International Journal of Sociology and Political Science
www.sociologyjournal.in
Online ISSN: 2664-7745
Received: 15-12-2025, Accepted: 17-01-2026, Published: 03-02-2026
Volume 8, Issue 1, 2026, Page No. 13-15

Cyber security and political will in India

Dr. Sumit Prasher
Associate Professor, Department of Political Science, ARSD College, University of Delhi, New Delhi, India

Abstract
More and more people are using internet in the country and this access is which is increasing everyday. India is considered to be the second largest internet market in the world. It is also true that this advancement brings along with it various benefits but also brings various challenges of cybercrime that affects people at a global level. These crime includes that of Pegasus scandal and various other forms of attack's that highlight the vulnerability of the system in India. Indian government has taken steps like Information technology Act of 2000 which provides for legal framework to regulate electronic transition and digitally undertaken communication. It is noteworthy that while government has been taking steps towards curbing cyber frauds, one finds that private sector and general public still does not take it seriously. Many people still does not use cyber protection software that protect them from cyber frauds. Many a times private sector plays a role in transferring or selling of consumer data to various agencies who in turn use or misuse them for their own benefit.

Keywords: Malware, Phishing, Cyber Terrorism, Human Resource, Data.

Introduction

Over a period of time India has come a long way in becoming a technological power house by adopting advanced methods of digitalisation ranging from E-governance initiatives to encouraging greater use of mobile technology. Today we found that our country is running on digitalised modes of communication and nearly every household is using internet facilities or making payments through digital channels. In past few years, the use of digital technology has grown manifold. The data suggests that today about one billion people are engaging into digital system. Nevertheless, it is true that any new step comes with its challenges also. India today faces challenges like cyber fraud, theft of data, and hacking of computer system. It is seen that governmental agencies have been making consistent efforts to minimize these cyberthreats but those steps look inadequate. Over a period of time, Indian government has taken steps like Information technology Act oof 2000 which provides for legal framework to regulate electronic transition and digitally undertaken communication. It is noteworthy that while government has been taking steps towards curbing cyber frauds, one finds that private sector and general public still does not take it seriously. Many people still does not use cyber protection software that protect them from cyber frauds. Many a times private sector plays a role in transferring or selling of consumer data to various agencies who in turn use or misuse them for their own benefit. India has witnessed a substantial rise in digital technology adoption over the past decade with over 900 million internet subscribers, it ranks as the second largest digital user base globally after China. This surge is particularly prominent in rural areas, largely driven by the digital infrastructure into service delivery across the country. There have been improvement in signal quality coupled with declining cost f smartphones and data plans have significantly broadened digital access. As per data of 2024, nearly 67% of India's population was digitally connected with rural user accounting for 42% of the total users. Consequently, average monthly data consumption per user rose markedly in 2023 with rural users accounting for nearly 53% of total data. Finding suggest that young, educated males from different background are more likely to engage in information seeking transactions and personal development activities. Socially disadvantaged groups, despite often spending more time online, tend to use digital tools for entertainment gaming or social networking which are seen as less capital enhancing. One finds that there are various types of cyber threats witnessed namely:

1. **Phishing:** It is a cyber-attack in which criminals impersonate those entities that are trusted by the people like reputed companies, banks and other financial institutions like LIC. Scammers send deceptive messages and lure the victim to click on links or an attachment.

2. **Malware:** It is a kind of a cyber-attack in which malicious software like those containing viruses is able to infiltrate the system and is able to steal the data. Attackers usually use it for the purpose of blackmailing or to extort money from the victim.

3. **Insider threats:** It is seen as a risk of security from the person who works within the organisation and is able to misuse his authorized arm to breach date. This kind of attack is very dangerous and hard to control as someone who is trysted would get involved in such criminal activities.

4. **SQL injection:** It highlights a major system vulnerability which leads the hacker to with the fiddle against the queries of application which are a part of a database. An attacker can manipulate this input to alter the logic of query or its structure

5. **Zero Day Attack**: It is a kind of an attack where there is a software which has vulnerability that is unknow to the developers and giving them zero day to protect it. Meanwhile attackers can use it easily as there is no security or Défense exist against it.

Various forms of Internet threat in India:

1. **Cyber terrorism**: It is an attack which is digitally undertaken with a motive to attack computer systems to incite violence.

2. **Data Threat:** In India online transactions have seen a sharp rise. Also, establishments today are looking to collect data like customer information, by the way of product survey market information), they also create intellectual property that is in itself an attractive target.

3. **Cyber warfare:** It involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks.

