Topic: Preventing and Combating Cybercrime

Committee Introduction

ECOSOC

The UN established ECOSOC in 1945 as one of the six main organs of the United Nations to advance three dimensions – economic, social and environmental. The Economic and Social Council (ECOSOC) is the United Nations' central platform for reflection, debate, and innovative thinking on sustainable development.

CCPCJ

The United Nations Office on Drugs and Crime (UNODC) is a UN office established in 1997. The Commission on Crime Prevention and Criminal Justice (CCPCJ) was established by the ECOSOC as a governing body of the UNODC. The Commission acts as the principal policymaking body of the United Nations in the field of crime prevention and criminal justice.

Definition of key terms

Cybercrime

Cybercrime is defined as a crime which has some kind of computer or cyber aspect to it. Computers are usually the object or tool of the crime. Due to the sheer number of connected people and devices, cybercrime has become an issue that cannot be ignored. Cybercrime involves a wide range of illegal acts, and the following are the definitions of some key terms of cybercrime that we will mainly discuss in the committee.

(a) Identity theft

Identity theft is a crime in which an imposter obtains key pieces of personally identifiable information, such as ID card number, and the account name and password of social networking websites or online shops, in order to impersonate someone else for illegal use.

(b) Ransomware

Ransomware is a kind of malware that locks the data in victim's computers, typically by means of the encryption. The data will not be decrypted until the ransom is paid. Payment is often demanded in a virtual currency, such as bitcoin, so that the cyber criminal's identity won't be identified.

