The Issue of Cybersecurity in Today's Digitally Empower Society in the light of Digital India Mission

Biswajit Samaddar, W.B.E.S.
Assistant Professor
Government College of Education, Banipur
West Bengal, India.

Abstract:

Now we are in the era of the fourth industrial revolution, which has the potential to change social structure with the ability to improve the standard of living for citizens around the globe. Today's digital innovation and related services enhance the efficiency and pleasure of people's personal life. Billions of people are connected by one smartphone, which can easily be in the pocket with unprecedented processing power, storage capacity and almost unlimited access to knowledge. The present times are witnesses that the people are simply drifting away with digital innovation from the time they get up in the morning to go back to sleep at night. This attachment makes available increasing amounts of data about the people which raises questions about their privacy, security and identity. As a result, the protection of personal data and privacy is becoming a serious issue today in front of the people. It is true that life is not easy without technology today and people are comfortable interacting in cyberspace, but the question is how many people are aware about the cyber safety and security related safeguard. This study focuses on why cyber security is a concerning issue today along with its various dimensions that impact people's lives. In the year 1970, cybercrime was introduced and today it is recognized as a global problem. But it is not right to think like, cyber threats & the disruption that comes with it, is an exogenous force over which people have no control. Important factor is our awareness is our protection, so be aware and be safe, the study also provides the possibilities to prevent cyberthreats.

Keywords: Empowerment, Unlawful Action, Citizen Security & Possibilities.

Introduction:

Technology in the present times has witnessed a remarkable evolution to become a need rather than an option. This has transformed our lives and for most of us, life may not be that easy without technologies. Technology has permeated our lives immensely. People are simply interacting with technology from the time they get up in the morning till the time they go back to sleep at night. Information communication technology has become an integral part of life, impacting most aspects of people's day to day life. At present the new generation is getting exposure to cyberspace at a very early stage through the smart phones. It is not rarely found that they spend their time on various social networking sites to play games, make friends, interact with their friends, share updates and shopping or financial transactions etc. As digital technology increasingly becomes a part of every aspect of our lives, the importance of cyber security cannot be understated. The cyberspace connects people virtually with millions of online users from across our mother earth. The significant issue is with increasing use of cyberspace, cyber threats are also increasing rapidly. Sometimes people are tarnishing emotionally, psychologically and socially.

Objectives:

The purpose of this study is to provide an insight why cyber security is a concerning issue at present. To highlight various types of cyber threats and its impact on citizens today's life. To indicate safeguards in preventing cybercrimes. And to empower people to be responsible and careful cyber citizens for their safe future.

Digital Society and Citizen Security:

Our society refers to a group of people living together in a community with common traditions and interests. Society plays a vital role in shaping the lives of individuals and providing a framework for their interactions, beliefs and behaviours. At present time the society in which people live has already started to alter by digital technology. Technological transformation affecting all aspects of people's lives. Innovations are reshaping our society with a scale and speed like never before. Today in daily life digital technologies like computers, the internet, smart phones and cloud computing are widely used and adopted. The people are more connected than ever before.

In July 2015, the Government of India took remarkable initiatives to launch the 'Digital India' mission to improve online infrastructure and increase internet accessibility among citizens, thereby empowering the country to become more digitally advanced. Digital India is a flagship programme of the Indian government with a vision to transform India into a digitally empowered society and knowledge economy. The key objectives of the mission are to establish a secure and stable digital infrastructure, deliver digital services and ensure that every citizen has access to the Internet. The Government has taken up many initiatives under the Digital India campaign such as, DigiLockers – this flagship initiative aims at 'Digital Empowerment' of the citizen by providing access to authentic digital documents to citizen's digital document wallet. BHIM – Bharat Interface for Money is an app that makes payment transactions simple, easy and quick using Unified Payments Interface (UPI). The e-Kranti - National e-Governance Plan (NeGP) is also an integral part of the Digital India Programme, aimed at transforming the delivery of all government services electronically to the citizens.

Table 1: **Trend of Internet service use by the people (in million)**

Continent wise	Over the Years		
	2001	2011	2021
World	**503.74**	**2220**	**5020**
Asia	149.93	1070	2750
Europe	136.09	482.69	654.93
Africa	6.19	115.69	553.21
North America	168.07	309.95	502.54
South America	19.97	171.59	317.74
Oceania	12.46	22.36	34.74

Source: https://ourworldindata.org/internet.

Followed by the Table No. 1 the widespread adoption of the internet service, mobile devices and digital platforms, which provides virtually endless possibilities to the people. But parallelly citizen's personal digital footprint makes available increasing amounts of data about themselves which raises questions about their

privacy, security and identity. This serious issue over the protection of personal data and privacy comes today in front of the people.

