Forum: Human Rights Committee

Issue: Establishing Cyber Rights for Individuals

Student Officer: Jvalant Parekh

Position: President of the Human Rights Committee

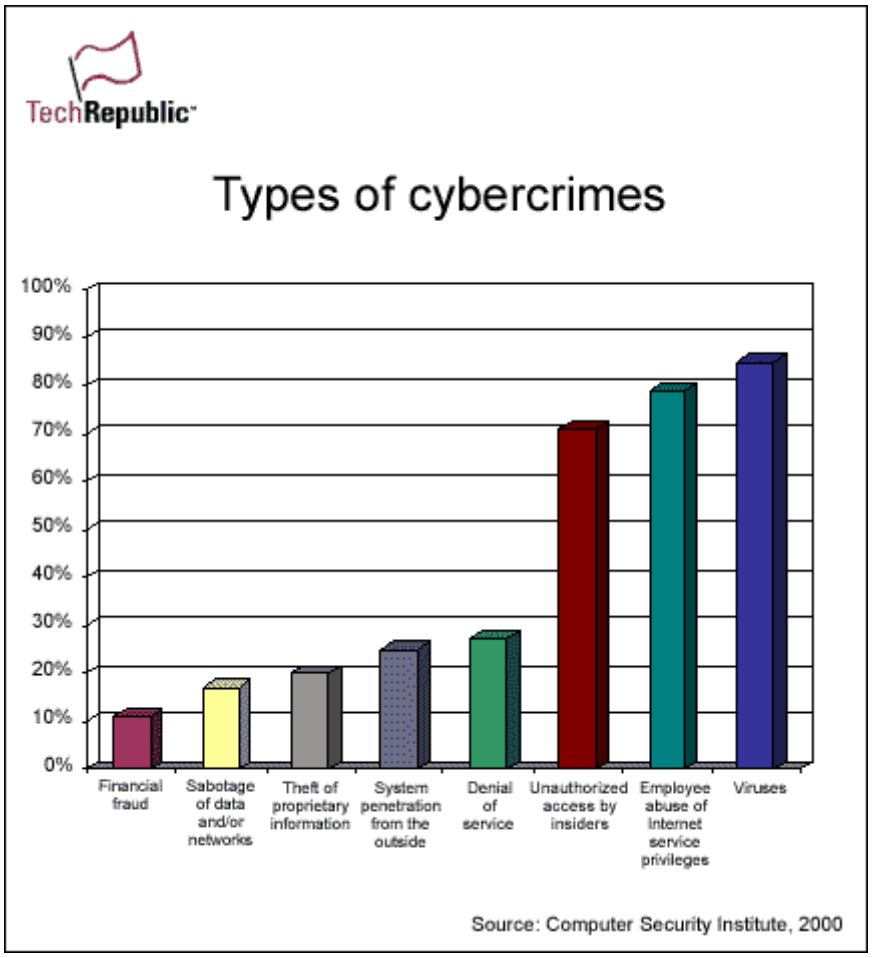
Introduction

The world as we know it is based around an array of technology. From the moment we wake up to an alarm clock on our phones to using desktops, laptops and tablets for reading the news. We often do not realize the problems that these devices can hold for the millions of people around the world that use them. They are not only a dangerous risk, but also potentially fatal.

When we use these devices, we are often connected to the internet; an entirely different world in comparison to Earth. The establishment of cyber rights for individuals is something that must not be taken lightly. Yes, there are other critical problems going on in the world at the moment but just recently, an article published by the BBC claim that a hacker had gained access to the BBC network and was ready to sell it before he could be stopped. It is cases like this that make people repeatedly realize the importance of staying safe on their computers and on the internet. It is vital that people recognize that they have rights when they are browsing the web. Key issues arising from a lack of such knowledge include cyber bullying, hacking and other cybercrimes. Cyber rights will enable a person to remain protected when they are using their computer or are connected to the internet.

There is current legislation regarding the issue of cyber rights, rather cyber security whereby people are protected as per the privacy they choose to have. Many social media sites are particularly susceptible to having their user's personal and private information being taken by hacker; something that requires immediate attention. The introduction of privacy settings to ensure that people are able to control what others see is an important step in trying to mediate the issue of establishing cyber rights because at least, the people are able to control what they show to the public. However, it still remains an open world with hackers constantly trying to gain access to people's private information through constant innovations in viruses and other malware designed to steal information and gain access to people's accounts and private information.

Another perspective on cyber rights is the right of the development of legislation to protect intellectual property of people. The famous case documented by the movie "*The Social Network"* defined and showed that intellectual theft, whether committed or not in the movie is another case, is a problem in the world and needs to be handled. The minimum legislation is in place and stricter protocol is required to tackle such an issue.