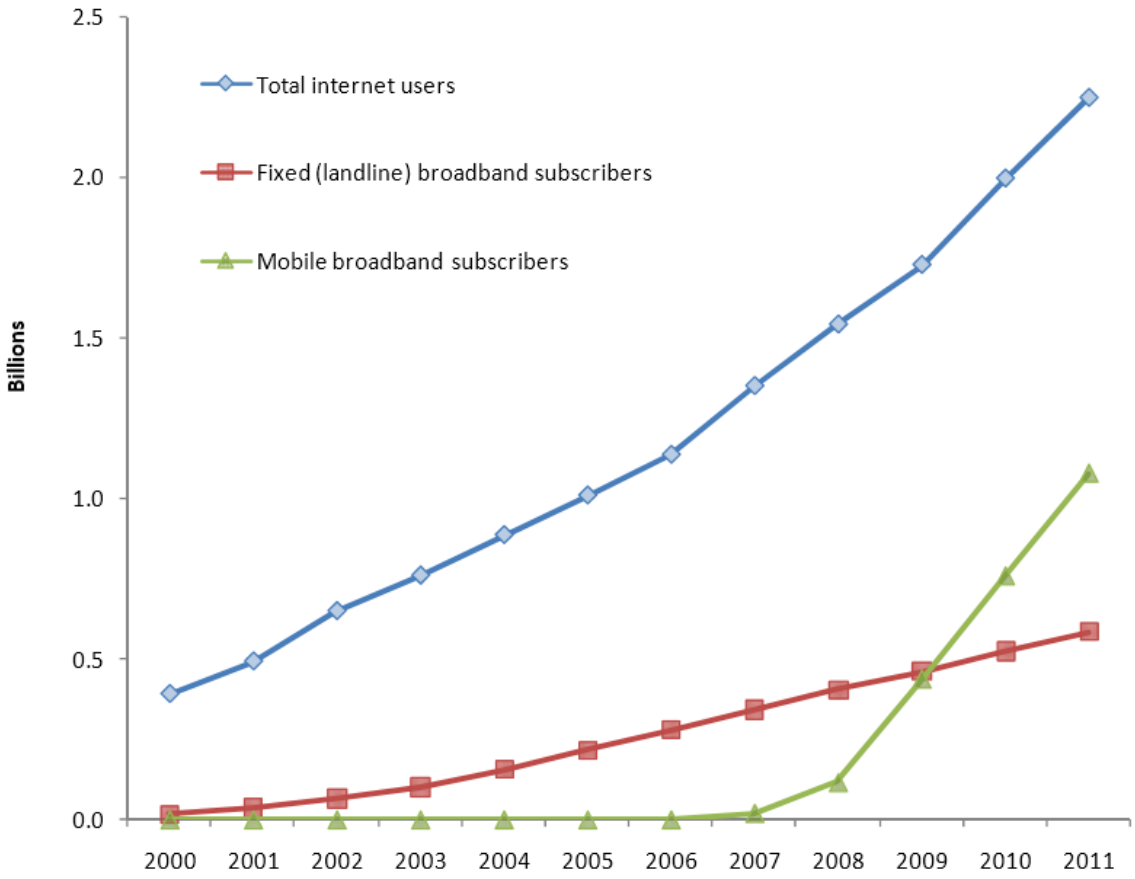
(c) Copyright infringement

A copyright infringement is a violation or theft of an individual or organization's copyright through the unauthorized use of holder's copyrighted materials. The number of such materials illegally stolen and the speed at which they are exploited are far beyond our expectations. The level of infringing traffic varies by internet venue, being is highest in areas such as P2P services or 'cyberlocker' download sites commonly used for distribution of films, television episodes, music, computer games and software.

Overview

Since the information revolution started from the 1980s, cybercrime has become a new form of violation that massively affects our daily lives and even threatens the well-being of the society. As is revealed in a comprehensive survey conducted by United Nations Office on Drugs and Crime (UNODC) in 2013, "In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet. Over 60 percent of all internet users are in developing countries, with 45 percent of all internet users below the age of 25 years."

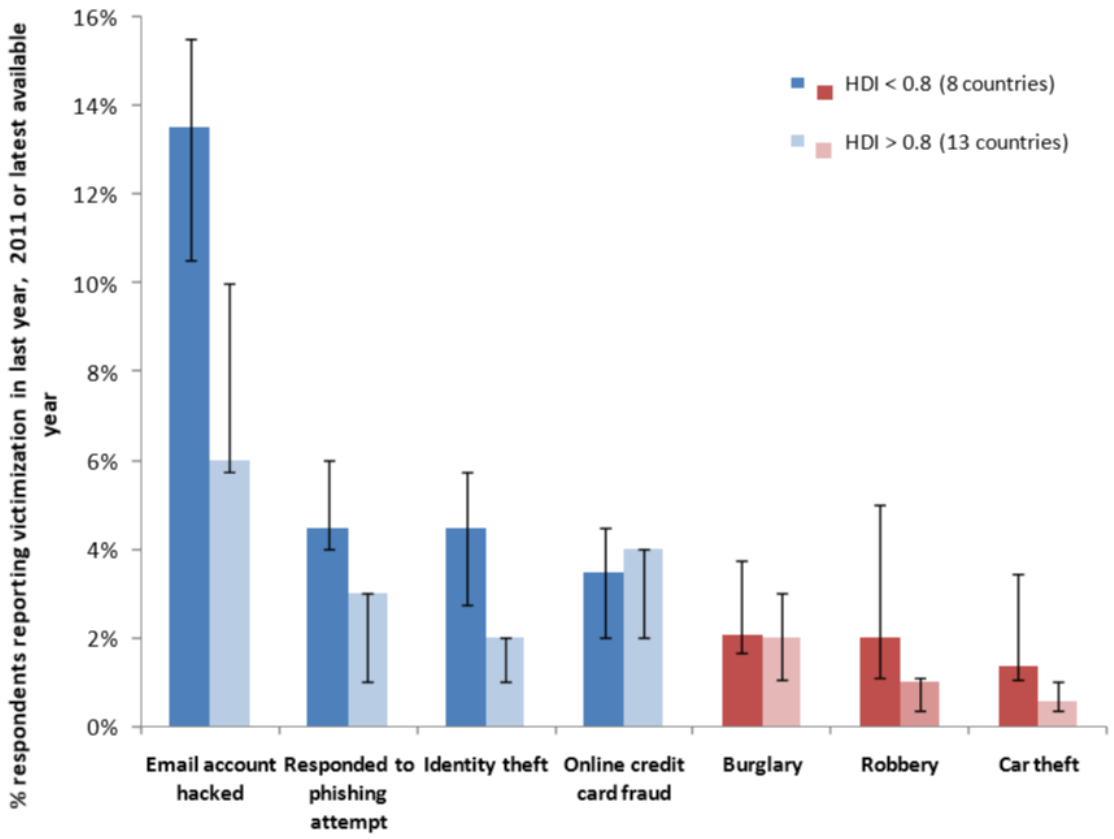
Figure 1.2: Global internet connectivity 2000 - 2011