4. **Infrastructure Concerns:** Today computer systems are prone to threats by various sources Most equipment and technology systems are vulnerable to cyber threats. In India government has established National Critical Information Infrastructure Protection Centre (NCIIPC) to deal with such concerns..

5. **Shortage of specialists:** Today, India is second in terms of Internet users only after China (Internet World Stats, 2017). Still, India faces a huge shortage of cyber-security specialist who can assist the government in implementation of measures that counter such threats.

6. **Absence of enforcement mechanisms:** India's has not been able to bring out a systematic plan regarding enforcement of the laws that are made by the government. Country has not been able to strictly enforce laws and bring justice to those who have faced cybercrime.

7. **Coordination among the agencies:** One finds that in India there are many agencies working to fight cybercrime but they have not been able to show a coordinated effort thus leaving loopholes in the system.

Initiatives of the Indian government:

1. **Information Act, 2000:** The Information Act, 2000 which was amended in 2008 is considered to be the basic law that deals with cybercrime in India. It is able to give legal status to e-commerce transactions, digital signatures and electronic records.

2. **National Cyber Security Policy, 2013**: It focuses on securing infrastructure and creating a secure ecosystem. 1930 number is launched as a helpline number to report cyber crime. Various strategies are devised to protect cyber space of the users in India

3. **The CERT-In (Cyber Emergency Response Team – India):** It is in operation since 2004. It is a body working at national level that collects threat intelligence and technical assistance to stakeholders against hacking.

4. **Indian Cyber Crime Coordination Centre:** The Indian Government has established 14C under the Ministry of Home Affairs. It is the highest body which acts as a coordination centre dealing with cybercrimes.

5. **The Cyber Warrior Police Force:** In 2018, the government announced its plans to introduce CWPF. It is proposed to be raised on lines of the Central Armed Police Force (CAPF). It acts like a specialized units within the police department that investigates crimes like child pornography, online stalking and financial fraud.

6. **Prevention of cyber-crime against Women & Children' Scheme: It was brought into force** by the Ministry of Home Affairs, it's aim is to stop cybercrimes undertaken against women and children. Here crimes like Information Technology Act and POSCO Act are handled by the specialists who remain sensitive to privacy and security of children and women.

Way Forward

1. **Increasing capabilities:** India has to increase its capabilities so as to be able to provide a safe environment for internet users in the country.

2. **Encouraging Human resource:** The need of the hour is to undertake development of human resource so as to increase hiring of those experts who can counter the actions of the criminals.

3. **Research and Development:** Investments in India must encourage dedication through research and development so that there are precautionary mechanisms developed to counter actions of cyber criminals.

4. **Government Policies:** In India there should be a strong political will that should be exhibited to meet the challenges of cyber crime and police, courts and other governmental agencies should come down heavily on those who are found to be involved in such crimes.

5. **Spreading Awareness:** It is stated that prevention is better than cure likewise people must be educated about the threats of cyber-attacks and how to deal with them. There should be campaigns launched regularly that spread awareness among the masses.

6. **Public Private Partnership:** Indian government must establish public private partnership so as to make sure that sharp minds of the I T sector join hands with the government al agencies to restrict unethical practices..

Although the Indian undertaken many steps still much is needed to be done. Still, we find that everyday thousands of Indians are becoming victims of Cybercrime and digital arrest is faced by many people especially elderly people. It is also found that many of these criminal's activities remain unsolved as it is very difficult to trace the criminals. It is important that government should outline a policy that effectively implements it. India at present is standing at the helm of information transformation, which is why it has become a magnet for cyber fraudsters. In order to realise, the safety of the internet users the governments have to establish quick cyber response team that can prevent fraud and is destroy scam operations. Today it is a responsibility of both i e the government and the citizens who should act

together to counter cyber criminals. It is needed that a greater awareness is undertaken by the government by the way of advertisement in newspaper, T V and other social media platforms.

References

1. Shinde Anand, "Introduction to Cyber Security: Guide to the world of Cyber Security", Notion Press, 2024.
2. Rathod Falgun, "A Guide to Cyber Security and Data Privacy", Writer's Pocket, 2025.
3. Muralidharan K M, "Laws of Cyber Crimes in India", Asia Law House, 2023.
4. Prasad Pilani, "White Collar Crime ", Whiteman, 2020.
5. Sharma Abhishek, "Hack the Future: Unlocking the World of Cyber Security", S K Kataria & sons, 2025.
6. Tripathi P K, "Cyber Security", S K Kataria & sons, 2024.