Special Issue
"(Global Partnership: India's Collaboration Initiatives for Economic and Social Growth)"

Cyber-crime: a threat to national security

Babita Rani Srivastava
Researcher, Department of Economics, M. J. P. Rohilkhand University, Bareilly, Uttar Pradesh, India
Correspondence Author: Babita Rani Srivastava

Abstract
The evolution of technology, particularly the advent of the internet, has brought about a new era of crime known as cybercrime. This paper explores the various forms of cybercrime, including hacking, virus dissemination, identity theft, phishing, and more. Cybercrime poses a significant threat to national security, as it can disrupt essential services, compromise sensitive information, and facilitate terrorist activities. Despite efforts to combat cybercrime, its perpetrators often remain elusive due to the complexities of cyberspace. This paper emphasizes the importance of raising awareness, strengthening legislation, and enhancing cybersecurity measures to safeguard against cyber threats. Failure to address cybercrime could have dire consequences for global security and economic stability.

Keywords: cybercrime, national security, hacking, virus dissemination, identity theft, phishing, cybersecurity, terrorism, legislation, internet privacy

Introduction

When Blaise Pascal built the first non-electronic computer in 1642, little did he know that centuries later the descendants of this innovation would change the way we live and rewrite legal lexicons. These electronic behemoths became a substitute for human brains. In 1969, the birth of the internet multiplied the power of this wonder machine, and the world was never the same again. New crimes appeared, old crimes disappeared, and what counts as a crime varied across societies.

Cybercrime combines the term "crime" with the root "cyber" from the word "cybernetic," derived from the Greek word "kubernan," which means to lead or govern. The cyber environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "computer crime" to encompass crimes committed using the internet, all digital crimes, and crimes involving telecommunications networks.

Definition of cyber crime

Cybercrime, also known as computer-oriented crime, involves criminal activities that utilize computers and networks. It encompasses a broad spectrum of illicit activities where computers or computer networks serve as either the instrument, target, or site of criminal operations. These delineations are not rigidly exclusive, as many activities can straddle multiple categories. Examples of cybercrime include identity theft, internet fraud, copyright infringement via file sharing, hacking, dissemination of computer viruses, perpetration of denial-of-service attacks, and spamming.

According to Search Security, cybercrime is defined as "any unlawful activity that primarily relies on a computer for its execution." The U.S. Department of Justice extends this definition to encompass any illegal activity that utilizes a computer for the storage of incriminating evidence.

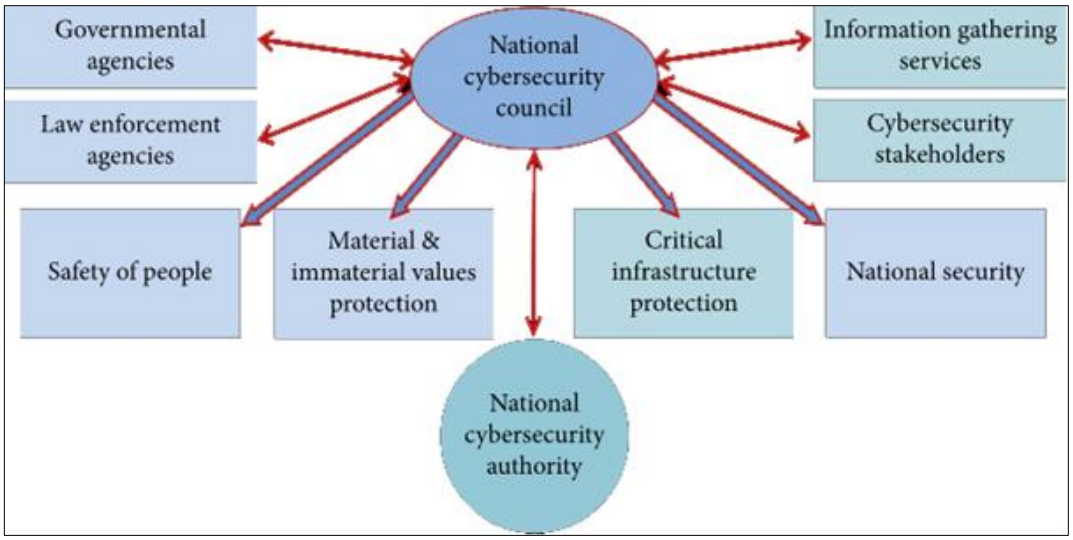
Types of cyber crime

1. Hacking

Hacking constitutes an endeavor to exploit a computer system or penetrate a private network housed within a computer. In essence, it entails unauthorized access to or manipulation of computer network security systems for nefarious intents. Put plainly, hacking denotes an act carried out by an intruder who gains entry into your computer system without your explicit authorization.