Source: ITU World Telecommunication ICT Indicators 2012

Also, this high connectivity of networked devices has aroused safety concerns. The percentage of respondents reporting victimization of cybercrime, which includes 14 acts in three categories, outnumbered that of conventional crime, such as burglary, robbery and car theft.

Figure 2.4: Cybercrime and conventional crime victimization



Source: UNODC elaboration of Norton Cybercrime Report and crime victimization surveys.

On the one hand, cybercrime can menace individual rights, for example, fraud, the violation of copyright and identity theft. On the other hand, cybercrime can be a national or global explosive that would impair our safety and human rights via the borderless realm of cyberspace.

To stress our concern over this issue, we encourage delegates to propose feasible solutions to improve global information safety and impede transnational cybercrimes with regional and technical restrictions. We should never compromise and gather resources to fight off cybercrime.

However, while the governments make their effort on overseeing online activities, they should also strike a balance between protecting privacy and maintaining social orders.

Acts against the confidentiality, integrity and availability of computer data or systems

- Illegal access to a computer system
- Illegal access, interception or acquisition of computer data
- Illegal interference with a computer system or computer data
- Production, distribution or possession of computer misuse tools
- Breach of privacy or data protection measures

Computer-related acts for personal or financial gain or harm

- Computer-related fraud or forgery
- Computer-related identity offences
- Computer-related copyright or trademark offences
- Sending or controlling sending of Spam
- Computer-related acts causing personal harm
- Computer-related solicitation or 'grooming' of children

