Issues and Challenges to Cyber Security: Indian Context

Prof. Surendra Kumar

Professor, Department of Political Science,Patliputra University, Patna.

ABSTRACT

Cyber security is the practice of protecting network, computers, data, and programs from unauthorised and malicious attacks. Cyber intrusions and attacks have increased dramatically in recent years, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. Cyber security faces various challenges in today's digital era. These challenges emanate from the complex nature of cyber threats. Some of the key challenges include dealing with sophisticated cyber-attacks, insider threats, acute scarcity of cyber security professionals, lack of awareness and education, resource constraints, *etc*. As the threats have become much more sophisticated, it is essential that organizations, businesses and individuals understand the trends and risks so that they can protect themselves from cyber-attacks. With a combination of well-thought-out strategies such as network segmentation, regular patching, two-factor authentication and user education, the inherent vulnerabilities can be mitigated. With the continued efforts of the Government and the private sector, let us hope that the state of cyber security in India will continue to improve and a secure future for all the users can be ensured in the years to come.

Keywords: Network segmentation, social media, hacking, cyber warfare, two-factor authentication

Received : 11/10/2025 **Acceptance : 25/10/2025**

Introduction:

Cyber security, also known as information technology security, encompasses various domains and practices, including network security, data protection, and incident response. It plays a vital role in safeguarding sensitive information and maintaining trust in the digital eco-system. Cyber security is essential for all those who regularly and frequently use electronic devices. With so much of our sensitive data and documents stored on gadgets, it is essential to ensure their protection. There are several ways to protect devices from cyber threats such as using anti-virus and anti-malware software and implementing end user protection solutions. Taking the necessary steps to secure devices can help keep data safe and secure. Hence, the primary goal of cyber security is to prevent unauthorised or unattended access, destruction and changes to data, networks, programs and other information. Security threats and cyber-attacks have made cyber security a very important issue in the modern world.

Cyber security is a complex issue which calls for multi-dimensional, multi-layered initiatives and responses. It has proved to be a challenge for the governments because it involves various ministries and departments. It is more difficult primarily due to the diffused and varied nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators.

The rapid development of technology and the availability of the internet to most of the public broadens the pathway of cybercrime. In this age, where the use of computer has become commonplace, cyber security is a major concern. With growing internet protection, cyber security is of paramount importance for India's growth. The threat from people with malicious intent can be caused due to negligence and vulnerabilities.

The increasing use of the internet and social media has made cyber security even more important than it was before. Now, we need a more advanced security system to minimise the threat. More awareness among the masses should be there and the users should remain vigilant about protecting their data. With the rise of technology and its integration into our lives, cyber security has become an integral part of our lives, and it is important to understand different forms of cyber security threats, their challenges and the measures to combat those threats and, thus, to ensure cyber security in the country.

Threat Perception to Cyber Security:

Cyber security threats can broadly be classified into two categories *viz.,* Cybercrime and Cyber warfare (Ojha, 2020, p.32). Cybercrime implies use of cyberspace *i.e.,* computer, internet, cell phone, and other technical devices to commit a crime by an individual or organised group. Cyber attackers use numerous software and codes in cyberspace to commit cybercrime. They exploit the weaknesses in the software and hardware design through the use of malware. Hacking is a common way of piercing the defences of protected computer systems and interfering with their functioning.

Cybercrimes may occur directly *i.e.,* by targeting the computers directly by spreading computer viruses. Denial-of-Service (DOS) is another form of directly committing cybercrime (Gaurav, 2020, p. 56). It is an attempt to make a machine or network resource unavailable to its intended users. It suspends services of a host connected to the internet which may be temporary or permanent.

