Volume 13, December 2020 ISSN 2581-5504

"Contemporary Issues and Challenges in Cyber Security"

Yashwanth A S
Dr. RML College of Law,
Bangalore

Introduction:

The effectiveness of contemporary computer applications is generally considered a function of 5 basic attributes of secure computer and data systems: availability, accuracy, authenticity, confidentiality, and integrity. The concepts generally apply to government, business, education, and therefore the ordinary lives of personal individuals. The considerations normally involve extended Internet applications hence the name Cybersecurity. Achieving and maintaining a secure cyberspace could be a complicated process, and a few of the concerns involve personality, privacy, material possession, the critical infrastructure, and therefore the sustainability of organizations. The threats to a secure operating infrastructure are serious and profound: cyber terrorism, cyber war, cyber espionage, and cyber-crime, to which the technical community has responded with safeguards and procedures, usually supplied by the private sector.

The big data environment supports to resolve the problems of cyber security in terms of finding the attacker. There are security challenges of massive data still as security issues the analyst must understand. It's more focused on the tools and techniques of knowledge mining for the employment of massive data analytics in terms of security and also the use of techniques for security to guard big data in terms of applying encryption capabilities. Cyber security may be a continuously evolving enigma which can't be ignored by the organizations anymore. Since the attack techniques have gotten intrusive still sophisticated, it's become mandatory for a business to take a position in its cyber security to reduce the possibilities of cyber-attacks.

Throughout history, mankind has waged war, seeking to further national agendas in an ever changing international game of power. From the sword battles of the past to the un-manned drone strikes of today, this game of power is consistently driven to shift and evolve by technology. The event of armoured vehicles, aircraft, ships and therefore the use of electronics and telecommunications have all expanded the battle space and introduced new and innovative ways to achieve a bonus over opponents. Even as the technological innovation of flight triggered a race to dominate the skies, the emergence of cyberspace has opened new strategic possibilities and threats, causing a scramble to secure a dominant position within it. Conflict and war in any form has the potential to the touch all and sundry, whether as a combatant, relative of a combatant, civilian, business entity or nation state. This makes research into cyber warfare both valuable and essential to unravel the growing number of issues raised by this new domain of war.

Contemporary research into the subject is wide ranging, covering variety of sub topics starting from legal issues on lawful competency to attempts to exactly define what a cyber weapon is. For anyone attempting to approach the sphere of cyber warfare, there's a challenge in gathering an understanding of all issues involved, how they relate to every other, what this state of research is and where future research is required.

Interconnectivity between elements is desirable and typically cost effective, so a good style of dependencies have evolved in normal circumstances, and cyber intrusions have emerged.Thus, a tiny low group of people can compromise an outsized organization or facility, which is usually referred to as an asymmetric threat against which methodological protection is important.

“Cyberwar refers to conducting, and preparing to conduct, military operations per information-related principles. It means disrupting if not destroying the data and communications systems, broadly defined to incorporate even military culture, on which an adversary relies so as to grasp itself: who it's, where it's, what it can do when, why it's fighting, which threats to counter first, etc.

It means trying to understand all about an adversary while keeping it from knowing much about oneself. It mean stunning the balance of data and knowledge in ones favour, especially if the balance of forces isn't. It means using knowledge so less capital and labour may must be expended Arquilla and Ronfeldt see cyberwar as a battle for control over information and communication flows, with the last word aim developing a bonus over an opponent. During this respect, there are similarities with the ideas of knowledge warfare.

From a security perspective, the employment of the term “cyber” generally means over just the net, and typically refers to the utilization of electronics to speak between entities. The topic of cyber includes the net because the major data transportation element, but also can include wireless, fixed hard wires, and electromagnetic transference via satellites and other devices.

Cyber elements incorporate networks, electrical and mechanical devices, individual computers, and a spread of smart devices, like phones, tablets, pads, and electronic game and entertainment systems. The near future portends road vehicles that communicate and driverless automobiles. An affordable view would be that cyber is that the seamless fabric of the fashionable information technology infrastructure that permits organizations and personal citizens to sustain most aspects of contemporary existence.

Further Interference:

There are numerous technological advancements over the last decade. Nowadays we've got come upon number of crimes against women. Cyber Crimes against Women in India reveals loopholes within the present laws and policies of the Indian scheme. Recent researches reveal that over the years the cybercrimes have increased by nearly 63.7 per cent.

Types of cybercrime that are committed against women:

- Harassment via e-mails: Harassment through e-mails isn't a brand new concept. It’s very like harassing through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via email. E-harassments are almost like the letter harassment but creates problem very often when posted from fake ids.

• Cyber-stalking: Cyber stalking is one amongst the foremost talked about net crimes within the times. The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the net by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles.

• Cyber pornography: Cyber pornography is that the other threat to the feminine netizens. This may include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and also the Internet (to download and transmit pornographic pictures, photos, writings etc.)

• Defamation: Cyber tort including libel and defamation is another common crime against women within the net. This happens when defamation takes place with the assistance of computers and / or the web.

• Morphing: Morphing is editing the first picture by unauthorised user or fake identity. It absolutely was identified that female's pictures are downloaded by fake users and again re-posted/uploaded on different websites by creating fake profiles after editing it.

• Email spoofing: A spoofed e-mail is also said to be one, which misrepresents its origin. It shows its origin to show a discrepancy from which actually it originates.

