Manuscript ID:
TIJCMBLIR-2025-020614

Volume: 2

Issue: 6

Month: December

Year: 2025

E-ISSN: 3065-9191

Submitted: 15 Nov 2025

Revised: 27 Nov 2025

Accepted: 15 Dec 2025

Published: 31 Dec 2025

Address for correspondence:
Dr. Dalbir Singh
Associate Professor & Head, Dept. Of Commerce, Gaur Brahman Degree College Rohtak (Haryana)
Email: kaushikdalbir@yahoo.com

DOI: 10.5281/zenodo.18345985

DOI Link:
https://doi.org/10.5281/zenodo.18345985

Securing the Digital Frontier: Cyber Security in the Era of Digital India

Dr. Dalbir Singh
Associate Professor & Head, Dept. Of Commerce, Gaur Brahman Degree College Rohtak (Haryana)

Abstract

Whenever discussions are held with global technology leaders about India's flagship programmes—Digital India and Smart Cities—the conversation eventually shifts from the vast scale and execution capacity to the critical issue of cyber security. Today, security breaches have become almost routine. While these initiatives aim to generate new social and economic avenues, they also expand the digital ecosystem, creating more entry points for cybercriminals. The success of a fully connected economy depends heavily on the safety and reliability of the devices and systems that make up this network. Therefore, this study focuses on understanding the rising necessity of cyber security in an increasingly digital era. The research is based on secondary sources such as books, journals, reports, and online material relevant to the topic.

Keywords: *Cyber Security, CAMS, Digital India*

Introduction:

Digital India progresses and Smart Cities become a reality; security must be embedded into the planning stages rather than treated as an additional requirement. According to Tarun Kaura, Director of Technology Sales at Symantec India, ensuring the safety of data, protecting citizens' personal information, and securing critical digital infrastructure requires strict adherence to security policies along with the adoption of advanced tools and techniques.

India's digital economy is expected to reach nearly USD one trillion within the next few years. With cyber security becoming a top priority, the government is actively collaborating with several countries, including the United States, to curb cyber espionage and digital threats, as stated by Union Minister Ravi Shankar Prasad. The global response to the Digital India initiative has been highly positive, and the minister believes that the coming years will see a significant rise in digital service delivery, with governance increasingly shifting to mobile platforms.

India presents enormous potential for digital transformation, supported by over 319 million internet users and around 214 million mobile subscribers. Encouraged by this demographic strength, Prime Minister Narendra Modi continues to push the Digital India vision, aiming to elevate the economy from USD 8 trillion to USD 20 trillion. One of the major innovations under this initiative is DigiLocker, a platform that offers citizens secure digital storage for government-issued documents and supports digital signatures.

Some key initiatives under Digital India include:

- Increasing public Wi-Fi availability by adding 500 railway stations through a partnership with Google
- Expanding the National Optical Fibre Network to connect over 600,000 villages in collaboration with Microsoft
- Strengthening the foundation for mobile governance through various applications
- Developing digitally empowered citizens
- Creating Smart Cities to accelerate technological and economic growth

To achieve these goals, India has partnered with leading global technology companies such as Microsoft, Google, Apple, and Facebook. Qualcomm has committed USD 150 million to support mobile and IoT startups, while Foxconn plans to establish manufacturing operations in the country. Modi's wider reform agenda—focused on deregulation and a more business-friendly environment—further supports innovation-driven growth. However, like any major digital transformation, the Digital India programme brings with it significant concerns about privacy, data protection, and overall cyber security.

During his address at the Digital India event in Silicon Valley, Prime Minister Modi highlighted his vision of a highly connected India—where social media platforms become digital neighbourhoods—and encouraged active participation

How to Cite this Article:
Singh, D. (2025). Securing the Digital Frontier: Cyber Security in the Era of Digital India. The International Journal of Commerce Management and Business Law in International Research, 2(6), 61–65. https://doi.org/10.5281/zenodo.18345985

from the global technology community. Some major points from his speech include:

1. For the younger generation, one of the most common debates today revolves around choosing between Android, iOS, and Windows.
2. India is combating poverty by leveraging digital networks and mobile technology to create new opportunities for empowerment and inclusion.
3. The rapid adoption of digital tools across age groups, languages, educational backgrounds, and income levels shows the transformative potential of technology.
4. With nearly a billion mobile phones and a fast-growing smartphone market, mobile governance will play a central role in public service delivery.
5. India aims to digitally connect its entire population of 1.25 billion people, with broadband usage rising significantly—by 63% last year alone.
6. A major expansion of the National Optical Fibre Network is underway to bring broadband to 600,000 villages and link educational institutions across the country.
7. Free Wi-Fi services will be extended beyond airports to railway stations, with 500 stations being modernized in partnership with Google.
8. The goal is to convert rural areas into smart economic hubs and help farmers access markets more efficiently.
9. The government seeks to promote the manufacturing of high-quality and affordable digital products under initiatives such as Make in India, Digital India, and Design in India.

