"THE OUTBURST OF CYBERCRIME AND CONSEQUENCES OF DARK WEB"

TOSHESH BANTHIA & KRIYA DHARA K

INTRODUCTION

The world in which we live today is far most advanced than it used to be, technology is a man-made science which is used in almost every aspect of life. From the age of birth till death science has always been inter connected with us. In the field of science one of the significant inventions is the internet. Every single human in this planet is living in the world of internet. We have shown many improvements in our lives with the usage of internet. The internet has two phases one is the positive usage and the other one is the negative usage. Most of us are familiar with the term piracy, it means trying to get a content from internet without paying a single penny, it can be music, movie software etc., but some of us use internet for productivity, to improve our knowledge by reading, watching or through live interaction with the prominent personalities in a particular field, all of these are done with the assistance of internet. Though there is a constant development in the field of internet there has also been many new improvements which has been introduced, for instance sending text message using the subscriber identity module (SIM card) has become very much limited, at present we use applications like WhatsApp, Twitter, Telegram etc., to communicate. By stepping inside the world of internet we are giving our personal information and all of our information are stored in the cloud servers, it is not difficult for hackers to get those details they use such information to commit crimes. Dark net is yet another platform which can be called as a twin of internet but the only difference is that it's not commonly used by the people. As per the recent times it is used for the purpose of conducting all sorts of illegal transactions, there are many organizations formed across the world for the purpose of monitoring the activities taking place inside the dark web.

CYBER-TERRORISM

There are many types of crime in this world, from the early stages of life the types of crimes have considerably increased and in recent times the most developing area is the cyber-crime. The initial beginning step of cyber-crime is to hack into the data and collect all the information about an individual, company or an organization. Data is the personal information of a person or a company and it is considered as a valuable resource for many companies. There has been an enormous growth under the hood of cyber-crime and the most dangerous aspect in cybercrime is the cyber-terrorism, when we think of terrorists the first thing that comes to our mind is ammunition, bomb blasts and death of

numerous innocent civilians, but as a matter of fact internet has reached even the terrorists and they have started using it as their median to conduct their terrorist activities. There are many terrorist organizations, being the basic goal of such organization is to convince people to join and praise their ill motives internet has made the job of such groups much easier, as the approach of these people is to convince innocent people from all over the world to fight for their moto and through internet they are safely seated in their protected arena and contacting the weak-minded people. Every young person is connected with the internet hence, they use this as an opportunity to brainwash such minds and convert them as a terrorist and convince them to work for them. They use internet as a biggest medium to communicate with such persons through sending encoded messages[1]. In a broader sense the primary motive of these terrorist groups is to disseminate antagonism among the people, they are so trained that they do not let the receiving end to give it a second thought of what they have conveyed, they consider it as an order and blindly follow it. There are various desperados across the world, it will be a high-wire act to publicly communicate with them hence, these terrorist organizations have started using internet as a median to communicate which hides their identity and also ensures that the communication is entirely encoded and adding to it, it also makes it challenging to uncover the persons who is actively behind it. Jihadism is a movement conducted by Islamic people there are many organizations formed by them one of the most popular is the Al-Qaeda the founder of this group is said to be Osama Bin Laden, this organization got its attention only after the so called 9/11 attack which happened in the year 1998. After this attack the US Government an agency to counter terrorism the primary duty was to keep a track on the leaders, the financial aids funded to the organization and also to trace out the communication. For any type of terrorist attack communication plays a significant role more particularly when the attack is on an enemy country. Communication is the first key to execute their end goals, even if a leader of an organization is killed yet it is not easy to close the entire organization, the very next day a new leader will be selected among the existing members. Communication is one of the major weapons and also a shield used by the terrorist groups. The world is getting more and more smarter each and every day and as far as these organizations are financially equipped all kinds of latest technologies will be used by them. There is also a flip side to cyber terrorism, when a person or a group of persons tries to hack into the systems of military of a specific country and collects the undercover information and leaks it to the hostile territory then it also amounts to cyber terrorism. As and how the world has started developing their knowledge by using internet, even the terrorist has also started using the hyperspace knowledge to benefit and fulfill their demands.