Cybersecurity - Concept and Concerning Issue:

The internet, computers with smart phones accessories and other social networking platforms have become an integral part of people's day to day life. Now is the time to envision how much time people are investing in their daily life on these platforms. The people have habituated to interact with others through the social networking sites i.e. WhatsApp, Twitter, Facebook, Instagram, email etc. as part and parcel of their everyday activities. But the significance matters are how many people are aware about the cyber safety and security related safeguard to protect themselves. How many people know that whatever personal information is shared on the internet stays online forever as it is extremely difficult to delete completely. Another question also raises how many people are known to use the internet responsively, ethically and respectfully. Cybersecurity is the practice of protecting computers, servers, networks, devices and sensitive data from malicious digital attacks and unauthorized access. It encompasses a comprehensive set of security measures, tools and best practices to safeguard individual users and organizations from evolving cyber threats. These cyberattacks are usually aimed at assessing, changing or destroying sensitive information and extorting money from users.

Cybercrimes & Its Various Trends:

Cybercrime involves unlawful actions executed using computers or the internet, focusing on attacking networks, stealing data or committing fraud. This includes illegal activities like unauthorized system access, identity theft and online scams. In the year 1970, Cybercrime was first recognized as illicit activities exploiting digital technologies. Cybercrime has grown up and today is recognized as a global problem. Cyber criminals use psychological manipulation, phishing and malware to exploit individuals and organizations, causing financial losses and disrupting business operations. The rise of cryptocurrencies, the dark web and sophisticated scams and the shortage of cybersecurity related knowledgeable professionals has added fuel to the fire. At present these threats are not limited to any one demographic. From unsuspecting individuals to multinationals and even governments, no one is safe. The cybercrime monster is growing and poses a threat to our security, privacy and way of life. Now cybercrime has become a social epidemic that knows no borders.

Cybercrimes are the offences that may be responsible for individuals or groups by using accessories related to digital technology such as computers, internet and smartphones. The criminals use platforms like email, chat boxes, websites, pirated software, social networking sites etc. to attack victims. Cybercrimes are becoming very sophisticated with increasingly targeted on stealing the individual's personal sensitive data such as contact numbers, pictures, social ids (Email-Instagram-Facebook-WhatsApp) etc. and this information may be used by criminals against that person. Teenagers with children are also vulnerable to the different types of cyber threats. There are various possible ways that can be used by cyber criminals to attack someone, such as:

- *Malicious Files Applications*: A malicious application refers to a software program that is designed to obstruct networking services by exploiting vulnerabilities in the control plane or by dropping packets selectively. It can bypass security mechanisms and pose a threat to the network security. In this way the

criminals are providing to the people malicious files through the gaming, messaging or email etc in order to get access to an individual's personal gadgets like smart phone or computer.

➢ *Social Engineering:* This is the process used by criminals to obtain confidence to get an individual's personal information. Social Engineering is basically the psychology of persuasion. Its targets are to gain the trust of individuals depending on what individuals like to do mostly, resulting in lowering their guard, and then encourage them into taking unsafe actions such as divulging personal information or clicking on web links or opening attachments that may be malicious.

➢ *Email Spoofing & Phishing Scams:* Email spoofing is a threat that involves sending email messages with a fake sender address that looks genuine and trusted but actually is not. In this case, the client application assigns a sender address to outgoing messages, as in fact outgoing email servers cannot identify whether the sender address is legitimate or spoofed. Spoofing involves using a fake email address to make it appear as if the message is coming from a trusted source. Phishing scams are one of the most common types of cybercrime. The information targeted in phishing attacks is broad in scale, phishing attacks pose a big threat to brand reputation. These scams involve fake emails or messages designed to trick victims into giving up personal or institutional information. Attackers send emails that appear to come from reputable sources, such as banks, social media platforms or online services. These emails often contain a sense of urgency, prompting the recipient to click on a malicious link or download an attachment. A fake email from a bank asking someone to click a link and verify the account details and resulting financial loss, may be an example of deceptive phishing scams.

➢ *Identity Theft:* Identity theft is a serious form of cybercrime. It's when cybercriminals get the personal information such as transactional data to make unauthorized transactions or enable other fraudulent activities. Cyber criminals deliberately use someone's personal stolen information for unauthorized transactions or to gain financial advantage. The effects of identity theft can be huge, some of the consequences may be highlighted as unexplained withdrawals from bank accounts, mysterious credit card charges with psychological distress etc.

