International Journal of Research in Social Sciences
Vol. 8 Issue 1, January 2018,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

ROLE OF UN IN TACKLING CYBER CRIME

Pallvi Sharma[*]

Abstract

Of lately women are working in many sectors such as the IT sector. The growing online presence of women on the internet has made them more vulnerable to become victims of cybercrime. Women face harassment through many types of cybercrime. The UN, through the international Telecommunications Union (ITU), its specialised agency for information and communication technologies has a vital responsibility to ensure the safety of all those who venture online, especially as online services become an integral part of people's lives. The paper has tried to find out the key steps taken by UN to curb the crime.

Key Words: Cyber Crime, Physiological, Mental Harassment, Attitude, Teenage.

[*] **(Ph.D Research Scholar), Dept of Defence & National Security Studies, Panjab University, Chandigarh**

Introduction

The idea of an international organization for maintaining peace and human betterment is very old and traced back to the ancient times. It was the urge for pace and self-preservation and violence of war that inspired man to devise institutions for greater international cooperation and avoidance of confrontation.[1] The United Nations (UN) comprises a group of international institutions that include the central systems located in New York, the specialised agencies such as the World Health Organization (WHO), International Labour organizations (ILO) and programs and funds such as the United Nations Children's Fund (UNIEF) and United Nations Development Program (UNDP). Created more than half a century ago in the aftermath of the Second World War, the United Nations reflected the hope a century ago in the aftermath of the Second World War, the United Nations reflected the hope for a just and peaceful global community. It is the only global institution with legitimacy that derives from universal membership and a mandate that encompasses security, economic and social development, the protection and of human rights and protection of the environment. Although the UN was created by the states, for the states, the relationship between state sovereignty and the protection of the needs and interests of people has not been fully resolved. Questions about the meaning of sovereignty and the limits of UN action have remained key issues of discussion.

UN is working for global interconnectivity at an unprecedented pace. According to International Telecommunications Union (ITU), a specialised agency of the UN, estimated that two billion people were online by the end of 2010; by 2015 the number had reached five billion. The ITU also reckons that 143 countries currently offer 3G services, potentially providing Internet access through smartphones to a growing portion of the estimated 5.3 billion people with mobile subscriptions, 3.8 billion of which are in the developing world. Unfortunately, the more the number of people online, the more vulnerable they become to cyber threats.[2]

Of lately women are working in many sectors such as the IT sector. The growing online presence of women on the internet has made them more vulnerable to become victims of cybercrime. Cybercrime has become one of the burning global issues. Many crimes are committed against women such as rape including marital rape, domestic violence and cybercrime. Cybercrime against women through internet has assumed alarming proportions. Women face harassment through many types of cybercrime. A few organisations have emerged as the silver lining by making efforts for improving the status for women and gender equality by tackling cybercrime. The objective of UN Women is not only to promote the rights of women, but also to seek freedom from forced marriage, prostitution, malnutrition, illiteracy, unequal treatment in family, society and professional sectors. However in many countries, women and girls face discrimination and harassment through Cybercrime. Women do two-thirds of the world's work, but receive only 10% of the world's income and own only 1 percent of the means of production.[3]

Global international efforts by the United Nations to curb Cyber crimes

Another issue that is of prime concern to the UN in present times is Cyber crime against women. The UN, through the international Telecommunications Union (ITU), its specialised agency for information and communication technologies has a vital responsibility to ensure the safety of all those who venture online, especially as online services become an integral part of people's lives. The ITU has dealt with security issues since its inception in 1865 from the invention of the telegraph, through the era of radio and television to the deployment of the satellite and Internet based technologies. ITU recognizes that information and technology are critical priorities for the international community. Cyber crimes have become one of the biggest global network of open conduits. While these bring untold benefits in terms of access to information, they also lead to an alarming rise in the number and scale of cyber threats, cybercriminals and cyber terrorists. For example, according to the International Multi-stakeholder partnership against Cyber Threat (IMPACT) more than a million ICT systems worldwide are affected at any given time by malware. Cyber security is one of the most critical concerns of the information age. It forms the cornerstone of a connected world. It is a global issue that demands at truly global approach. The virtual world increases in its power and reach with every passing day. The internet may open our minds to new possibilities, but it also exposes us to the pitfalls and dangers of cyber threats. The internet has become has become integral part of modern societies. Cyber threats such as malicious software (malware) are becoming extremely sophisticated. This is especially true with the increased presence of organized criminal groups online. But criminals are not the only threat on the internet. The vulnerabilities of ICT'S also extend to cyber warfare, espionage and terrorism all of which can pose serious threats to critical information infrastructure. The ITU Secretary General launched the Global cyber Security Agenda (GCA) on May 17, 2007 to provide a framework within which an international response to the growing challenges to cyber security can be coordinated and addressed. The GCA is an international cooperation framework and strives to engage all stakeholders, including governments, private sector, civil society and international organizations, in a concentrated effort to build confidence and security in the information society.