In line with these developments, the government places the utmost importance on cyber security, data privacy, and protection of intellectual property as India becomes increasingly digitized.

Objective Of the Study:

The main objective of this paper is to discuss about why there is a need of security in the age of digital India and what are the steps should be taken for cyber security.

Research Methodology of The Study:

This study is based entirely on secondary sources of information. Relevant data was collected from books, academic journals, magazines, and published research papers. Online resources were also used to access updated reports and credible digital content. All collected material was reviewed, analysed, and compared to understand trends in cyber security. The findings are derived through qualitative assessment of these secondary data sources.

Why There Is a Need of Cyber Security for The Digital India Campaign?

Digital India Initiatives & Need of Cyber Security

We have already discussed about the alarming rise of cybercrimes in India and government's continuous struggle to cope up with the latest trends of attacks. Apart from domestic cyber threats, India also faces tough cyber-attacks from countries including Pakistan, China, UAE, US, Turkey, Brazil, Bangladesh, Algeria and nations in Europe.

As per the statistics from the National Crime Records Bureau and other sources:

- 1,791 cases were registered in 2011, which grew to 2,876 cases in 2012 and to 4,356 cases by 2013.
- Hacking formed close to 60 per cent of all cyber offences.
- 58 per cent attacks are for financial gains and 42 per cent by foreign governments
- 155 .GOV and .NIC domains were hacked last year
- 32,323 public Indian website were hacked in 2014 with 14 per cent Y-o-Y increase

To counter this alarming situation, Indian Government has aimed to step up cyber security measures under Digital India programme starting with a Rs. 800-crore center that will help people check and clean their computer system from viruses and other malwares. The programme is intending to build capability to tell you that not only can track the malwares in computer system but will clean that infection as well.

A year in the works, the National Cyber Security and Coordination Centre (NCSC) will analyze Internet traffic data scanned and integrated from various gateway routers at a centralized location. It will facilitate real-time assessment of cyber-security threats and generate actionable reports for various agencies.

As a multi-agency body under the Department of Electronics and IT, the NCSC will include the National Security Council Secretariat, the Intelligence Bureau, the Research and Analysis Wing (RAW), the Indian Computer Emergency Response Team (CERT-In), the National Technical Research Organisation (NTRO), the three armed forces and the Department of Telecommunications. It is expected to subsume the work done by CERT-In as well as issue alerts in the event of a cyber-attack.

The Growing Gap in Digital Literacy

India's Prime Minister called the country "a nation of one billion cellphones". However, quantity doesn't mean quality, and this has never been truer in terms of cyber security. Security experts, concerned with where could "Digital India" go wrong, reveal alarming trends:

- Nearly 1/3 of Indian organizations are unfamiliar with cyber attack prevention ("Get Ahead of Cybercrime", EY's global information security survey). They seem to lack agility, finances and employees that have the appropriate set of skills.
- 92% of the Indian youth (constituting a huge chunk of the mobile user base) frequently share private information online without realizing the risks. 51% of them didn't even care about the concept of "online privacy" (McAfee report).
- Close to half of the Indian citizens are uneducated about online transactions and often rely on a third party to execute this transaction. Personal information leaks are a daily occurrence (S. N. Ravichandran, member of the Cyber Society of India).

The Chain Reaction Triggered by Data Breaches

Ambitious as Modi's plan is, before fully implementing "Digital India", one should take care of limiting these trends and educating the population on the importance of cyber security. India is in the global top three when it comes to cyber attacks and data breaches caused – a trend that is not only here to stay, but will increase as India's digital citizens rise in numbers. If individual data vulnerability is as bad as it looks, we also have to keep the Bring Your Own Device trend in mind. Because it is perfectly possible that one compromised device can affect the whole multi-tenant network of a company. In this, cyber security becomes a must for both individual users and enterprises alike. Otherwise, economic circles risk to be put in a situation similar to a recent case where a Middle East-based hacker group extorted a staggering $10 million from two Indian companies.