➢ *Ransomware Attacks:* Ransomware attacks are a type of malicious software that exploit computer networks to encrypt victims' files and block access until a ransom is paid. This type of cybercrime can lead to data breaches where victims pay the ransom to get access back to their files or systems. Ransomware is usually distributed through phishing emails or drive-by downloading. Once inside a computer system, the malicious software spreads its arms, encrypts files and demands a ransom, often in the form of cryptocurrency, in exchange for the decryption key.

➢ *Job Frauds:* Hiring Scams occur when criminal actors deceive victims into believing they have a job. Scammers post fake jobs advertisements on online platforms and sometimes make the ads look like they're from real companies. Criminals leverage their position as employers to persuade victims to provide them with personally identifiable information or ask to pay to get a job.

➢ *Cyber Bullying:* Cyber bullying is one of the usual crimes being faced by children and youth at present. Though it can affect anyone yet due to limited knowledge towards cyber threats, therefore children become easy victims through this process. The example of cyberbullying may be indicated as sending, posting

or sharing negative-rude messages, harmful videos or false images to intentionally harass someone and causing embarrassment or humiliation. Cyber bullies can be a known person like a friend, relative or even an unknown person to whom the victims met regularly through online platforms.

➢ *Cyber Grooming:* This type is growing as one of the major threats also faced by children and adolescence. In this process where someone develops an emotional bonding with children through social networking platforms with the aim of getting their trust for sexually abusing or exploiting them. Cyber groomers can use fake accounts and initially provide compliments, gifts or modelling job offers but later they can start sending obscene messages, pictures or clips and will ask to share teenagers sexually explicit photos/clipping with them. The online groomer generally targets teenagers as in adolescence they face immense personal, biological changes. The impulsive and curious characteristic of adolescents encourages them to engage in such types of online activities which makes them easily vulnerable to online grooming.

➢ *Emerging Cybercrime Trends:* Significantly, the above-mentioned all forms related to the cybercrimes though which are not exhaustive, but it covers the main types of cybercrime. Cybercriminals adapt to technology, they are using emerging technologies like cryptocurrency and blockchain to steal funds or money laundering from exchanges, wallets and smart contracts. Now phishing attacks have also gotten more sophisticated with cybercriminals using real-world events like tax season and shopping promotions to lure victims. In the fast-paced digital world, cyber scams have become increasingly sophisticated and continue to evolve with new technologies and tactics. One of the most alarming cyber threats is the 'Digital Arrest' scam, very recently revealed in society. Unlike general cyber fraud, digital arrest scam involves criminals impersonating law enforcement officials to intimidate victims into transferring money or sharing sensitive information. In this tactic cybercriminals falsely accuse individuals of breaking the law, often claiming the existence of a digital arrest warrant. These scammers pose to the victims as officials from organizations such as police, customs, income tax or even central investigative agencies. Other emerging trends are cyber-activism, automotive hacking and the impact of artificial intelligence (AI) on cybercrimes.

Impact of Cyber Threats:

At present in the digital society, cybercrime is becoming a rising menace to the individual, group and also to any management system or organization. Makes them vulnerable to data loss, identity theft, emotional trauma and eventually hurting their reputation. Cyber threats have a deep impact on both individual's and organization's physical, emotional as well as psychological wellbeing (Table No. 2). It can not only impact teenagers' academic performance but also their daily life to a great extent. Even a single small security infringement can lead to unprotecting the private information of millions of people and brings strong harmful impacts. In some cases, this is observed that the companies face financial damage and also loss of the trust of customers. In some cases, the cost of a cyberthreats can be so severe that it instigates business shutting down. So, because of that, cyber security is very essential to protect individuals and businesses from cyber spammers and criminals. The devastating effects of cyber grooming or bullying can sometimes be long term and can even haunt the victim in their adulthood. The experience of a ransomware attack also has a significant impact on individuals' mental health and emotional wellbeing, which increases and sustains stress with anxiety.