Computer content-related acts

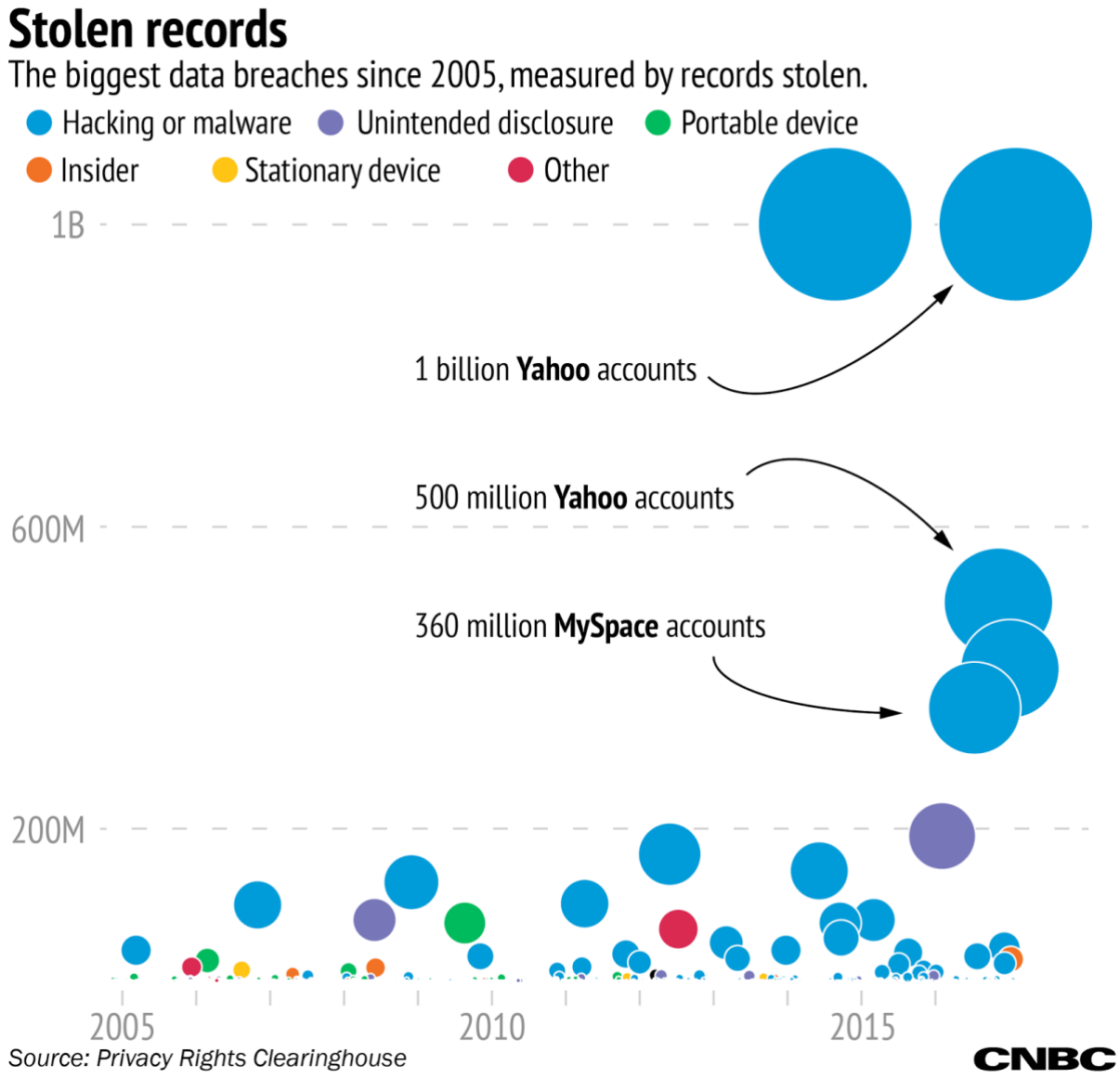
- Computer-related acts involving hate speech
- Computer-related production, distribution or possession of child pornography
- Computer-related acts in support of terrorism offences

Recent Incidents

As what we might have seen on the news, one of the most influential technology company in the world, Yahoo, just suffered a disastrous cyberattack in August 2013, which affected more than one billion accounts and triggered panic. Similarly, many people fell into ambush of a rampant ransomware named “WannaCry”, and compromised a great amount of properties in order to redeem their important files. Moreover, the numerous frauds on social medias and the Internet also assault the trust system that human beings have long been maintaining. Nevertheless, these incidents are only involved in infringements of individual rights, and sometimes cybercrime can be a culprit of violation of collective welfare. For example, the Ukraine power blackout on December 23, 2015

left approximately 230 thousand people in the darkness for a period from 1 to 6 hours, and on June 27 in 2017, the same kind of attack took place again, leading to a gigantic financial lost to the whole country.

Cybercrime can also be involved in political activities, such as Russia's doubtful intervention of US presidential election and its involvement in cyberespionage. In addition to the incidents above, the recent shutting down of a popular "stream-ripping" website, which can convert Youtube video to MP3 file, just reminded us of the importance of protecting copyrights.



Challenges

(a) Fragmentation at international level & Diversity of national cybercrime

Different legal families, religion and social customs can lead to divergences in national cybercrime laws. As a result, provisions sometimes contradict each other, leading to collisions of law, or fail to overlap sufficiently, leaving jurisdictional gaps. Different countries hold different perspectives on the acceptability of forms of internet content, leave a number of which create criminal safe havens for technology criminals.

To solve this problem, consistency of laws is necessary, especially for differences between national criminal laws in the area of cybercrime. Criminalization differences introduce challenges for effective international cooperation in criminal matters involving cybercrime. The details of cybercrime criminal offences, such as the technical means, can be the decisive element to judge whether they are crimes committed, which may influence international cooperation against cybercrime.

