ISSN : 3048-5320 (Online)

CSIBER International Journal - CIJ

Vol. 3, Issue 4, December, 2025

MULTIDISCIPLIANRY JOURNAL

MAKE IN INDIA

Published by : CSIBER Press, Central Library Building, CSIBER Campus, University Road,Kolhapur-416004, Maharashtra, India.

Find the Journal Online at
https://www.siberindia.edu.in/journals
E-mail : cij@siberindia.edu.in

CSIBER International Journal (CIJ)

CONTENTS

ISSN: 3048-5320 (Online)

Towards A Secure Digital Governance in India: Assessing Cybersecurity Initiatives and Strategy Therefore

Prof. (Dr.) Shyam T. Shirsath
[1]Department of Public Administration, Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar, Maharashtra, India

Mr. Swapnil S. Kumare
Department of Public Administration, Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar, Maharashtra, India

Abstract

Cyber security has become a very critical concern that needs the attention of researchers, academicians, and organizations to confidentially ensure the protection and security of information systems. After all Digital technology has transformed how governments deliver services, improved productivity and increased citizen engagement. Yet this digital transformation comes with a host of new cybersecurity challenges that could jeopardize the integrity, confidentiality and availability of government systems and data. This paper examines the critical need for balancing innovation with robust cybersecurity measures within government frameworks. It explores the dual imperatives of fostering technological advancements and ensuring the security of sensitive information against increasingly sophisticated cyber threats. By analyzing case studies of successful and unsuccessful cybersecurity projects in different governmental environments to reveal best practical futuristic technologies, but still effectively secure cyberspace. The paper also examines the importance of resilient policy, private partnerships and resiliency-related workforce training. The findings from the study aims to provide useful knowledge and evidence-based suggestions for policy making on innovation, as well as public administration in efforts regarding sustainable balance between innovating while maintaining safety in the public and private organization

Keywords: Cybersecurity, Government, Innovation, Digital transformation, Public & private sector, Cyber threats, Data security, Technological advancements

Introduction

Evidently, the existing environment characterized by a constant launch of new technologies makes the maintenance of proper cybersecurity levels a difficult task for government organizations. Decision makers in government are presented with the challenge of encouraging innovation while protecting the information and assets important to a nation. The focus of this research paper, lies on analyzing the contemporary and complex nature of cybersecurity governance frameworks, including the possible considerations and achievable strategies that the government agencies should focus on to improve their cybersecurity and protect their valuable digital resources adequately (Perumal et al., 2018). Governments have to embrace a radical change in the existing approach to cybersecurity governance that cannot be addressed through conventional IT-centric solutions. This calls for the inclusion of cybersecurity factors within the overall policy-making and implementation process in governmental context. In taking more of an enterprise approach for the government agency, it can improve the alignment of cybersecurity programs to the overall mission and objectives of the agency, as well as improve its responsiveness to the needs of the people it serves. Such an approach allows governments to promote the development of new technologies, advance their cybersecurity preparedness, and safeguard important data and infrastructure assets. Despite awareness by governments on the need to enhance cybersecurity measures, establishing proper governance frameworks remain a complex process.

Research Objectives

This study aims to:

- Examine the contemporary challenges faced by government agencies in cybersecurity governance.
- Identify adaptive strategies to incorporate cybersecurity within policy-making and operational frameworks.
- Propose a balanced framework that allows government agencies to protect digital resources while fostering technological innovation.
- Assess effective cybersecurity practices in various governmental contexts and recommend improvements.

Research Methodology

This research employs a Mixed Method Research Methodology, analyzing secondary data from case studies, policy documents, and recent literature on cybersecurity governance in government sectors. The study evaluates adaptive governance frameworks emphasizing organizational culture, workforce preparedness, and advanced technological integration.