But even more vulnerable is the concept of smart cities – a foundation of the future for Prime Minister Modi. With devices connected with each other, sharing the cloud infrastructure, any data breach will have a devastating domino effect. And if we take note of the worrying trends pertaining to privacy/security literacy of youngsters (who will shape this future of this smart settlements), any smart city is a data breach nightmare waiting to be set in motion. Battling illiteracy and empowering digital citizens through knowledge – not only through innovative infrastructure and increased digital services, is a must. However, the Modi government should also think of its own part of the deal.

Security and privacy should be carefully woven and ingrained in the initiative's foundation, not come afterwards. They should be widely discussed with private entities and experts, as well as security providers in order to maintain a flawless data encryption model and eliminate data breach risks. The legal system should receive "an update" too – strengthening the current model when it comes to addressing cybercrime cases, which are becoming the norm.

The Us and India: Strengthening Security Cooperation

As China, the current economic superpower of the East, becomes increasingly unstable and its markets unpredictable, many are focusing newfound attention southward on India. With its economy growing at a rate of seven percent, India is poised for an economic surge similar to that of China, with the benefit of drawing greater appeal from foreign investors who are deterred by the communist and authoritarian rule of India's northern neighbor.

Wider Issues in The Digital Era

With threats to national and international security on the rise, all agree that security services have to be able to operate in order to address them. However, as the haystack of data necessary to do so has become an object of interest, along with the algorithms that find the needles in it, it has become clear that the traditional mechanisms used to control surveillance are inadequate.The conundrum is how to ensure protection while retaining the critical underpinnings of our democratic systems – free speech, freedom of assembly and association, and, critically, the right to privacy. It is clear that with the acceleration of technologies, there are no easy lines to draw. Moreover, in the internet age, almost all boundaries are being erased or redefined.

Hidden Vulnerabilities In The Digital Era

Is it possible to be secure without giving up some privacy? Theoretically yes, although in reality it is not so easy to implement. But stating this has never been so contested. The strategic environment in which state intelligence operators maneuver is evolving rapidly, from an increasing number and different types of intelligence consumers, to demands for faster and more efficient responses in the roiling confluence of threats. There's also the increasing complexity of cross-border terrorism and asymmetric war, and the full-on return of interstate strategic conflict. Thus, keeping distinctions between domestic and international does not work anymore.

Today, the situation has shifted dramatically. The recently released Global Terrorism Index report (GTI) from the Institute for Economics and Peace shows that between 2012 and 2013, the number of people killed in terrorist incidents saw the largest increase in history, to 18,000 lives lost, which is a 61 percent increase from one year to the next.

Mass Data

Is it problematic if government agencies collect our digital footprint, metadata, online habits and digital history for eternity? This data can potentially be used and abused – but it can also keep people safe. When reflecting on this question it is important to remind ourselves that, between the telecommunication companies, internet search engines and social media apps, you may have already consented to share a lot of your data, including your needs, preferences and dislikes.

Transparency As A Driver Of Better Intelligence

For the intelligence community and the wider government apparatus, this is a matter of public image. To build trust, both groups need to be far more effective in explaining how they honour their responsibilities towards the privacy of individuals, especially in communities that feel they bear the brunt of scrutiny.

On the cooperation front, there must be more clarification regarding the distinction between mass collection of information and mass surveillance. Through this clarification, there must be more knowledge among lawmakers about security implications, so that informed legislation and regulatory frameworks can be put in place. In particular, knowledge and legislation must be increased dramatically around the issue of cybersecurity.

Public-Private Collaboration

Cooperation can also be preventative and on a larger scale. For example, in the digital world of big data, it behooves intelligence agencies to try to enlist the help of the private sector to collect and share data. This type of cooperation also serves the purpose of creating an ally in the private sector to influence

legislation and regulations on a global level. Yet, normally such information sharing only occurs when the parties truly have an incentive to do so, and for the private sector, the case has generally not been compelling. Thus most so-called public/private information sharing has produced little, if any, meaningful sharing.