#Caption 1 - Image of types of cybercrimes and the rates of each type.

Definition of Key Terms

Cyber

Cyber refers to anything related to computers, information and technology and virtual reality. It also infers the relation to anything done on a computer or any general user interface that provides human interactions with a technological innovation. Thus the act of using a phone, computer, tablet, online gaming and online chat rooms can be included in the general meaning of cyber.

Security

A state whereby the feeling of being able to confine oneself within a given area to

feel a sense of safety. In the cyber world, this refers to cyber security whereby a person ensures that they can avoid the danger posed to them whenever possible. However, it also includes privacy settings and the importance of ensuring that a person is given maximum protection from possible stalkers and viruses. In many situations, the cyber security can be provided by software specifically developed to tackle both malware and adware to ensure greater safety of the user of the computer.

Human Rights

A right believed to belong to every single person living regardless of race, sex, nationality, ethnicity, religion, language or any other status. They are the fundamental rights of an individual as each individual is entitled to these rights without discrimination. Human Rights can be defined as those articles included in the Universal Declaration of Human Rights.

Cybercrime

These are simply criminal activities carried out using a computer or through the internet. The range of these crimes range from the sending out of spam, phishing (sending out e mails in the name of corporate businesses, usually with the aim of encouraging people to give out their personal, financial business) and forwarding of viruses containing malware with malicious content.

Cyber Law

Legal legislation designed with regards to information technology in the attempt to conserve people's rights and ensure levels of safety whilst on the internet.

Intellectual Property

This is defined as intangible property that is made by an individual on the basis of creativity and is protected against theft. However, the theft of such property continues to occur requiring continual changes to nation's legislation in order to change it and prevent such intellectual theft from occurring.

History

When we think of cyber rights, we establish the connection between computers and the rights of an individual. There are several things that we think of when this is suggested. The history of cyber law and cyber rights is minimal considering the significant development of technological devices in the turn of the 21st century. This makes the issue a more modern and novel problem.

Cyber rights were considered insignificant and were never developed in the past. That means that organizations such as APEC and the ASEAN along with global initiatives

such as the IGF have had to campaign and spread awareness in recent light. However, it is important to note that nothing more than that has been done to date. Nations have developed legislation but not followed through with it to the full extent that it should be regulated. Due to this, they fail to appreciate the grave danger and harm that has been caused as a result of this and this allows a nation's citizens cyber rights to be violated without any punishment.

Key Issues

Cybercrime and cyber security are not a 'priority' for countries at the moment

When the theme of the conference is considered in the fulfillment of the Millennium Development Goals, one must recognize that cyber related issues are not in there and thus not on the top of the list for many countries globally. Thus the initiative has been taken up elsewhere, by many organizations worldwide. Although the importance of safety on a computer and internet does not go unnoticed, the fact that other issues are facing countries on a greater scale means that it is a problem that has be de-prioritized. Consequently, the big problem is that countries are not focusing enough attention on something that will potentially be extremely harmful and threatening to the security of a nation and its citizens.

Cyber rights are not currently being developed, or not developed to the extent they need to be. Thus only minimum legislation regarding the matter is present.

The fact that countries are not considering it an issue of importance at the moment means it doesn't get the attention it needs. By having cyber rights implemented, people would be safer online. We would not need to hear the big stories about scandalous cybercrimes such as the recent hacking of the BBC server as crimes like these, with the correct implementation of cyber law, would become heavily punishable, a deterrent factor and maybe even impossible to carry through. The scandal involving the phone app "Snapchat" where 3 million users' personal numbers were downloaded from the Snapchat server shows the high degree of vulnerability people place in their technology. People should have the right to know that they are safe when using the internet and web based applications and thus the creation of legislation and cyber rights would provide a whole new pathway in counteracting cybercrime, security and prevention of hacking.

Major Parties Involved and Their Views

Organizations

There are many organizations that have been highly involved and very important in trying to maintain a sense of peace in cyber security. They have been imperative in the ensurance that cyber threats are reduced, thus helping people to establish their own cyber rights. There have been countries involved too in trying to create greater cyber law and

establishing legislation for punishment if cyber law is breached. In the need for cyber rights to be established, several worldwide organizations, some of whom are UN based are attempting to control cyber security.

Region Specific

Asia-Pacific Economic Cooperation (APEC)

APEC has a very strong influence in the Asia-Pacific region because of the unity it has created across all the nations. It has set about on a mission to improve telecommunication and information infrastructure across the region calling on all members to implement policies to create a greater sense of cyber security. This will in itself enable people to have greater purpose when using computers or the internet as they will know that they themselves possess cyber rights. APEC has taken the initiative into its own hands by publicizing the need for cyber security and cyber rights. Such actions are indicated in events such as the Cyber security Awareness Day.

