol agents do not make arrests, a practice that would unacceptably infringe on the national sovereignty of member countries. Instead, the organization, at the request of NCBs, sends out “red notices,” based on warrants issued by member countries, calling for the arrest and extradition of specific individuals. Interpol also issues other “coloured” notices: yellow to help locate missing persons, blue to collect information on illegal activities or on an individual’s identity, black to request information needed to identify a body, green to warn agencies about criminals from one country who may commit additional offenses in other countries, and orange to warn law-enforcement agencies of dangers from bombs and other weapons.

History of Interpol

Interpol traces its history to 1914, when a congress of international criminal police, attended by delegates from 14 countries, was held in Monaco. In 1923, following a significant increase in international crime that particularly affected Austria, representatives of the criminal police forces of 20 countries met in Vienna and formed the International Criminal Police Commission (ICPC) that year. The ICPC’s headquarters were established in Vienna, and the head of the Vienna police, Johann Schober, became the organization’s first president. The ICPC flourished until 1938, when Nazi Germany annexed Austria; the ICPC’s records were subsequently relocated to Berlin. The outbreak of World War II effectively ended the ICPC’s activities.

After the war the ICPC accepted an offer from the French government of a headquarters in Paris together with a staff for the General Secretariat consisting of French police officials. The ICPC was thus revived, though the loss or destruction of all its prewar records required that it be completely reorganized. In 1949 the ICPC was granted consultative status by the United Nations. From 1946 to 1955 its membership grew from 19 countries to 55. In 1956 the ICPC ratified a new constitution, under which it was renamed the International

Criminal Police Organization (Interpol). The organization moved to its present headquarters in Lyon in 1989.

Interpol was at first mainly a European organization, drawing only limited support from the United States and other non-European countries (the United States did not join the ICPC until 1938). Under the leadership of French Secretary General Jean Népote (1963–78), Interpol became increasingly effective. By the mid-1980s the number of member countries had risen to more than 125, representing all of the world's inhabited continents; by the early 21st century membership had surpassed 180.

In the 1970s the organization's ability to combat terrorism was impeded by Article 3 of its constitution—which forbids "intervention or activities of a political, military, religious or racial character"—and by a 1951 resolution of the General Assembly that defined a "political" crime as that whose circumstances and underlying motives are political, even if the act itself is illegal under criminal law. One source of these obstacles was removed in 1984, when the General Assembly revised the interpretation of Article 3 to permit Interpol to undertake antiterrorist activities in certain well-defined circumstances. Interpol was reorganized in 2001 following the September 11 attacks on the United States. The new post of executive director for police services was created to oversee several directorates, including those for regional and national police services, specialized crimes, and operational police support.

Introduction to the Agenda Item

Addressing the threat of cybercrime: Strengthening global cybersecurity frameworks and managing the intersection of military operations in cyberspace

Definition for cybercrimes

Cybercrime consists of criminal acts committed online by using electronic communications networks and information systems.

Cybercrime is a borderless issue that can be classified in three broad definitions:

1)crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts)

2)online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code

3)illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia

What is Cybersecurity

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. It seems that everything relies on computers and the internet now—communication (e.g., email, smartphones, tablets), entertainment (e.g., interactive video games, social media, apps), transportation (e.g., navigation systems), shopping (e.g., online shopping, credit cards), medicine (e.g., medical equipment, medical records), and the list goes

on. How much of your daily life relies on technology? How much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system.

Keywords for Cybersecurity

1)Hacker, attacker, or intruder — These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes benign and motivated by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious activity (stealing or altering information).

2)Malicious code — Malicious code (also called malware) is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses. (See Protecting Against Malicious Code for more information.) Malicious code may have the following characteristics:

It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular webpage.

Some forms of malware propagate without user intervention and typically start by exploiting a software vulnerability. Once the victim computer has been infected, the malware will attempt to find and infect other computers. This malware can also propagate via email, websites, or network-based software.

Some malware claims to be one thing, while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

3)Vulnerabilities — Vulnerabilities are flaws in software, firmware, or hardware that can be exploited by an attacker to perform unauthorized actions in a system. They can be caused by software programming errors. Attackers take

advantage of these errors to infect computers with malware or perform other malicious activity.