Table 2: **Impact of Cyber threats on both individual's and organization's level.**

Cyber Harm	Physically	Psychologically	Economically	Reputationally
Individual Level	Damaged, Compromised, Exposed, Abuse, Prosecution, Pain, Loss of Life	Confusion, Frustration, Anxiety, Feeling upset/depressed, Loss of Self-confidence.	Loss of Capital, Regulatory Fines, Compensation Payments, Extortion Payments, Job Loss, Reduced Economic Strength	Shameful, Embarrassed, Face Loss, Discomfort, Loss of Acceptance
Organizational Level	Infected, Leaked, Corrupted, Reduced Performance, Theft, Destroyed	Low satisfaction, Negative Changes in Perception	Disrupted Operations, Reduced customers, Disrupted Sales, Reduced Profits & Growth, Reduced Investments, Fall in Stock Price	Reduced Goodwill, Damaged relationship with customers & Suppliers, Reduced Business Opportunities, Loss of Accreditations, Reduced credit scores

Strategic Measures to Avoid Cyber threats:

The citizen needs to be careful to protect themselves from cyber-attacks and for this purpose they should control their own behavior in a disciplined way such as – never accept friend requests from unknown persons on social networking platforms. The rule should be to add only that person online who will be known offline also. At the same time people should be restricted from sharing any personal sensitive information such as date of birth, contact number or ids. We should go to the privacy settings of social networking platforms to select who can access our posts or comments and try to restrict our own profile to known persons only. Always should be cautious when the chat friends provide many compliments regarding appearances in a short span of acquaintance. Strictly avoid communicating to people who ask you various questions related to private life like biological or sexual experience and should not share personal explicit pictures and video clips. Never install unwanted applications or software from unauthorized sources. Strictly follow to never turn on your own webcam while the chat partner does not connect to the webcam. It is also important for people, especially teenagers, to be careful about the risks associated with online gaming. Many aggressive players may be found online who can bully, sometimes they simply harass using inappropriate languages. In the initial stage the criminals may try to befriend by providing tips about the online games to obtain the trust but these techniques may compromise people's personal information. Sometimes, people are asked to share financial details for credit or debit purposes and in this way some infected online games can capture ATM/Credit card details to misuse. To keep this in mind, never share any Password/PIN/OTP/CVV code to anyone. It will be best practice to change financial codes or passwords on a regular interval and ignore unknown links. Always remember, legitimate authorities will never ask people for payments or sensitive details over the phone or social networking online platforms.

Finally, if faced with a problem in online platforms by some ones, without time lost should immediately inform the elders or guardians and narrate the entire issue clearly, so that they can support and protect primarily. Then try to identify, that person is a known or stranger and after that block him/her. It is also important to try to collect and save the messages which were used against the victim for future evidence or legal action. In this situation the role of parents is also a very important factor to support or recover the victim from the cyber

criminals and should take necessary initiatives to report or lodge a complaint to the authority concerned if feel to need to. Along with that, parents should assure the victims that you are there for them no matter what. In such a situation it may be considered as a good practice from the parents' end to never blame victims (Childs) because it may affect them very deeply, make them understand the cruciality of the practice such that they would not repeat it.

Conclusion:

The digital advancement and use of internet services recently have provided many ways to connect to others across the globe. As of 2001 more than 500 million World population was accessing internet service and after two decades in the year 2021 the volume has increased almost ten times and reached to 5020 million (Table No. 1). Today the development of highly technological societies implies the need to ensure digital security. Because, there are so many online threats in the society, and the significant issue is the threats are coming day by day in new forms. In the present situation, we often consider cybersecurity as an ongoing battle between criminals and the security experts. Significantly, the battle is escalating also due to advances in technology. Hence, the question today is 'How do we protect ourselves from the cyber threats?' and the answer is our awareness is our protection, so be aware, be safe, stay informed and never let fear dictate your own social, cultural or financial actions.

References:

[1] Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: does control over personal information, user awareness and security notices matter? *Information Technology & People*, 28(3), 426-441.

[2] Bubukayr, M. A. S., & Almaiah, M. A. (2021). Cybersecurity concerns in smart-phones and applications: A survey. *International Conference on Information Technology (ICIT) IEEE*, 725-731.

[3] Demertzis, K., & Iliadis, L. (2015). A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security. In: Daras, N., Rassias, M. (eds) Computation, Cryptography, and Network Security. Springer, 161-193. https://doi.org/10.1007/978-3-319-18275-9_7

[4] Humayun, M., Niazi, M., & Jhanjhi, N. et al. (2000). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, 45, 3171–3189.

[5] Lanning, K. (2017). The Evolution of Grooming: Concept and Term. *Journal of Interpersonal Violence*, 33(1), 5-16.

[6] Mosteanu, N. R. (2020). Artificial intelligence and cyber security–face to face with cyberattack–a maltese case of risk management approach. *Ecoforum Journal*, 9(2).

[7] Patil, P. (2016). Artificial intelligence in cybersecurity. *International journal of research in computer applications and robotics*, 4(5), 1-5.

[8] Sinrod, E. J., & Reilly, W. P. (2000). Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws. *Santa Clara High Technology Law Journal*, 16(2), 177-229.