Adaptive Cybersecurity Governance Framework

The governments need to employ an adaptable approach of cybersecurity governance to ensure counter threats as they emerge while fully incorporating advances in technology. This framework should focus on cybersecurity-oriented workforce, and the process of changing organizational culture. (Perumal et al. , 2018) (Melaku, 2023) Moreover, government agencies remains relevant and prepared with the current and emerging dangers in cybersecurity to ensure that their protective strategy is align with operational requirements. The key components of an adaptive cybersecurity governance framework for government agencies should include such as consistent threat scanning and evaluation, the implementation of constant risk mitigation measures, good cooperation and information sharing among government agencies as well as with the private sector, an extensive education and sensitisation of employees towards cybersecurity, and the application of advanced technologies such as artificial intelligence and machine learning in risk detection and prevention. Therefore, urgent actions that are required to tackle the cybersecurity threats that confront a safety and stability of nation.

Balancing Innovation with Security

The governments have now a challenge of balancing between adopting new technologies and at the same time ensuring their systems have strong security systems. On the one side, there is an opportunity that the advancement of IT technologies will assist in the improvement of governmental performance, quality of delivered service, as well as the ability to meet the new demands of society. Nonetheless, incorporation of these new technologies may also bring in some new threats and risks to the security that are avoidable. (Alenezi, 2022) Governments face the challenge of leveraging new technologies for enhanced performance and service delivery while ensuring robust cybersecurity. While technological advancements offer efficiency and responsiveness, they also introduce potential security threats, necessitating a careful balance between innovation and protective measures to mitigate risks effectively.

In order that all of this becomes a reality, it will be necessary for government agencies to begin to focus more on the role of security requirements in the processes of design, development, and deployment of these new technologies. This can be in form of; The use of secure software development methodologies, continuous security assessment and evaluation, and effective security incident management frameworks. Moreover, the government entities should assess how other cutting-edge technologies like artificial intelligence and machine learning can be applied to improve the cybersecurity perspective that would let the government entities create powerful and effective mechanisms for the perception, analysis, and response to the threats (Melaku, 2023) To ensure secure technology integration, government agencies must prioritize security in design, development, and deployment stages. This includes secure software practices, ongoing security assessments, and incident management. Leveraging AI and machine learning can further enhance cybersecurity, enabling better threat detection, analysis, and response mechanisms.

Technological Advancements and Cybersecurity Threats

The development of the technology has not only created an opportunity for the government to improve its services but also a new threat to cybersecurity. The opponent has utilized these advances in technology to come up with complex attack strategies, which limit the usefulness of passive defence strategies. (Kuvan and Kimani, 2022) To counter these emerging threats, leading governments have moved away from the traditional fixed security systems to more flexible approaches to security. One of them is the use of artificial intelligence and machine learning as part of cybersecurity approaches. These technologies can help government agencies to identify threats and cyber risks in real-time, perform the data analysis and identification of patterns that could be behind them, and modify their security policies in order to put up with new threats and risks. In the same respect, new technologies such as cloud computing and the Internet of Things (IoT) may improve the efficiency and services of the government; however, these innovative technologies also present novel security threats that arise from their use. (Ghaffar, 2020); (Lasisi et al. , 2022) Technological advancements offer governments enhanced service delivery but also introduce sophisticated cybersecurity threats, as attackers exploit these innovations. Traditional, static defenses are insufficient, prompting a shift to adaptive security approaches incorporating AI and machine learning. These tools enable real-time threat detection, data analysis, and proactive policy adjustments. However, emerging technologies like cloud computing and IoT also require vigilant security measures to counter new vulnerabilities effectively.

ISSN: 3048-5320 (Online)

Reviews of Cybersecurity Initiatives

Cybersecurity initiatives have become essential as governments shift from passive to proactive defense strategies. Many countries are adopting AI-driven tools, continuous security assessments, and collaborative threat intelligence frameworks to combat complex cyber threats. These initiatives have improved real-time threat detection and response capabilities, strengthening national security. However, adapting to rapid technological changes remains a persistent challenge. Many State governments have implemented innovative cybersecurity initiatives to address the evolving threat landscape.