Certains Cybercrime Incidents in the past

1)Stuxnet

Stuxnet is a powerful computer worm designed by U.S. and Israeli intelligence to disable a key part of the Iranian nuclear program. Targeted at an air-gapped facility, it unexpectedly spread to outside computer systems, raising a number of questions about its design and purpose.

https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Here is a video for stuxnet incident

2)Ashley Madison

In July 2015, an unknown person or group calling itself **"The Impact Team"** announced that they had stolen user data of Ashley Madison, a commercial website billed as enabling extramarital affairs. The hackers copied personal information about the site's user base and threatened to release names and personal identifying information if Ashley Madison would not immediately shut down. To underscore the validity of the threat, personal information of more than 2,500 users was released. Ashley Madison denied that its records were insecure and continued to operate.

Because of the site's lack of adequate security and practice of not deleting personal information from its database – including real names, home addresses,

search history and credit card transaction records – many users feared being publicly shamed.

On 18 and 20 August, more than 60 gigabytes of additional data was publicly released, including user details. This included personal information about users who had paid the site to delete their personal information showing that the data was not deleted.

The Impact Team announced the attack on 19 July 2015 and threatened to expose the identities of Ashley Madison's users if its parent company, Avid Life Media, did not shut down Ashley Madison and its sister site, "Established Men''.

On 20 July 2015, the Ashley Madison website put up three statements under its "Media" section addressing the breach. The website's normally busy Twitter account fell silent apart from posting the press statements.One statement read:

At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber-terrorism will be held responsible. Using the Digital Millennium Copyright Act (DMCA), our team has now successfully removed the posts related to this incident as well as all Personally Identifiable Information (PII) about our users published online.

The site also offered to waive its account deletion charge.

More than 2,500 customer records were released by "The Impact Team" on 21 July, but the company initially denied the claim that its main database was insecure and had been hacked.However, more than 60 gigabytes of additional data was released on 18 August and was confirmed to be valid. The information was released on BitTorrent in the form of a 10 gigabyte compressed archive; the link to it was posted on a dark web site only accessible via the anonymity network Tor. The data was cryptographically signed with a PGP key. In its message, the group blamed Avid Life Media, accusing the company of deceptive practices: "We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data ... Too bad for ALM, you promised secrecy but didn't deliver.

3)Bangladesh Bank Cyber Heist

On February 4, unknown hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.

The hackers managed to get $81 million sent to Rizal Commercial Banking Corporation in the Philippines via four different transfer requests and an additional $20 million sent to Pan Asia Banking in a single request. But the Bangladesh Bank managed to halt $850 million in other transactions. The $81 million was deposited into four accounts at a Rizal branch in Manila on Feb. 4. These accounts had all been opened a year earlier in May 2015, but had been inactive with just $500 sitting in them until the stolen funds arrived in February this year, according to Reuters.

A printer "error" helped Bangladesh Bank discover the heist. The bank's SWIFT system is configured to automatically print out a record each time a money transfer request goes through. The printer works 24 hours so that when workers arrive each morning, they check the tray for transfers that got confirmed overnight. But on the morning of Friday February 5, the director of the bank found the printer tray empty. When bank workers tried to print the reports manually, they couldn't. The software on the terminal that connects to the SWIFT network indicated that a critical system file was missing or had been altered.

When they finally got the software working the next day and were able to restart the printer, dozens of suspicious transactions spit out. The Fed bank in New

York had apparently sent queries to Bangladesh Bank questioning dozens of the transfer orders, but no one in Bangladesh had responded. Panic ensued as workers in Bangladesh scrambled to determine if any of the money transfers had gone through---their own records system showed that nothing had been debited to their account yet---and halt any orders that were still pending. They contacted SWIFT and New York Fed, but the attackers had timed their heist well; because it was the weekend in New York, no one there responded. It wasn't until Monday that bank workers in Bangladesh finally learned that four of the transactions had gone through amounting to $101 million.

Bangladesh Bank managed to get Pan Asia Banking to cancel the $20 million that it had already received and reroute that money back to Bangladesh Bank's New York Fed account. But the $81 million that went to Rizal Bank in the Philippines was gone. It had already been credited to multiple accounts---reportedly belonging to casinos in the Philippines---and all but $68,000 of it was withdrawn on February 5 and 9 before further withdrawals were halted. The manager of the Rizal Bank branch has been questioned about why she allowed the money to be withdrawn on the 9th, even after receiving a request that day from Bangladesh Bank to halt the money.

The hackers might have stolen much more if not for a typo in one of the money transfer requests that caught the eye of the Federal Reserve Bank in New York.

Further Reading and Resources

https://www.britannica.com/topic/Interpol

https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

https://www.cisa.gov/news-events/news/what-cybersecurity#main

https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

https://www.bbc.com/news/stories-57520169

https://youtu.be/wVnnHyp7WEo?si=6Wky9Xa4Ll5hmcEb

https://impact.economist.com/projects/smart-cyber-security/

https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/