Another form of directly committing cybercrime is Malware (malicious code). It is a software used to disrupt computer operations, gather sensitive information or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware refers to a variety of forms of hostile or intrusive software, for example, trojan horses, rootkits, worms, adware, *etc.* Yet another way of committing cybercrime is independent of the computer network or device. It includes economic frauds. It is done to destabilise the economy of a country, attack on banking security and transaction system, extract money through fraud, acquisition of credit/debit card data, financial theft *etc.*

Other ways of committing cybercrime which are independent of the computer network or device include hindering the operations of a website or service through data alteration, data destruction, using obscene content to humiliate girls and harm their reputation, spreading pornography, threatening e-mails, assuming a fake identity, virtual impersonation, misuse of social media in creating intolerance, instigating communal violence, inciting riots, *etc.*

Cyberspace could become the theatre of warfare in 21st century(Shinde, 2021, p. 88). Future wars will not be like traditional wars which are fought on land, water or air. When any State initiates the use of internet-based invisible force as an instrument of State policy to fight against another nation, it is called cyber war. Attacking the information systems of other countries for espionage and for disrupting their critical infrastructure may be referred as cyber warfare. It includes hacking of vital information, important webpages, strategic controls and intelligence.

The attacks on the website of Estonia in 2007 and of Georgia in 2008 have been widely reported (Kant, 2019, p. 118). Although there is no clinching evidence of the involvement of a State in these attacks, it is widely held that in these attacks, non-State actors (for example, hackers) may have been used by State actors. Since these cyber-attacks, the issue of cyber warfare has assumed urgency in the global media.

Personal gain is perhaps the most common motivation for cybercrime, as it can be very lucrative. Cyber criminals may engage in activities such as identity theft, phishing scams, and credit card fraud in order to make money. Some cyber criminals commit crimes out of a desire for revenge or simply to cause havoc. They may engage in different activities such as denial of service attacks, website defacement, or event (releasing personal information online) (Relia, 2016, p. 78). In some cases, cybercrime is committed for political or ideological reasons. For example, hackers may attack a website in order to protest its content or disrupt its operations.

Challenges Confronting Cyber Security:

Cyber security faces various challenges in today's digital landscape in India. These challenges emanate from the complex nature of cyber threats and the evolving technology landscape. The dearth of skilled cybersecurity professionals continues to be a major concern. Globally, India ranks second in terms of the number of internet users after China (Prasad, 2017, p. 54). However, India has a negligible base of cyber security specialists when compared to internet user base. India's approach to cyber security has so far been *ad hoc* and unsystematic. Despite the number of agencies, policies and initiatives, their implementation has been far from satisfactory. Due to the existence of too many agencies with overlapping functions in the field of cyber security, coordination between these agencies is poor.

The lines between the physical and digital realms are blurring rapidly, making critical infrastructure extremely vulnerable to attacks from hostile State and non-State actors. Cyber capabilities can be used to undermine critical infrastructure, industry, and security, as seen in the ongoing conflict in Ukraine where electronic systems in warheads, radar, and communication devices have reportedly been rendered ineffective using hacking and GPS jamming (Kumar and Minocha, 2023, p. 109).

Private sector participation remains limited in India's cyber security structures, and collaboration with like-minded inter-governmental and state frameworks is necessary to protect users and customers from cyber breaches. With more inclusion of Artificial Intelligence (AI), Machine Learning (ML), data analytics, cloud computing and Internet of Things (IOT), cyberspace will become a complex domain, giving rise to issues of a techno-legal nature(Ratan and Zaidi, 2018, p. 73). Further, the introduction of 5G and the arrival of quantum computing will increase the potency of malicious software.

Insider threats pose a significant challenge, as individuals with authorised access may misuse their privileges for malicious purposes. With the advancement of technology, cyber criminals are employing increasingly sophisticated techniques to breach security systems. Individuals and organizations have limited knowledge about best practices of cyber security making them vulnerable to cyber-attacks. Acute resource constraints are yet another challenge to cyber security. Implementing effective cyber security measures requires substantial resources, including financial investments, skilled personnel, and advanced technologies(Halder, 2016, p. 119).

These are some of the challenges the country is confronting today in the realm of cyber security which need to be addressed to ensure a safe cyberspace free from potential cyber threats.

Suggestions for Increasing Cyber Security:

Various suggestions and recommendations may be extended for enhancing cyber security in the country. For example, strong passwords for all types of accounts should be set. Password should be hard to guess and should never be shared with anyone. A combination of upper and lowercases, numbers, and symbols should be used. Many password management tools like LastPass, Dash Lane or Sticky Password can be used to keep track of everything for an individual. These applications help use unique and secure passwords for every website one needs and keep track of all the passwords. It is also important to change passwords periodically.