[1]Gilbert Ramsay, *Conceptualising Online Terrorism,* vol.2 JSTOR 3, pp.3-10(2008). https://www.jstor.org/stable/26298357?seq=1&cid=pdf-reference#references_tab_contents

CYBER DEFENCE MECHANISM

Cybercrime is one of the rapidest growing aspect throughout the world, breach in cyber security is a real threat to various companies. In the year 2014 almost 97% of organizations from across 63 countries have detected a breach in their cyber security[2]. The people hacking into the system of major companies tries to stay on their network as along as plausible, while they are on their network they try to collect as much information possible from their companies. In the year 2014 the hackers were on an undisclosed network for 205 days, until they were detected and for such cybercrime there was a huge loss of almost $7.7M. These groups who has the control of the networks of major companies tries to use all the collected information to make lumpsum money. There are certain group of people who asks for ransom by blackmailing the owners of the companies. One of the prominent examples is that there is a forum which is famously known as the 'TamilRockers', this forum is maintained by group of people throughout the world. The ideology of this forum is to release movies in the net before its actual release date. They blackmail the film industry people to extort money and threatens them that they would release the movie beforehand. The companies shall invest ample amount of time and money for strengthening their cybersecurity, it is one of the emerging issues where companies focusing on expansion and development often loses a whole lot of their capital because of the cyber breaches. At present the environment of companies is at high threat it is the duty of all the companies to protect their sensitive, confidential and personal information, there shall be an implementation of cyber security programs in order to decrease the vulnerability of the companies. Cyber threat intelligence is one the basic necessity for all the multinational companies.

CYBER DETERRENCESS

Taking a look at the criminal aspect of cybercrimes the most common question which arises is the variance between the conceptual and practical applicability of the cyber assault. On questioning about the cyber deterrence few theories have proved it to be difficult. Moreover, the cyber-attacks are said to be over exaggerated than it actually is, as the applicability is more complicated than it seems to be in the theories[3]. Cyber space has become one of the most evolving crimes, as it has created many conflicts between countries. Cyber-crime has the ability to destroy a country's economy. For instance, in 2008, Georgia underwent cyber-attack campaign, as a result of this a war erupted between Georgia and Russia[4], similarly in countries such as the United States, South Korea and North Korea cybercrime prevailed. "Cyberwar" has lured the attention of scholars over the subject of conflict in cyber space,

[2] Earl D. Matthews, Harold J. Arata III and Brian L. Hale, *Cyber Situational Awareness*, vol.1 JSTOR 35, pp.35-46(2016) https://www.jstor.org/stable/10.2307/26267298?seq=1&cid=pdf-

[3] Will Goodman *Cyber Deterrence: Tougher in Theory than in Practice?* vol.4 JSTOR 102, pp.102-135(2010) https://www.jstor.org/stable/10.2307/26269789

[4] Matthew Crosston, *Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game*, vol.6 JSTOR 100, pp.100-118(2012) https://www.jstor.org/stable/10.2307/26269789

this created anxiousness in the minds of the theorists on how to defend cyber-attack in the upcoming years. The outcome of this was deterrence, it has become one of the feasible ways to address cybercrime issues. It is said to be that deterrence is the most inexpensive alternative to curb cybercrime. Cyber-attack in a country destroyed many factors especially when such attack directly affects the economy of the country. Over the past few decades there has been many issues between two countries which has escalated solely due to cyber-attacks, as cyber space being a new and emerging concept, resolving a dispute of such nature of crimes do not have many options, cyber deterrence supposedly being one of the reliable method by which such crimes can be minimized. The theory behind this concept has been influenced from the deterrence theory under criminology. Hence, every state should have the resources to protect their data from cyberattacks.