Policies	Key Initiatives	Impact
National Cyber Security Policy (NCSP) – 2013	- Establishment of CERT-In (Indian Computer Emergency Response Team) to monitor and respond to cyber threats. - Promotion of a culture of cybersecurity awareness. - Development of a national-level mechanism for monitoring and defending against cyberattacks.	Increased cooperation between public and private sectors, introduction of cybercrime investigation training programs, and guidelines for data security management.
Digital India Campaign - Cybersecurity Initiatives	- Creation of Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to assist individuals and organizations in detecting and preventing malware. - Promotion of the Cyber Surakshit Bharat Initiative, a public-private partnership to raise awareness about cybersecurity among government officials and organizations. - Establishment of e-Governance Security Infrastructure to protect government databases and digital platforms.	Improved awareness among government employees and citizens, leading to increased adoption of safe online practices and secure use of digital services.
Maharashtra Cyber Security Project	- Establishment of Maharashtra Cyber, the state's dedicated cybersecurity unit. - Cybersecurity training programs for police officers and public sector employees. - A focus on public-private partnerships to enhance cybersecurity practices.	Increased awareness and preparedness of government departments in Maharashtra, along with the establishment of a dedicated Cybercrime Coordination Centre.
Tamil Nadu has proactively built a Cyber Crime Wing*	- Setting up of specialized Cybercrime Cells in police stations. - Launch of cybercrime awareness campaigns and online portals for citizens to report crimes. - Introduction of specialized training programs for law enforcement to handle digital crimes.	Faster response times in cybercrime investigations and increased public participation in reporting cyber incidents.
Karnataka's Cyber Crime Incident Report (CIR) Platform	- The Cyber Crime Incident Report (CIR) platform, enabling citizens to report crimes like identity theft, hacking, and online fraud. - Collaboration with the central	Significant reduction in investigation time and improvement in the state's cybercrime detection and resolution capabilities.

 ISSN: 3048-5320 (Online)

	government for enhanced cybercrime investigation training.	
CERT-Goa: State-Level Cybersecurity Efforts	- Collaboration with national CERT bodies and private organizations to build a comprehensive cybersecurity framework. - Training programs for law enforcement, government officials, and educators to ensure better cyber safety practices.	Increased response to cybersecurity incidents and improved preventive mechanisms at the state level.
CyberDome (Kerala)	- Use of cutting-edge technologies like AI and Big Data analytics for cybercrime prevention. - CyberDome also plays a role in creating awareness through workshops, seminars, and partnerships with educational institutions.	Improved collaboration between the police, tech industry, and academia, leading to faster identification and mitigation of cyber threats.
Meghalaya Cyber Security Policy	- Cybersecurity capacity-building initiatives for state employees. - Implementation of robust security measures for digital platforms and public data.	Enhanced readiness of state-level digital infrastructure and improved cyber hygiene practices among public officials.
Telangana Cyber security framework policy	- Security Operations Centre (SOC): Real-time monitoring and threat detection. - Cyber Warrior Teams: Ethical hackers and experts auditing government systems. - Cyber Security Task Force: Collaboration with industry experts for knowledge sharing. - Partnership with NASSCOM: Skill development and best practices for cybersecurity. - Government Data Security Framework: Enforcing strong data protection measures. - Cybersecurity Training (TASK): Developing skilled professionals in cybersecurity. - Public Awareness Campaigns: Educating citizens on safe digital practices. - Cyber Crime Units: Specialized police units for cybercrime investigations.	- Improved infrastructure security: Reduced cyberattacks on government systems. - Public awareness: Safer online practices among citizens and government staff. - Better cybercrime handling: Faster investigation and resolution of cases. - Stronger public-private collaboration: Enhanced cybersecurity ecosystem. - Skilled workforce: Increased cybersecurity talent through training programs.

India's cybersecurity initiatives across various states and national programs have greatly strengthened its digital resilience. Through policies like NCSP-2013 and Digital India's Cybersecurity Initiatives, along with state-specific projects, there is now enhanced cooperation, infrastructure security, and citizen awareness on safe digital practices. Specialized units, public-private partnerships, and training programs have cultivated a skilled cybersecurity workforce and improved state readiness to handle and mitigate cyber threats effectively.