The International Telecommunication Union (ITU) is collaborating with both UN member states and private sector partners to identify current challenges, consider existing and emerging threats and propose global strategies goals:

- Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.
- Elaboration of global strategies for the creation of appropriate national and regional organizational structure and policies in cybercrime.
- Development of a strategy for the establishment of globally accepted minimum security and accreditation schemes for hardware and software applications and systems.
- Development of a strategy for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.
- Development of a global strategy for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.
- Development of a strategy for the creation of a global framework for watch, warning and incident response to ensure cross border coordination between new and existing initiatives.
- Development of a strategy for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.
- Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structure to ensure the recognition of digital credential across geographical boundaries.
- Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organisational structure to ensure the recognition of digital credential across geographical boundaries.

- Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organisational structure to ensure the recognition of digital credential across geographical boundaries.
- Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structure to ensure the recognition of digital credential across geographical boundaries.
- Development of global strategies to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors.
- Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above mentioned areas.[4]

There some convention or protocol and resolution passed by the UN to combat cybercrime such as:

The convention Protocol on Cybercrime and cyber security by the UN in 2010. The final draft code was prepared by the International law commission. A combined global initiative at the UN level by organizations such as United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) should be established. This initiative could have as a final goal, a Draft convention that should be submitted to the International Law Commission for considering a UN sponsored Convention on peace and security in Cyberspace. General principles relating to mutual assistance as described in the Convention on Cybercrime Articles 26-35 are included in the assistance that Interpol may offer to their member countries, and need to be included in a convention.

Trans-border access to stored computer data with consent or where publicly available, as described in Articles 32, must be based on consensus by each country. Some countries do not accept such principles, and must be based on consensus by each country. Some countries do not accept such principles and must be respected for their opinions. With regard to the 24/7 Network, as described in Article 35, is not needed in a convention. Both Interpol and the G8 countries offers a 24/7 network. The G8 24/7 network is offered to countries outside member countries and includes more than 40 countries.[5]

- In its resolution 65/230, the General Assembly requested the Commission on Crime Prevention and Criminal justice to establish an open-ended intergovernmental expert group which should conduct a wide-ranging study on problems related to cybercrime and responses to it by the member states. The international community and the private sector advocated for including information technology in national legislation besides incorporating best practices, technical support and international cooperation with a view to examining options to support existing laws and to propose new national and international legal other responses to cybercrime. These proposals were included in paragraph 42 of the Salvador Declaration on comprehensive Strategies for global challenges: Crime Prevention and Criminal Justice Systems and their Development in a changing world. The first session of the expert group was held in Vienna from January 17-21, 2011. The group of experts reviewed and adopted a collection of topics and a methodology for the study in that session.
-

The general assembly noted in its resolution 67/189, that an open-ended inter-governmental expert group should conduct a wide-ranging study for the problem of cybercrime and urged it to increase its efforts to complete its work and to present the outcome of the study to the Crime Commission in due course. The second session of the expert group was held from February 25-28, 2013. At that session, the expert group took note of the wide ranging study on the problems of cybercrime and the responses to it by the member states, the international community and the private sector, as prepared by the United Nations office on drugs and crime (UNODC) under the auspices of the expert group, pursuant to the mandate contained in General Assembly resolution 65/230. The third session of the expert group was held in Vienna from April 10-13, 2017for further information and a comprehensive study on cybercrime.[6]

- Resolution 55/63 combating the criminal misuse of information technologies.

The UN millennium Declaration, in which member states resolved to ensure that the settlement of new technologies, especially information and communication technologies (ICT), in conformity with recommendations contained in the Ministerial Declaration of the high level segment of the substantive session of year 2000 of the Economic and Social council, are available to all.

In its resolution 45/121 of 14 December 1990, the member states also recalled the recommendations of the 8th UN Congress on the prevention of Crime and the Treatment of offenders, and noted in particular the resolution on computer related crimes, in which the 8th Congress called upon member states to strengthen their efforts to combat computer- related crime more effectively and highlight the assistance that the UN and in particular the Commission on Crime Prevention and Criminal Justice can provide in making efficient and effective law enforcement and administration of justice of the highest standards of fairness and human dignity. The congress also advocated for free flow of information which can promote economic and social development, education and democratic governance. The resolution also noted the importance of advancements in the development and application of information technologies and means of telecommunicati- on. Explicit worries that technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies were cited and called for increased the global cooperation and coordination that may vary from state to state.