2. Virus dissemination

Viruses are software programs that attach themselves to or infect systems or files, often spreading to other computers on a network. They disrupt computer operations and compromise stored data by either modifying or deleting it entirely. In contrast, "worms" do not require a host to propagate; they replicate autonomously until they consume all accessible memory within the system.



Source: Google net

Fig 1

3. Identity theft and credit card fraud

Identity theft happens when an individual acquires your personal details, such as credit card information or Social Security number, with the intention of perpetrating fraud or engaging in other illicit activities. They assume your identity to gain access to resources like credit cards, bank accounts, and other privileges in your name. Moreover, the impostor might exploit your identity to commit additional offenses. "Credit card fraud" is a broad term encompassing crimes associated with identity theft, wherein the perpetrator employs your credit card to finance their transactions.

4. Logic bombs

A logic bomb, also known as “slag code.” Is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event? It’s not a virus, although it usually behaves in similar manner. Malicious Software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known ass ‘time-bombs”. The majority of logic bombs typically remain confined to the network where they were deployed, implying that they are predominantly an insider's undertaking. Consequently, they are often easier to devise and implement compared to viruses.

5. Phishing

Phishing refers to the deceptive practices employed by malicious individuals or groups aimed at scamming users. They achieve this by sending emails or creating web pages designed to deceive individuals into divulging their online banking, credit card, or other login credentials. These emails and web pages are crafted to mimic legitimate companies, thereby gaining users' trust and coaxing them to enter personal information. Phishing is essentially a scam wherein email users are tricked into revealing personal or confidential information that scammers can exploit illicitly. It involves extracting confidential data such as credit card numbers and username-password combinations by posing as a legitimate entity. Phishing is typically executed through email spoofing.

6. Email bombing and spamming

Email bombing entails an abuser sending massive volumes of emails to a target address, leading to the victim's email account or mail servers crashing. These messages are typically nonsensical and excessively long to consume network resources. If multiple accounts of a mail server are targeted, it can result in a denial-of-service impact. Such bombardment of emails can be easily detected by spam filters. Email bombing is commonly executed using botnets (private internet-connected computers compromised by malware and under the attacker’s control) as a Distributed Denial of Service attack.

7. Web jacking

Web jacking, derived from 'hijacking,' involves a hacker fraudulently seizing control of a website. The hacker may alter the site's content or redirect users to another fake page under their control. Once hijacked, the original website owner loses control, allowing the attacker to exploit the website for personal gain. Instances have been reported where attackers demanded ransom or posted obscene content on the site. In some cases, web jacking is used to create a clone of the website, with the victim presented a new link claiming the site has moved. Unlike typical phishing methods, hovering over the link may display the original URL, but upon clicking, the user is directed to the malicious server. The address bar might display a slightly altered URL, tricking users into believing it's a legitimate site.

