Cyber Terrorism and Cyber Warfare

Abhilasha Sharma[1]
[1]*Student, SHEDS College of Law Solan (H.P.)*

***Abstract*—Cyber is an internet related prefix used in a number of terms. An online dictionary defines 'Cyber Crime' as a 'A crime committed on a computer network'. Cybercrime is not a new topic it is simply 'old wine in a new bottle' old crime in a slightly new guise. In crime cyber terrorism and the cyber warfare is common concept which is faced by world as a whole. Cyber terrorism consists of using computer technology to engage in terrorism. Since 'crime' and 'terrorism' are similar in certain respect and since both targeted society's ability to maintain internal order.**

Basically, crime is 'personal' while terrorism is 'political'. Cyber warfare is a cyber-attack launched against a country or state with the aim of gaining a strategic or military advantage. Cyber warfare can include attack on civil infrastructure, financial institution, military facilities and individual citizen. Cyber terrorism has become a critical concern due to dependency on networked communication.

***Index Terms*—Cybercrime, Cyber terrorism, Cyber warfare, Network communication**

I. INTRODUCTION

We live in the digital era which is one of the reasons of our smartness. Because today we have lots of sources for gaining knowledge and prove yourself best in the society. We are so fortunate for it. But we are also totally dependent upon the technology. As we know a coin consist of two aspects. And also, everybody has their two aspect i.e., positive and negative. Now the question about our technology? So yes, where our technology is so helpful for us as well as it creates a fear of an end of everything. In which cybercrime plays a vital role. Cybercrime is computer-based crime where a person steals your information, your bank details, destroy software etc. Now I would like discuss about Cyber terrorism and Cyber warfare which is the part of cybercrime. It doesn't affect an individual even it destroys the whole nation.

II. HISTORICAL BACKGROUND

Cybercrime is one of the largest and globally most active forms of crime. After all, the internet is available and visible to everyone, and that of course involves risks. Committing a crime via a computer or other device that is connected to the Internet is dangerous because the identity of the perpetrator is difficult to find out. Cybercrime occurs in various forms and always continues to develop. Security software companies are therefore constantly looking for ways to better protect people. Always being on the alert and using security software or a VPN service are essential to protect yourself against cyber criminals. In addition, these security measures should make surfing the internet not only safer, but also more enjoyable.

A. Hacking in the 80's

Actually, there was no real cybercrime until the 1980s. One person hacked another person's computer to find, copy or manipulate personal data and information. The first person to be found guilty of cybercrime was Ian Murphy, also known as Captain Zap, and that happened in the year 1981. He had hacked the American telephone company to manipulate its internal clock, so that could still make free calls at peak times. Hackers, however, proceeded in different ways over time. Although telephone companies were the very first target, banks, web shops and even private individuals quickly followed suit. Nowadays, online banking is very popular, and that also carries a big risk. For example, hackers can copy log-in codes and names, or retrieve passwords from credit cards and bank accounts. The result is that one can just empty accounts or make purchases online with someone else's account.[1]

[1] https://goosevpn.com/blog/origin-cybercrime

III. PARTIES INVOLVED[2]

- Cyber Terrorists

Cyber terrorists are state-sponsored and non-state actors who use cyberattacks to achieve their objectives. Actors such as transnational terrorist organizations, insurgents and jihadists have used the internet for planning attacks, radicalization and recruitment, propaganda distribution, a means of communication and for disruptive purposes.

- Cyber Spies

Cyber spies steal classified or proprietary information from governments or private corporations to gain a strategic, security, financial or political advantage. They often take directions from foreign government entities and target government networks, cleared defense contractors and private companies.

- Cyber Thieves

Cyber thieves engage in illegal cyberattacks for monetary gain. An example is an organization or individual who accesses a system to steal and sell credit card numbers.

- Cyber Warriors

Cyber warriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks to support a country's strategic objectives. Entities may or may not be acting on behalf of the government in terms of the target, timing of the attack and type(s) of cyberattack — and they are often blamed by the host country when accusations result from the attacked nation.

- Cyber Activists

Cyber activists perform cyberattacks for pleasure or philosophical, political or other nonmonetary reasons. Examples include an individual who hacks a system for a personal challenge or a "hacktivist" like a member of the cyber-group Anonymous.