The developing countries acknowledge that gaps in the access to and use of information technologies by states can diminish the effectiveness of international cooperation in combating the criminal misuse of information technologies and nothing the need to facilitate the transfer of information technologies in particular; recognizing the need for cooperation between the states and the private industry in combating the criminal misuse of information technologies and in this context stressing the role that can be played by both the UN and regional organizations.

The work of the 10th UN Congress on the prevention of Crime and the treatment of Offenders and the work of the Committee of experts on crime in cyberspace of the Council of Europe on a draft convention on cybercrime, the principles agreed to by the Ministers of Justice and Interior of the Group of 8th Congress in Washington, D.C on December 10, 1997, which were endorsed by the heads of State of the Group of Eight(G-8) in Birmingham, UK and northern Ireland on may 17,1998, the work of the Conference of the group of eight on a dialogue between government and industry on safety and confidence in cyberspace, held in Paris from 15-17 May, 2000 and the recommendations approved on 3 March 2000 by the Third Meeting of Ministries of justice or of Ministries or Attorneys General of the Americas convened in San José, Costa Rica from 1-3 March 2000 within the framework of the Organisation of American states.

The efforts of the above mentioned bodies to prevent the criminal misuse of information technologies culminated into measures to combat such misuse. The key measures include:

a) The states should ensure fair and strict implementation of their laws and eliminate safe heavens for those who criminally misuse information technologies.

b) Law enforcement and cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned states.

c) Information should be exchanged between states regarding the problems that they face in combating the criminal misuse of information technologies.

d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies.

The United Nations efforts to Tackle Cyber Crime

The United Nations which is a forum of 191 member States played an active role in the field of Cyber security protection and cyber crime prevention. In 1985, the General Assembly of the UN in its resolution 40/71 of 11 December called upon governments and international organisations to take action in conformity with the recommendations of the Commission on the Legal Value of Computer Records of 1985 in order to ensure legal security in the background of broadest possible use of information processing in international transactions.

Concerning computerized personal data files, the UN General Assembly adopted the guidelines in 1990. It proposed to take appropriate measures to protect the files against both manmade and natural dangers. The guidelines extended the protection of governmental international organizations.

For further international work, ‘The international Review of Criminal policy, UN Manual on the prevention and Control of Computer related Crime’ presents a comprehensive statement of the problem. It stated that at the international level, further activities could be undertaken, including harmonizing substantive law, and establishing a jurisdictional base.

At 10th UN congress, the Background paper for Workshop on Cyber crimes proposed two levels of definition of crimes related to computer networks. In brief, the Strict Computer Crime had to refer to "any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them." For further explanation, Cyber Crime can be denoted as "any illegal behaviour committed by means of, in relation to, a computer system or network.

The UN General assembly has endorsed several resolutions dealing with its desire to witness progress regarding cyber crimes namely Checking Resolution 55/63(2000) and 56/121(2001) on combating the criminal misuse of Information Technology. All states were urged to consider the eight principles of checking Resolution 53/70(1998), 54/74 (1999), 55/28 (2000), 56/28 (2000), 56/19 (2001), 57/53 (2002), 57/239 (2002) and 58/199 (2003). All these resolutions called on the member states "to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats." These resolutions have the same motive to improve the Cyber security awareness at both the international and national levels.

In resolution 55/63(2000), the UN General Assembly highlighted the importance of the following measures to combat computer misuse:[7]

a) to ensure the elimination of safe havens for Cyber criminals.

b) to coordinate in the investigation and prosecution of Cybercrime.

c) to share information for Cybercrime.

d) to train and equip law-enforcement personnel to address Cybercrime.

e) to protect the security of data and computer systems from Cybercrime.

f) to permit the preservation of and quick access to electronic data pertaining to particular criminal investigations.

g) to ensure mutual assistance regime for the timely investigation of Cybercrime and the timely gathering and exchange of evidence.

h) to remind the general public of the requirement to prevent and combat Cybercrime.

i) to design information technologies to help to prevent and detect Cybercrime.

j) to take into account both the protection of individual freedoms and privacy and the preservation of the capacity of Government to fight Cybercrime.

The UN General Assembly invited the member states to consider the measures in their endeavour to fight the criminal misuse of information system, and decided to maintain the question of the information technologies on the agenda of its future session.