Association of South-East Asian Nations (ASEAN)

ASEAN strives to improve stability and punish cybercrime. Again an organization which has unified member states in thoughts and ideology to some extent, it has campaigned against cybercrimes and recognizes the importance of establishing cyber rights. The mission it has set itself includes developing framework to exchange information between different agencies. ASEAN has held several meetings among the member nations throughout 2013 and in November 2013 Singapore Prime Minister recognized the importance of preventing hacking and allowing not only people but nations to have a sense of security by establishing commitment in stopping cybercrimes. He recognizes the need to strengthen defenses against such crimes in order to ensure countries maintain their ability to conserve sensitive information.

NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE)

NATO CCD COE has also been vital in establishing cyber defense in member nations as it strives to improve several of its IT based services including its capability to share, store and communicate information between the member nations. It also strives to become the worldwide leader in accumulating and creating information and knowledge on cyber defense worldwide as it seeks to share the information that it discovers. NATO CCD COE has also been important in creating awareness of the issue as it provides exercises and courses for people to successfully qualify as NATO CCD COE members on behalf of their member

nations. NATO CCD COE is also very important in the development of actual cyber rights for individuals as it seeks to establish a common law and legislative stature amongst all of its member states.

EuroISPA

EuroISPA is currently representing over 1700 internet provides across the entire European continent. It seeks to ensure European competence in cyber defense but also ensure that people are kept safe on the internet whilst delivering high quality internet. Whilst also trying to establish a free and open telecommunications market, it is also wants to ensure cyber rights can be created and maintained for individuals in order to facilitate safer surfing of the web.

International Specific

International Criminal Police Organization (INTERPOL)

INTERPOL seeks to not only implement improved cyber rights and cyber security, but also to ensure that worldwide police are able to communicate and receive and transfer information regarding criminals and criminal activity between each other. The importance of such a mission demands the education and understanding of all those involved in being safe online. As they establish such means they will pass it on to nations and the knowledge they have gained will become public information for people to use and keep safe when using computers themselves.

Internet Governance Forum (IGF)

With all UN member nations being members of the IGF, it is the perfect platform for launching global large scale changes in establishing cyber rights and countering cyber crime whilst improving cyber security. They currently seek to improve the security of the millions of people connected to the internet on a daily basis. They also provide a very important detail in that they make appropriate recommendations to the public when they find new information regarding better safety. They are also involved in the development of legislation to counteract cybercrime.

Countries

India

India has very recently recognized the threat of cyber security for its citizens

and implemented policies to establish rights for them. The recent "National Cyber Security Policy 2013" was a step forward and indeed a successful one for the nation as it strives to improve the rights of individuals for the betterment of the country. In particular, it also seeks to develop safety of the country's private information following recent issues with the USA with their own information being leaked out online.

USA

Citizens of the USA may have felt that their privacy was reduced significantly when Edward Snowden leaked classified information about the USA to the world. It showed that although there are cyber rights set up in the sense of human rights, further changes are necessary for the development of the nation as it seeks to improve its image. The US government however, continues to stress the fact that it seeks to maintain rights of individuals on computers and on the internet, but the validity of this statement is truly questionable.

Timeline of Relevant Resolutions, Treaties and Events

Date	**Event**
10th December 1948	Universal Declaration of Human Rights by the UN
15th August 2006	International Cybercrime Treaty
2011	Resolution 20/7 - Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building
2013	Resolution 22/7 - Strengthening international cooperation to combat cybercrime
2013	Resolution 22/8 - Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime

Evaluation of Previous Attempts to Resolve the Issue

Mentioned before are just some of the many organizations that have funded and attempted to solve the issue of cyber crime whilst developing cyber rights for individuals. Nevertheless, their attempts so far have not been enough for the extent that is needed. There have been no proper attempts to actually solve the problem at hand or as a matter of fact, to try to provide the necessary level of legislation in order to provide cyber rights to individuals. As such, many organizations such as APEC and ASEAN have campaigned repeatedly and attempted to strive to raise awareness on the issue of protecting people, establishing cyber rights and preventing cybercrime.

Furthermore, they have also been able to counteract and force people to recognize one more thing: cyber attacks are a real threat and people need to be prepared for any sort of attack. If people want to be protected on the internet, they themselves must take primary precautions in order to prevent themselves for having to go through serious consequences.