IV. CYBER TERRORISM

Cyber terrorism (also known as digital terrorism) is defined as disruptive attacks by recognized terrorist organizations against computer systems with the intent of generating alarm, panic, or the physical disruption of the information system. Cyber terrorism can be also defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives. Experienced cyber terrorists, who are very skilled in terms of hacking can cause massive damage to government systems and might leave a country in fear of further attacks. The objectives of such terrorists may be political or ideological since this can be considered a form of terror. While we've become used to hearing about cyber-attacks, cyber terrorism instills a different type of worry. Computer hackers have long worked to gain access to classified information for financial gain, meaning terrorists could do the same. The more mainstream idea of cyber terrorism is the hacking of government or private servers to access sensitive information or even siphon funds for use in terror activities.

A. New Perspectives for cyber terrorism[3]

Cyber Terrorism requires some new perspectives. The following concepts must be considered in order to fully understand cyber terrorism threats:

1. The motivations behind a cyber terrorist may be the same as any other type of terrorists att[4]ack. Cyber Terrorism is another tool, as are explosive and automatic weapons.
2. Cyber Terrorism can require technical expertise that exists outside the realm of a terrorist organization. Frequently, a system cracker may be hired to execute the cyber terrorism act. This may be a professional looking for money.
3. Like many terrorist attacks there may not be warning. However, with Cyber Terrorism one may not even know that the act has taken place until sometimes after the attack. Attack on computer systems can go unnoticed.
4. Cyber Terrorism requires only an inexpensive personal computer, modem, phone line, and software tools-tools which are available free and in multiple locations on the Internet. Tracing a terrorist's equipment or even his activities are complex and frequently near impossible to accomplish in real time.
5. Intelligence gathering on Cyber Terrorism is difficult. Tradecraft and Intel gathering is complicated by virtual meetings, drops sites, encryption.

[2] https://online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/

[3] Law & emerging technology Cyber Law

[4] en.m.wikipidia.org

V. EXAMPLES

As an example, one can hack into the computer network of a Bank and leave an encrypted threatening message for senior directors saying that if they do not pay desired amount of money they would use anything from logic bombs to high emission radio frequency guns to destroy the Bank's files stored in their computers. Most of the Banks would rather pay the money than letting the public know how vulnerable they are.

Another example of cyber-terrorism could be hacking into a hospital computer system and changing the patient's medicine prescription to a lethal dose as an act of a revenge. There are many such examples of cyber terrorism in its many forms.[5]

Zeran v. America on Line,[6]

The outlined the reason of such immunity by saying that congress recognized the internet and interactive computer services as offering a forum for a true diversity of political discourse, unique opportunities for cultural development and myriad avenues for intellectual activity.

VI. MOST NOTORIOUS CYBER ATACKS [7]

A. The 2014 Yahoo Attack:

In 2014, Yahoo became the victim of one of the biggest data breaches in history. Approximately 500 million accounts were hacked by a state-sponsored actor. The theft was the biggest known cyber breach recorded at the time, and criminals were said to have stolen everything from names and email addresses to telephone numbers, passwords, and date of birth details. Although the attack officially took place in 2004, Yahoo only discovered the incursion after later reports were filed relating to a secondary breach.

B. Adobe Cyber Attack:

In 2013, Adobe, one of the world's leading software developers, confirmed a cyber-attack had compromised around 38 million accounts among active users. Originally, the firm had believed around 2.9 million accounts had been affected. Adobe further announced the hackers had stolen parts of the source code of Photoshop, its picture-editing technology.

Following news about the attack, a spokeswoman for Adobe revealed the initial statement made by the brand did not reveal the full scale of the problem. Adobe was fined over $1 million in a multi-state suite over the breach. What's more, the reputation of the company was significantly damaged.

C. The Nasa Cyber Attack:

Another major cyber security event to take place in 1999, the NASA cyber-attack involved the breach and subsequent shutdown of NASA's crucial computers for around 21 days. Around 1.7 million pieces of software were also downloaded during the attack, which cost the space company around $41,000 on repairs. What made this attack so famous wasn't the expense associated with the crime, but the criminal responsible for the action. Soon after the attack took place, a fifteen-year-old computer hacker pleaded guilty to the issue and was sentenced to six months in jail. As part of his sentence, the boy was required to write letters of apology to both the NASA administrators and the secretary of defense.

VII. CYBER WARFARE

The Internet has created the biggest threat of being exposed to the cyber warfare also known as information warfare. The weapons used in this warfare are simple, a personal computer, a keyboard, a mouse and an Internet connection. Cyber war can be against a nation, a corporate house or an individual. At level the attacker may be engaging in this warfare for the financial gains, mischief blackmail or for some other darker motives.