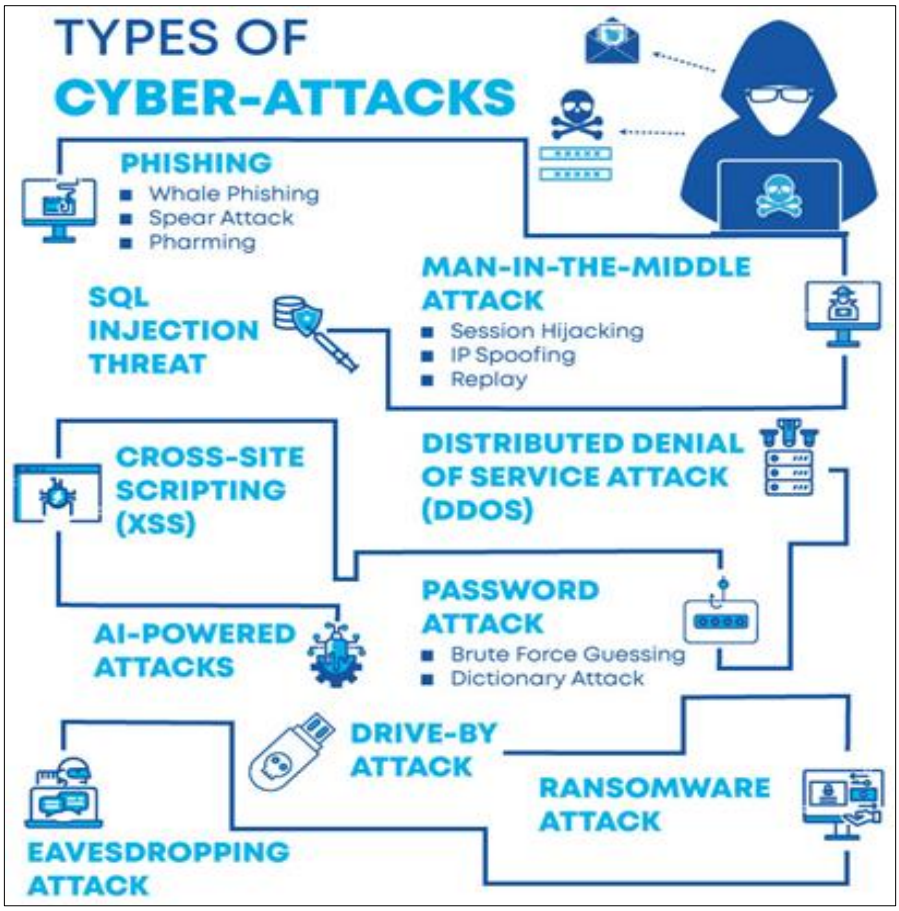


Fig 2

8. Cyber stalking

Cyberstalking is a new form of internet crime in our society, where a person is pursued or followed online. A cyber stalker doesn't physically follow their victim; they do it virtually by monitoring their online activity to harvest information about the target and harass them, often making threats using verbal intimidation. It's an invasion of one's online privacy. Cyberstalking uses the internet or any other electronic means and is different from offline stalking, but it is usually accompanied by it. Most victims of this crime are women stalked by men, and children stalked by adult predators and pedophiles. Cyber stalkers prey on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know.

9. Data diddling

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and it difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

10. Software piracy

Internet piracy is an integral part of our lives, to which knowingly or unknowingly, we all contribute. In this manner, the profits of the resource developers are being significantly reduced. It's not only about illegally using someone else's intellectual property but also about sharing it with friends, further diminishing the revenue they rightfully deserve. Software piracy involves the unauthorized use and distribution of computer software. Software developers invest significant effort into developing these programs, and piracy severely impacts their ability to generate sufficient revenue to sustain application development. This has repercussions for the global economy, as funds are diverted from other sectors, resulting in reduced investment in marketing and research.

Effects of cyber crimes on national security

Cybercrime is a threat to national security which may be defined as 'The premediated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives'. Cyber Crime is a global phenomenon and, therefore, the initiative to fight it should come from the same level. Today cyber and organized crime has become the order of the day round the globe and the need to put an end to this criminal act cannot be kept aside. Research has shown that people lose millions of dollars daily to cyber criminals and we cannot continue to live with this set of people because they are enemies of progress of the nation. All efforts to put this to an end have proved unsuccessful why? Because the people fighting the crime are criminals.

The human mind's capacity is truly vast and complex. While it may not be feasible to entirely eradicate cybercrime from the digital realm, it remains within our means to mitigate its impact

on national security. Throughout history, no legislation has proven completely successful in eradicating crime worldwide. However, what is achievable is raising awareness among individuals about their rights and responsibilities, including the duty to report crimes as a collective obligation to society. Furthermore, enhancing the enforcement of laws can significantly curb criminal activities. Therefore, there is a pressing need to amend the Information Technology Act to bolster its effectiveness in combating cybercrime.

Technology is a boon but it also has dangerous implications if left undetected. Cyberspace is one such area that needs to pull all security strings together before things go out of hand. There is huge potential for damage to national security through cyber-attacks.

Conclusion

With the continuous advancement of technology, a concerning nexus between hackers and terrorists is emerging. It is foreseeable that terrorists themselves may soon possess formidable hacking skills, fundamentally altering the landscape of terrorism. Safeguarding national security in India necessitates the prevention of cybercrimes. Preserving the integrity of our information, documents, policies, and strategies is paramount for our safety and progress. Cybercrime demands urgent attention as it poses a significant threat. The potential consequences of technology overtaking an entire population are alarming. The pervasive threat of organized cybercrime looms over the entire world. It is imperative that action is taken promptly to address this issue before it spirals out of control.

Reference

1. https://en.wikipedia.org/wiki/Cybercrime
2. https://www.newworldencyclopedia.org/entry/Cybercrime
3. https://searchsecurity.techtarget.com/definiton/cybercrime
4. Kapender Sing. “Cyber threat is Global perpective” Gaurave book pvt. Ltd., Ansari road, Daryaganj, Delhi, p3.
5. https://study.com/academy/lession/what-is-cyber-terrorism-definition-case-example.html.
6. https://www.techopedia.com/definition/6712/cyberterrorism
7. https://economictimess.indiatimes.com/definition/hacking
8. https:www.digit.in/technology-guides/fastrack-to-cyber-crime/the-12-types-of-crime.html
9. ibid
10. https://guides.wsj.com/personal-finance/credit/how-to-protect-yourself-from-identity-theft
11. https//:www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html
12. https://www.computerhope.com/jargon/p/phishing.html
13. https://ww.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html
14. Pratiyogita Darpan, 2008 June, p2222.
15. http://www.merinews.com/article/cybercrime-a-threat-to-national-security/126460.shtml.