In India:

The information technology sector in India has seen a quantum jump since 1990s which continues to be continuing. Almost every household with moderate status have internet access. In other words, internet has brought the globe in our living rooms. People from the people of 13 to 70 years who have access to the net are continually using this either reception, or at workplaces, or at cyber cafes, or at education institutions etc.

Thus, it's exposed the society to a brand new world during which we will share our ideas and culture values and may enjoy all opportunities. But it's not a danger area. Cyber space has become an instrument for offenders to victimize or infringe women, the foremost vulnerable targets on internet after children. Internet has opened flood gates for various crimes against women within the cyber space.

Even though, draftsmen and other world leaders who participate in EU conventions for establishing strict rules to manage cybercrime against children, never considered victimization of ladies within the cyber space as a giant issue like porn or hacking etc. which require an attention.

Some Suggestions and Steps to Taken Care of:

Besides, reckoning on system against cyber-crimes, women need to remember of cyber victimization by self, because time has come to reject the acceptance of silent. Moreover cyber laws don't seem to be universal, as they vary country to country. Today, every netizen wants to browse web privately and safely especially women. We must always take some steps to tackle this problem. Here are some steps and suggestions that how women can save themselves of being victimized in cyber space and the way they'll make their online perceptions and skill safer one, areas follows;

- Change the Passwords for each month.
- Don’t keep one password to several apps, use different passwords.
- Keep changing Debit/Credit Passwords regularly.
- Activate the two Factor Verification within the email, WhatsApp and the other apps which allows you to activate the identical.
- Don’t share the OTP, ATM Pins, and Email Passwords with anyone.
- Don’t share any personal photos in any Social Media Platforms, it’s been causing the new way of Cyber-crime and harassing the people.
- Don’t post personal details within the Social Media, if needed, anybody can give the main points within the Messenger app if you don’t have Email or signal of someone.
- Use the Faraday Bag or Faraday Wallets to avoid the possibilities for a cyber-crime.
- Avoid the usage of Public Wi-Fi to avoid the Cyber Crimes. It should easily cause crime because not secured one and may take any details from the mobile especially the Banking Apps within the mobile, User ID and Passwords of the other apps.

Industry Safeguard Protocols:

- Industry players are important digital gatekeepers. They include ISPs, portable companies, social networking sites, online dating and gaming sites, website operators and software developers.
- Tech companies have to explicitly recognize cyber VAWG as unlawful behaviour, and demonstrate increased and expedited cooperation in providing relief to victims/survivors within the capacities that companies have.
- In particular:−Better systems for cooperating with law enforcement−More effective takedown procedures for abusive and harmful content an opportunity of account termination for misconduct production of transparency reports of records specific to cyber VAWG, detailing how and once they have responded.

Conclusion:

The visibility to beat the cybercrimes against women as an entire is challenging and therefore the only way is to know cybercrimes. Government must strengthen the system to lower cybercrimes, because criminals consider it much easier than traditional crimes because of less chance of being caught and fewer penalties.

Secondly, what has to be changed is that the sense or attitude of the society towards women, to not consider woman as a commodity. People need to understand that violence against women is nothing but a manifestation of gender discrimination and inequality in gender power relations.

Thirdly, women should understand that the time has come to reject the silence or reticence and are available forward for fighting against cybercrimes and for his or her rights.

Fourthly, it requires a daily research and a spotlight on cybercrimes. It must be studied thoroughly which should be funded by government.

Fifthly, police personnel must incline training so as to tackle and handle cybercrimes. For this purpose, workshops and seminars on cyber space education must be organized. Women should also participate in such style of activities. Again but, within the end people has got to change their state of mind towards women and will develop the sense of commonality because cleanliness starts from home.

Amongst the varied cyber-crimes committed against individuals and society at large the crimes mentioned above are specially targeting women. Cyber World could be a dark street wherein many people are laid low with different attacks but many are unaware of the actual fact that these styles of attacks are happening. Red Team has met and witnessed lot of victims where they don’t understand how to stop and punish those culprit. The most loophole that’s exploited by the attackers is that the lack of awareness.

The growth of cyber-crime in India, as everywhere the planet, is on the increase. Anybody who uses the net is in danger for becoming a victim of cybercrime. Cyber space offers a plethora of opportunities for cyber criminals either to cause harm to innocent people.

India is taken into account united of the only a few countries to enact IT Act 2000 to combat cybercrimes. This Act is widely covered commercial and economic crimes which is obvious from the preamble of the IT Act but it's observed that there's no specific provision to safeguard security of ladies and kids.

However there are few provisions to hide a number of the crimes against women in cyber space under that Act. So as to avoid the cyber-crime we should always not engage in conversation with people we do not know. People on the opposite end of the pc might not be who they claim to be. We must keep our passwords protected and don't keep sensitive material on the pc as which will be accessed by the hacker. If anything seems out of place or wrong, contact enforcement immediately. Indian women netizens are still not receptive immediately report the cyber abuse or cyber-crime. This nature provides the offenders the possibility to flee after the commission of cyber-crime. The matter would be solved only the victimized woman then and there report back or perhaps warn the abuser about taking strong actions.

With the exponential increase within the use of the net as a medium of communication and sharing of knowledge, chances of use of the online for publication of defamatory content has increased multi-fold and there's a coherent need for a transparent law during this area.