(b) Reliance on traditional means

Due to the volatile nature of electronic evidence, international cooperation in cybercrime requires immediate and specialized investigative actions. To obtain extra-territorial evidence, using traditional forms of international cooperation remains the mainstream.

Most of the requests use instruments as the legal basis. Response times for formal mechanisms also takes months, which obviously has got behind the speed cybercrime criminal offenses occur. The current form in international cooperation sees the emergence of a few absolute powers, with their specific procedures, that cooperated only among themselves.

This excludes many other countries who had no choice but to employ "traditional" modes of international cooperation that may take no account of the specificities of electronic evidence

(c) Transnationality

It is reported that more than 50 percent of cybercrime acts encountered by the police involved a transnational element. The use of proxy servers, and the influence of social media, were among the factors behind an increasing number of cases involving a transnational dimension.

Perpetrators are aware of jurisdictional issues and purposefully use internet resources, such as mail servers located abroad, in an attempt to hide evidence of their illegal activities. Under such circumstances, countries should get the consensus on uniting and strengthening criminal jurisdiction, while the sovereignty is protected so that every country has the obligation not to interfere in the internal and external affairs of other states.

Past Actions

The United Nations Congress on Crime Prevention and Criminal Justice is a United Nations congress on crime and criminal justice, held every five years. It is organized by the United Nations Office on Drugs and Crime (UNODC).

In 2010, the Twelfth United Nations Congress on Crime Prevention and Criminal Justice was held in Salvador, Brazil. Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and

Criminal Justice Systems and Their Development in a Changing World was presented. It recommends that the United Nations Office on Drugs and Crime provide relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities in cooperation with Member States. It is hoped to combat cybercrime and to enhance the security of computer networks.

In 2015, the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice was held in Doha, Qatar. Doha Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World was presented.

To create a secure and resilient cyber environment, it is urgent to protect children from online exploitation and abuse, strengthen worldwide consistency of law enforcement, and protect victims by removing child pornography, child sexual abuse imagery in particular, from the Internet. A secure and resilient cyber environment requests the expert group to conduct a comprehensive study of the problem of cybercrime and respond to it by Member States and the international community, and invite the Commission on Crime Prevention and Criminal Justice to consider recommending that the expert group continue to exchange information on national legislation, best practices, technical assistance and international cooperation.

The 2017 Commission on Crime Prevention and Criminal Justice was the twenty-sixth session. A draft resolution was revised during this session. It recalled both the Salvador Declaration in 2010 and the Doha Declaration in 2015. It is requested that Member States keep in line with the declarations and decides that the expert group dedicate future meetings to examining cybercrime legislation and frameworks, law enforcement and investigations, electronic evidence and criminal justice, international

cooperation, and prevention. Information on the latest development, progress made and best practices identified should also be periodically collected by the United Nations Office on Drugs and Crime (UNODC).

From September 26th to the 29th, the 86th Interpol General Assembly took place in Beijing, China. On October 4th, British Telecom (BT) and INTERPOL have signed an agreement which will see increased cooperation between the two organizations to prevent and combat cybercrime. Also, the United States government made changes to their law to grant FBI the permission to force entry - in other words, hack - into electrotronic devices around the world.

Question to Consider

1. Types of Cooperation among Countries

How can we provide a new or more effective form of cooperation among countries? Such cooperation should not only include the jurisdiction level but also education and propaganda level.

2. Capacity of Law Enforcement and Criminal Justice

How can countries get sufficient authority on investigation and jurisdiction when we need states to solve the problem timely while every state's sovereignty is still protected and respected?

3. The balance between policy and privacy

How much power can governments exploit in order to investigate and monitor the activities on the internet while it somehow infringes on people's privacy?

Supplementary Reading

Comprehensive Study on Cybercrime – Draft February 2013

https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Some synthetic information about cybercrime from norton

https://us.norton.com/cybercrime-definition

Resolution adopted by the General Assembly on 21 December 2010

http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/65/230