It is easy for an attacker to gain access to someone's network by using old credentials that have fallen by the website. Hence, it is always recommended to delete unused accounts. Enabling two-factor authentication to add extra security to someone's logins is a good practice. The extra layer of security makes it harder for an attacker to get into someone's accounts. One should be sure to protect one's personal information. One should not share password or any other sensitive information online or with any person. Also, an up-to-date anti-virus program should be used to scan the computer regularly to protect the system from malicious software. One should also stay informed about the latest cyber security threats. Keeping up with the news and reading articles on cyber security can help one stay aware of the latest threats and how to protect against them.

Investments should be made on R&D to develop more innovative technologies to address increasing cyber security threats. Immediate attention has to be given to human resource development which would increase the number of experts who can effectively manage the cyber security of the country. Likewise, duties and responsibilities should be defined clearly for smooth functioning and better coordination among departments and stakeholders. A periodic awareness campaign by the government and big private organizations should also be conducted to aware people about cyber security threats. It is also important for the corporates or the respective Government Departments to find the gaps in their organizations and address those gaps and create layered security system, wherein security threat intelligence sharing is happening between different layers. State Cybersecurity Framework should be envisaged in PPP Model. Government should partner with the private sector and the academia to strengthen cybersecurity posture of the state.

Security Audit adhering to international standards should be applicable to all Government websites and applications before hosting and publishing. State cybersecurity framework should support strategy and implementation mechanisms to prevent digital impersonation and identity theft and the security incidents. Framework of assurance should also be established to provide guidance on security certifications, qualification criteria and prescribe security audits of government ICT systems, projects and applications. Further, the Government agencies implementing IT Projects should allocate appropriate budget towards compliance with the security requirement of IT Act, 2000.

Last but not the least, it is of critical importance to ensure global cooperation through information sharing and strengthening joint efforts in cyber security research and development as most cyber-attacks originate from beyond the borders. India can consider joining Budapest Convention along with multilateral initiatives like QUAD (Rathore and Jamshed, 2017, Page. 138).

In this way, by keeping in mind the above suggestions and recommendations, cyber security in the country can be strengthened and the individuals, Government Departments and the private organisations can be adequately protected from various forms of cybercrimes.

Conclusion:

Although it and use proper anti-virus so that their system and network settings stay malware and virus free. The above suggestions and recommendations may also be followed in order to ensure a safe cyberspace. So far as the Government of India is concerned, it has taken many steps and still much needed to be done in this direction so as to enhance the country's cyber security by effectively implementing the laws and policies related to the security of the cyberspace. India can take the lead in conceptualising a global framework of common minimum acceptance for cyber security.This would be a significant contribution to collectively secure security and a step towards building consensus on cyber security emphasising the importance of taking preventive measures and developing effective cyber security policies.

References:

1. Halder, Debarati. (2016). Cyber Crimes against Women in India. Sage.
2. Kant, Mani. (2019). Legal Framework on Cyber Crimes. Kamal Publishers.
3. Kumar, Ashok and Minocha, O. P. (2023). Cyber Encounters: Cops' Adventures with Online Criminals. Prabhat Prakashan.
4. Ojha, Abhinav. (2020). Beginners' Guide to Cyber Security. Notion Press.
5. Prasad, Prakash. (2017). A Brief Introduction on Cyber Crime Cases under Information Technology Act: Details and Analysis. CreateSpace Independent Publishers.
6. Ratan, Deepak and Zaidi, M. H. (2018). Online Cyber Crime (Cyber Fraud). Alia Law Agency.
7. Rathore, Bhushan and Jamshed. (2017). Fundamentals of Cyber Security (Principles, Theory and Practices). BPB Publishers.
8. Relia, Sanjeev. (2016). Cyber Warfare: Its Implications on National Security. Vij Books (India) Pvt Ltd.
9. Roy, Gaurav. (2020). Cyber Security and Digital Privacy: Universal Approach. Highbrow Scribes Publications.
10. Shinde, Anand. (2021). Introduction to Cyber Security. Notion Press.