The target of warfare at the corporate level is business through the information stored on the corporate computer system, essential to perform daily operations pertaining to the image reputation of the company. It involves theft of secrets from a company and releasing the secrets, or even falsified secrets, that can damage the company in such a way that its survival is at stake. India has also been a victim of the cyber war from across the borders and the cyber-space has become another flashpoint after Kashmir

[5] Law & emerging technology Cyber Law

[6] 129 f.3d 327

[7] https://em360tech.com/top-10/top-10-most-notorious-cyber-attacks-history

During December, 2000, a notorious group of hackers, called G-Force Pakistan, hacked a site Zeetv.com and posted a message on Kashmir as well as derogatory remarks on Indian Army and Indian Government. G-Force has also hacked to sites of Indian Science Congress Asian Age newspaper. National Research Centre, Agricultural University of Maharashtra, Indian Institute of Management, Ahmadabad, the Gujarat Government, Centre for Electronics Design and Technology, Indian Institute of Technology. Madras, among several others.[8]

VIII. MOST NOTORIOUS CYBERWARFARE:[9]

1. Robert Tappan Morris—The Morris Worm (1988):

Robert Tappan Morris made the first internet computer worm in history. He was a student at Cornell University. Although Mr. Morris claimed he did it to explore the size of the cyber space, it soon evolved into a virus that caused between $10 million and $100 million in damage repair costs.

2. Google China Attack (2009)

In 2009, in an act of cyber espionage, hackers were able to get inside Google's servers and access Gmail accounts belonging to Chinese human rights activists. Upon further investigation, authorities discovered that many Gmail accounts of people in different countries had been penetrated.

3. A Teenager Hacks the US Defense Department and NASA (1999):

A 15-year-old named Jonathan James was able to get inside the U.S. Department of Defense's (DOD) computers and install a backdoor within its servers. He then used the backdoor to intercept internal emails, some of which had usernames and passwords inside. James then used his access to the DOD's system to steal NASA software used to support the International Space Station.

4. Hacking a Radio Phone System to Win a Porsche (1995):

A man named Kevin Poulsen heard of a radio station contest where you could win a sports car. He ended up winning a Porsche 944 S2 by being the 102nd caller. He accomplished this feat by hacking the phone system, locking out other callers, ensuring his victory. He ended up getting sentenced to five years in prison.

IX. LEGISLATIVE STEPS AGAINST CYBER TERORISM AND WARFARE IN INDIA

- Information Technology Act:

The Section 66F of the Information Technology Act addresses cyber terrorism. It was added in 2008 with various changes. These changes are the result of the well-known 26/11 terror attack. This tragedy is a memorable example of cyber network misuse. Terrorists used communication services in this case, resulting in more shooting attacks and casualties. Individuals who engage in C terrorism-related cybercrime must face appropriate punishment[10].

- Dark Blocking Access to Information:

Section 69A of the Information Technology Act, 2000 allows the Central Government or any of its officers specially authorized by it in this behalf to block any content online "in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offense relating to above." The intermediary who fails to comply with the direction issued shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.[11]

- Cyber Security Policy 2013:

The Government of India enacted the National Cyber Security Policy on July 2, 2013. Its guiding principle was to "protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation."

[8] Law and emerging technology cyber law book

[9] https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare

[10] IT ACT 2000

[11] IT ACT 2000

X. PUPNISHMENT FOR CYBER TERRORISM [SEC66F] (2)

Whoever commits of conspires to commit cyber terrorism must be punished with imprisonment which may extend to imprisonment for life.

XI. JUDICIAL OPINION

- The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time, the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

- Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 cr. cash was recovered from house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days. The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax.

- Bazee.com

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cybercrime cases and a lot of education is required.[12]

XII. CONCLUSION

As we have seen cybercrime is a serious threat to our society and it is essential to take steps to protect ourselves and our organization. Cyber-attacks can come in the form of viruses, malware, email phishing; social media fraud. The spectrum of cyber threats is limitless. We should take actions to protect ourselves such as enable multi-factor authentication, create a strong password, if you are unsure of who an email is from do not respond and click it, disconnect your devices when you are away from it. Cyber terrorism and cyber warfare are serious issues in today`s digital world. In a nutshell, cyber terrorism involves using digital tools to carry out attacks that can have serious consequences on national security and society. And cyber warfare is like a digital battlefield where countries or groups use cyber-attacks to disrupt or damage each other`s computer system and networks. Federal Bureau of Investigation (FBI) plays a crucial role in dealing with cyber terrorism and warfare. They work alongside other agencies to investigate and counter cyber threats, gather intelligence, and collaborate with international partners to enhance cyber security measures. FBI contributes significantly to safeguarding against cyber-attacks and protecting national security.

[12] Delhidistrictcourts.nic.in