In the USA, the recognition of intellectual property is a step forward in trying to solve the issue from an alternative perspective. The establishment of cyber rights to a small degree has meant people's work can remain protected and safe and will not be liable to intellectual theft without the claimant being able to legally take action against the person or people who have stolen the intellectual property.

Possible Solutions

Nations need to first and foremost, before any solutions can be found, recognize the problem in order for it to be rectified. If they leave cybercrimes and cyber security as not one of their strongest priorities, they will suffer because of the problems citizens in their country will have. At the click of the mouse, a hacker, on a whim of selfish desire, can enter a country’s Federal Reserve Bank records and take all the money they wish to. Yes, there may be security measures to prevent this set up but many may find that it is simply a matter of time before these security protocols are breached and someone is able to bypass it. Whether or not they are able to get away with it is an entirely different matter. The fact, however, that they can actually enter in the first place is a problem in its own way and one that needs to be solved as soon as possible.

There are two ways to look at the solutions to this problem. The initial short term solution would be to increase government expenditure in trying to solve the problem by hiring more IT technicians. They also need to educate the public otherwise; they will not have enough knowledge of cybercrime. They also need to set out certain legislation to try to create cyber rights as the rights of the people is a necessity that countries cannot ignore.

It is understandable, to an extent, the reasons why many countries do not prioritize the creation of cyber rights, After all, with the theme of the conference being the accomplishment of the Millennium Development Goals (MDGs), all countries are striving to create a better global picture of themselves by attempting to reduce problems that affect

people on a greater personal level such as the inability to access education, lack of access to clean water and eradicating poverty within their country's boundaries.

However, they also need to realize that within their country anyone who has access to a mobile phone, a computer, or just any technological piece of device that enables them to share files, communicate and access the internet is at a threat. There are cases of people whose bank statements are breached and their bank accounts emptied simply through the hacking of their computer. Education is the way forward. If people are brought to the idea that they are taking a risk and understand that, whilst taking the necessary precautions to remain safe when connected to a cyber device, it would benefit the society and community within that country to a much greater extent.

A long term plan would be the creation of a division within the government which targets the improvement and implementation of cyber rights for individuals and firms in order to improve safety online. If such a division was created, people would know that they will be able to stay safe when online. The case of cyber bullying would greatly reduce as people would be aware of the prosecution that they will face for defying the cyber rights of another individual. Furthermore, if this is considered by the United Nation, it will result in integration with the Universal Declaration of Human Rights. As a result of the developments that have taken place in the world, the reliance people have on technology that it would have to be taken into consideration in a modern day context.

Finally, a radical solution would be to force people to reduce the computer usage. By creating cyber rights for these people when they are online, they would understand that they are safe but possibly for a fixed period of time. Without this they may not remain safe.

When considering the alternative theory of intellectual property, another possible solution would be to try and introduce greater legislation and harsher punishments to ensure people recognize intellectual theft as a serious offence and are given the appropriate punishment in line with the seriousness of the crime.

Bibliography

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp

"Council of Europe." *Cybercrime Resources Competent Authorities and Points of Contact for International Cooperation*. N.p., n.d. Web. 09 Jan. 2014.

http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group/Cybersecurity-Awareness.aspx

"Cybersecurity Awareness Day - Asia-Pacific Economic Cooperation." *Cybersecurity Awareness Day - Asia-Pacific Economic Cooperation*. N.p., n.d. Web. 09 Jan. 2014.

https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ-ECOSOC/CCPCJ-ECOSOC-00/CCPCJ-ECOSOC-11/Resolution_20-7.pdf

"Resolution 20/7." *United Nations Office Against Drugs and Crime*. N.p., n.d. Web. 9 Jan. 2014.

http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr

"Intellectual Property." *FBI*. FBI, 16 Apr. 2010. Web. 07 Jan. 2014.

http://www.sans.org/reading-room/whitepapers/incident/international-cybercrime-treaty-ratification-1756

International Cybercrime Treaty." *SANS Institute*. SANS Institute, n.d. Web. 9 Jan. 2014.

http://www.webopedia.com/TERM/C/cyber_crime.html

"Cyber Crime." *What Is Cybercrime ?* Webopedia, n.d. Web. 07 Jan. 2014.

https://www.unodc.org/unodc/en/commissions/CCPCJ/05-resolutions-10.html

UNODC. "Crime Related Resolutions." *UNODC*. UNODC, 2010-2013. Web. 9 Jan. 2014.

http://dl.cbsimg.net/i/tr/cms/contentPics/r00620000616jsn01_01.gif

#Caption 1 - "Types of Cybercrimes." *TechRepublic*. TechRepublic, 2000. Web. 9 Jan. 2014.