In resolution 56/121 (2001)[8], the UN General Assembly invited states to consider the work and achievements of the commission on Crime prevention and Criminal Justice and of their International and regional organizations when developing national law policy and practice to prevent Cybercrime. The resolution emphasised the value of the measures set forth in Resolution 55/63 (2000) and again invited states to take them into account in their efforts to combat the criminal misuse of information technologies. However, the General Assembly decided to postpone the consideration of this subject, to consider pending work in the plan of action against high technology crime of the Commission on Crime prevention and Criminal Justice.

The consensus on Cybercrime in various forums of the UN remains a preliminary concern. In 2010 the UN rejected the request of Russia to hold a UN Convention on Cybercrimes stating that there is no need for a convention on Cybercrimes as there already exists a consensus based mandate on the subject, namely the 'Budapest Convention on Cyber Crime 2001' convened by the European Union Council. The UN has not taken much interest in Cyber Crimes; the International Criminal Law Network (ICLN) organized a Cyber Crime Conference in the Hague on 13-12-2012. Judge Stein Schjoldberg introduced a proposal for an International Criminal Court or Tribunal for Cyber space.

United Nations (UN) Global Cyber security Index 2017

The Global Cyber security Index (GCI) [9]is a survey that measures the commitment of Member States to cyber security in order to raise awareness. The GCI revolves around the ITU Global Cyber security Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was also collected. One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results reported herein cover all 193 ITU Member States. The 2017 publication of the GCI continues to show the commitment to cybersecurity of countries around the world. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions. However, there is space for further improvement in cooperation at all levels, capacity building and organizational measures. As well, the gap in the level of cybersecurity engagement between different regions is still present and visible. The level of development of the different pillars varies from country to country in the regions, and while commitment in Europe remains very high in the legal and technical fields in particular, the challenging situation in the Africa and Americas regions shows the need for continued engagement and support.

Suggestions

International organizations and national government are doing very less efforts to combat cybercrime and the given suggestions will be useful to tackle cybercrime.

a) To change passwords time to time. Mysterious and complicated passwords protect all accounts including mobile phones, emails, landlines, facebook, banking, credit etc. and are difficult for anyone to guess. Do not share any password with anybody. However, changing password can be very helpful to keep privacy safe.

b) It should be necessary to set up awareness campaign from the grass root level such as schools, collages etc about cyber crimes like cyber pornography, stalking cheatings, economic cheatings, defamatory activities, misusing emails and social networking websites, virtual rapes, email spoofing etc. These campaigns can be very fruitful in combating cyber crimes.

c) Woman should avoid unwanted or unsolicited phone calls and messages because cell phone may be monitored. If it happens again and again, it should try to record phone calls of harasser and report to cyber crime cell.

d) There should be an International coordination Centre. It should share the responsibility to improve the Internet security and co-ordinate effective international global response to computer security incidents and events.

e) There is an immediate need of a detailed legal structure followed by institutional arrangements for compulsory jurisdiction of judicial forum to adjudicate such violations. A wide-ranging international Conference with focal point on cyber crimes should urgently be formulated and an 'International Criminals Tribunal' with global jurisdiction to investigate, try and punish cyber offenders is to be set up.

Conclusion

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one major challenge underlines this. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach. Cyber security strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime. The development and support of cyber security strategies are a vital element in the fight against cybercrime.

References:-

[1] Kaur Swapandeep, "International Organisation", Shree Ram Law House, Chandigarh 2010, p.p.2

[2]Andreasson Kim, "Cybersecurity- Public Sector threats and responses", Auerbach publications, CRC press, London, NewYork, 2012,pp.13.

[3] Kumar Chanchal and Gupta Sanju, "United Nations and Global Conflicts." Regal publications, New Delhi, 2013, pp. 383-384.

[4] Andreasson Kim, "Cybersecurity- Public Sector Threats and Responses", Auerbach Publications, CRC press, London, NewYork, 2012, pp.77-84.

[5] Schjolberg Stein and Helie Solange Ghernaouti, "A global Protocol on Cybersecurity and Cybercrime,2009.

[6] https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-oncybercri me.html.

[7] General Assembly Resolutions 55/63-combating the criminal misuse of information technologies, A/RES/55/63, Fifty-fifth session, Agenda item 105, 22 January 2001. https://www.itu.int/ITU-D/cyb/ cyber-security/docs/UN resolution_55-63.pdf.

[8] Westby, J. (2004). International Guide to Cyber Security. American Bar Association, p.315.

[9] Itu.int. (2017). Cite a Website-Cite This For Me. [online] Available at: https://www.itu.int/dms_pub/itu-d/opb/ str /D-STR-GCI.01-2017-PDF-E.pdf [Accessed 3 Nov. 2017].