Cyber Security

Where cooperation becomes essential is in the realm of cybersecurity. Keeping tabs on dangerous actors online has increased the need for a stronger dialogue between intelligence operators and companies with vast experience in mining and interpreting massive data sets. Both the intelligence community and these companies can work together to increase the understanding among lawmakers about the growing number of "digital extremists", many of whom operate on the dark net, but most of whom are also still in the open, using social media platforms. The private sector carries a particular responsibility to put mechanisms in place to alert governments about the harmful use of their platforms or networks that compromise the security of individuals, nations and the global community. Despite agreeing that protecting public goods and security is a shared responsibility, many companies see this – commonly referred to as "digital back doors" – as posing great reputational risk and being bad for the bottom line (since the regulatory framework around where to draw that line remains unclear).

As the world becomes increasingly digital, the importance of understanding threats in cyberspace cannot be overstated. Terrorists use cyber tools for propaganda, recruitment and fundraising with such ease that intelligence agencies are truly struggling to keep pace. It is clear that in the field of cybercrime there has been a growing success in partnerships across countries as well as between public and private sectors. Now it is time to leverage this progress to attempt to build more and better bridges between the national intelligence community, the private sector and the wider public.

Agile Regulation in The Digital Era

By nature, intelligence agencies will constantly push the boundaries of legal frameworks to adapt to the rapidly changing security landscape. Such frameworks should be strong but elastic enough to adapt. Qualified decision-makers (those who can make informed judgement calls to determine the means necessary to justify security) are essential to this equation. And it is of vital importance that the authorities involved in regulations and oversight fully understand the evolving technology, tools and security issues. Educating the public to appreciate this paradox is also a necessity.

Although, to a degree, this phenomenon is already happening, it does not have strong enough support from key players to create the transparency that would foster more trust and support. The paradox is that more openness, more visibility and more engagement with other sectors are what will ultimately help intelligence agencies evolve into their role for a new security era.

Conclusion

The rapid expansion of Digital India and the development of Smart Cities mark a transformative shift in the country's social and economic landscape. However, this digital revolution also exposes India to unprecedented cyber security challenges. As the study reveals, the rising number of cybercrimes, increasing sophistication of attacks, and widespread technological illiteracy collectively make India vulnerable to large-scale data breaches and systemic cyber threats. These risks are further amplified by the interconnected nature of modern digital infrastructures, where a single compromised device or platform can trigger a chain reaction of failures across networks, institutions, and even entire smart city frameworks.

The government has taken several proactive steps, such as establishing the National Cyber Security and Coordination Centre (NCSC), collaborating with global technology firms, and expanding public digital infrastructure. Yet, the success of Digital India ultimately depends on embedding security into every layer of the digital ecosystem—technology, governance, industry, and citizens. Strengthening cyber hygiene, promoting digital education, and ensuring robust legal frameworks are essential to safeguard national security and public trust.

Equally important is the need for transparent cooperation between government agencies, private companies, and international partners. As cyber threats evolve, agile policies, advanced technologies, and informed oversight must work together to create a resilient digital environment.

In conclusion, the vision of a digitally empowered India can be realized only when cyber security becomes a shared responsibility. A secure digital foundation will not only protect citizens and institutions but also accelerate innovation, economic growth, and global competitiveness in the years ahead.

Acknowledgment

I express my sincere gratitude to all scholars, researchers, and authors whose books, research papers, reports, and online publications have contributed significantly to the completion of this study. Their valuable insights and scholarly work provided the theoretical foundation and critical understanding necessary for examining cyber security in the context of Digital India.

I am thankful to my colleagues and academic peers for their constructive suggestions and intellectual support during the preparation of this paper. I also acknowledge the support of my institution, **Gaur Brahman Degree College, Rohtak**, for providing a conducive academic environment and access to necessary resources.

Finally, I extend my heartfelt appreciation to my family and well-wishers for their constant encouragement and moral support throughout the research process.

Financial support and sponsorship
Nil.

Conflicts of interest
The authors declare that there are no conflicts of interest regarding the publication of this paper.

References
1. http://www.dnaindia.com/analysis/standpoint-why-cyber-security-is-critical-for-digital-india-2127604
2. http://www.financialexpress.com/article/india-news/tech/security-in-the-age-of-digital-india/91341/
3. http://forbesindia.com/blog/business-strategy/security-in-the-age-of-digital-technology/
4. https://www.linkedin.com/pulse/security-age-digital-india-mohd-ujaley
5. https://blog.perfectcloud.io/digital-india-great-overlooking-cyber-security-can-ruin/
6. http://www.bgr.in/news/10-things-narendra-modi-said-at-the-digital-india-event-in-silicon-valley/
7. http://www.asianage.com/business/india-touch-foreign-governments-cyber-security-ravi-shankar-prasad-260