THE BLAMELESS FALLING VICTIMS OF CYBER CRIME

Women is the most unsafe individual in this world. In every sector we have enacted various laws just to protect the safety of women. With special reference to cyber-crime women often fall prey to the online predators. The most common crime done by most of the molesters in today's scenario is 'stalking' a woman[5]. Almost most of the human in this planet has access to the internet, they learn positives as well as negatives, often to take revenge they tend to use all sorts of illegal activities with the knowledge they acquire from the internet. Stalking is one of the most common illegal acts happening against women, this illegal activity is not just done to intimidate her but also to mentally torcher, harass and sexually abuse her. Every single woman is connected with some social blogging sites, all women have the right to be socially active in the society but unknowingly they publicize their personal information to this ruthless society. Internet is more or less an online library which contains plenty of information which can be used legally as well as illegally. In today's growing world it is not a difficult task to learn about hacking the devices people often use it for various purposes, yet again women fall inside the trap of getting hacked. In India the dignity of women is considered to be more valuable than her life. If a person with an illegal intention hacks into a woman's social as well as personal life, such hacking leads to gathering sensitive information or data about the woman. In certain cases, they hack into their mobile phone and gets access to her camera, trying to record her personal movements and snaps nude pictures. They use all the information either to forcefully satisfy their sexual desires and also blackmails them for money. In some instance, as discussed above the people who hack into the system and collect inside information of women uses her picture to create an obscene image and circulates it in the internet, this is commonly known as 'Morphing'. Some people do this out of vindictiveness. They also try to spread all the sensitive information online for instance, they upload her social IDs, personal phone number with a note that "I am available for sexual needs". There are groups of people who hack

[5] Saumya Uma, *Outlawing Cyber Crime Against Women in India*, vol.6 Manupatra 103, pp.103-116(2017), http://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf

into the social lives of others just for minting money, it is known as spoofing or impersonation. The fundamental ideology behind this hacking is to use the social identity and contact the nearest or the dearest one and convince them that either they have won a lottery or there is some kind of emergency for which money is required. When we come across such messages, we blindly believe them and immediately do all those things they have demanded or requested without an iota of doubt. We generally speak about the crime against women, but there is also a part of society which commits crime against girl child. Looking inside the world of cybercrime even a naïve young girl is not left to be at peace, one of the serious and heinous nature of crime is child pornography. The society has reached to its highest saturation point where they have crossed the very limit of committing crime. Sexually abusing a child gives her severe pain and a mental trauma but still she is clueless of what's happening to her and the worst part is they video tape absurd activity and post it online.

CYBER GAMING A LIFE THREATENER

The most common and well-known cyber game up to date is 'PLAYERS UNKNOWN BATTLE GROUND'(PUBG)[6], it is a gaming application which is an internet-based gaming module. The basic outline of this game is shooting and killing the enemies. In India this game has enormously reached every nook and corner, even though the age restriction of this game is 17 years and above yet mostly school students are noticed playing this game. The psychological aspect of this game makes the player to get addicted and it also creates hatred toward the people who intrudes them while playing. In recent times a 16-year-old boy named Furqan Qureshi[7] died due to cardiac arrest because of the constant playing of this game for 6 hours straight. The doctors have mentioned that during the young age we tend to develop some kind of syndrome which make is difficult to come out of it and hence it causes an increase in the heart rate which leads of cardiac arrest. Many weak-minded teenagers in India became a victim of the 'suicide game' which was famously known Blue Whale Challenge. As per this game there will be a total of 50 tasks which has to be completed with the prescribed time in which some of the tasks were like piercing the figure of a whale on their forearms, waking up in the middle of the night to watch a horror movie etc., the final task of this game will be to kill yourself[8]. This game created a major fuss in the Indian society as there were many suicides. In the year 2016 a 21-year-old Russian was found guilty of being the creator of this deadly game. In the statement made by that person, he said that he was trying to cleanse the society, where in the beginning he felt it was wrong but, in the end, he thought he was doing the right thing. With reference to the above-mentioned game

[6] Amritanshu Mukherjee, *PUBG Mobile: What is it, is it Affecting Students and why have Gujarat, Vit and Other Institutions Banned it*, India Today(Feb.2, 2020, 2pm), http://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf

[7] Salil Mekaad, *MP:Boy Playing PUBG Dies of Heart Attack in Meemuch*, Times Of India(Jan.29, 2020, 10am.), https://timesofindia.indiatimes.com/city/indore/mp-boy-playing-pubg-dies-of-heart-attack-in-neemuch/articleshow/69577299.cms

[8] Ant Adeane, *Blue Whale: What is the Truth Behind an Online 'Suicide challenge'*, BBC News (Feb.2, 2020, 5pm), http://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf

there was yet another similar type of game called as the 'Momo Challenge' or 'Suicide Challenge'[9]. A UK base company found and declared that this game was a hoax. This shows that even though the man behind the suicide game was arrested still the concept is alive therefore, it is easy to kill a person who does criminal activities but it is difficult to kill his ideas.

THE DARKER SIDE OF INTERNET

We all are familiar with the concept of internet but very few are aware of the parallel world which exists and it is known as Dark-Web. Internet is accessible by every commoner right from the younger age to old age. Internet is said to be the 'upper layer' or 'surface web', it is a normal search engine where the ingress is straight forward and simpler, whereas the dark web is said to be the 'deeper layer' where the contents cannot be searched through normal search engine. It can only be accessed through a specific browser which cannot be done by a common person. In the current studies it has been found that 57%[10] of the dark web is being utilized for illegitimate intentions such as terrorism, drug dealings, trafficking, pornography, counterfeiting currency etc. In order to access deep web a particular software known as TOR (the online router) or I2P (invisible internet project) has to be used. At the initial phase TOR was established by the USA Naval Research Laboratory for having an anonymous communication through the online platform. Terrorists have been utilizing the deep net since 1990s, as the normal surface layer was considered to be unsafe for obscured communication and it can be located easily[11]. As a matter of fact, the website under name of a terrorist organization is not created by that organization itself the irony is that it is created by counter terrorism agencies. Hence, the terrorists group prefer to communicate using dark web, as it is considered to be much safer field than any other source. There has been many theories and researches conducted where it was found that, apart from the illegal activities carried out in the dark web there are other activities as well, such as sending possessed items, crucial evidences of unsolved murder cases, disturbing videos etc., therefore, in today's scenario dark web is very serious and a dangerous platform where many high profiled people commit illegal activities, even by mistake if a person enters this forum it will be a life long threat.

CONCLUSION

With regard to the industrial revolution the next major revolution has been the internet. It is at most necessity to understand the concept of cybercrime, as many intellectuals commits crime with the help of internet. Every individual in this planet is connected to internet hence, the perpetrator uses personal or confidential information to conduct illegal activities. Cyber terrorism is one of the major crimes

[9] Momo Doll Avatar *Momo Challenge: What is it and how did the Hoax Begin*, The Week (Feb.3, 2020, 3pm.) http://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf

[10] Abdullah Bin Khaled Al-Saud, *The Tranquility Campaign a Beacon of Light in the Dark World Wide Web*, vol.11 JSTOR 58, pp.58-64(2017) https://www.jstor.org/stable/26297779

[11] Gabriel Weimann, *Terrorist Migration to the Dark Web*, vol.10 JSTOR 40, pp.40-44(2016) https://www.jstor.org/stable/26297596

which is a growing threat to many countries. Every country shall invest a substantial amount of time to strengthen the cyber security. In this world not every country is well developed and has a wealthy economy therefore, these countries shall adopt the concept of cyber deterrence to stand against the cybercrime. One of the common preys in most of the crimes are women, in today's scenario cybercrime against women has massively increased. On the other hand, the teenager's psychological behavior is highly affected and disturbed due to a sudden increase in cyber gaming. Due to the increase in cyber gaming many young minds have killed themselves and they do not even hesitate to kill their own family members also. We all are aware about the usage of internet but there is a parallel world to the internet and it is called as dark web or dark net, in recent time it has been found out that dark web is used for illegal activities such like terrorism, drug dealings, trafficking, pornography etc. internet has changed the way of our living, we have almost forgotten the concept of emotion. It has become complex for us to have a face to face conversation rather we stared preferring to communicate through our smart phones.