Issues in Contemporary Cyber security Initiatives:

Fragmented Regulatory Framework

• India has no proper singular legislation that deals with the cybersecurity problem. Many organizations such as CERT-In, NCIIPC and others work under the ambit of different legal frameworks and hence there is a lot of synergy as well as variances in the way they function.

• Inter governmental relations are especially inadequate in terms of the coordination between central and state governments and across sectors.

Insufficient Data Protection Laws

• Since natural justice does not require there to be a strict data protection law in the country, there are no strict laws protecting personal data and personal data can easily be misused and breached if there is no Personal Data Protection Bill in the country. It generates confusion on the extent of protection afforded to individuals' privacy and restrains implementation on safeguarding information.

3.Cybercrime Proliferation

• The situation has worsened over the recent past with high-profile cases of ransomware, phishing and identity theft to mention but a few going unaddressed by the authorities. Police forces around the world can be ill-prepared to deal with the more complex cybercrimes.

• Cybercrime is under-reported because people do not know or are too afraid to go to the police thus keeping the countermeasures reactive.

4. Skill Shortages

• It is seen that there is a severe scarcity of qualified cybersecurity professionals to work as an expert and executioner to enforce security measures. This shortage is common across both public and private sectors which has impacted response abilities in general.

5. Limited Public Awareness

• People of society, small companies, and some employees of government organizations have poor knowledge about the threats that exist in the cyber world. Awareness campaigns are still not sufficiently developed and are implemented in an unequal manner.

6. Weak Critical Infrastructure Protection

• It can be stated that important industry segments such as energy, transport, healthcare, and banking have risks of cyber threats. Although there are standard procedures for protecting CIIs, there is normally inadequate means for executing these measures because of shortage of cash and human capital.

7. Lag in Technological Upgradation

• The government and most of the public sector institutions still use outdated systems, and therefore are vulnerable to cyber Later on, many government and public sectors still use old fashioned systems, and as a result are prone to cyber. Updates, patching systems and advanced security solutions which are supposed to be handled on a regular basis are sometimes done very rarely or not at all.

8. Ineffective Incident Response

• Cybersecurity IR continues to be reactive instead of proactive, and a significant number of agencies are not adequately equipped to deal with big attacks. These response mechanisms fail to offer adequate velocity, co-ordination and real time tracking response.

9. Challenges in Public-Private Collaboration

•Currently, cooperation between the government and private structures in the field of cybersecurity is rather ineffective. Threat information sharing and practices are usually informal with little or no well-defined frameworks even if many nations rely on public-private partnerships.

10. Cross-Border Cybersecurity Threats

•The attacks conducted by other states, including states-sponsored threats are quite complicated. The Indian policy framework facing a problem of not addressing cross border cybercrime issues pertaining to international cooperation and jurisdiction issues.

11. Lack of Cybersecurity Budget

•A wide part of allocated budgets for cybersecurity are usually not enough, particularly for state-level projects and for small businesses. Lack of funding means that there is restricted capacity for the development of strong infrastructures, training of professionals as well as the procurement and adoption of advanced security solutions.

India's cybersecurity challenges stem from fragmented regulation, insufficient data protection, and limited incident response capacities. A lack of unified laws and intergovernmental coordination hinders cohesive action, while inadequate data protection and public awareness increase vulnerability. Skill shortages, outdated infrastructure, and reactive responses compromise security efforts. Public-private collaboration remains insufficient, exacerbating challenges in cross-border cybercrime and critical infrastructure protection. Budget constraints further limit state-level and small business capacities to adopt advanced security measures, resulting in a cybersecurity landscape struggling to match the rapid pace of cyber threats and technological advancement.

Way forward: To achieve secure digital governance in India, a comprehensive cybersecurity framework is essential. This includes enacting unified legislation to bridge regulatory gaps, establishing a stringent data protection law, and fostering robust coordination between central and state governments. Proactive public-private partnerships and clear threat-sharing frameworks can enhance security capabilities. Investing in cybersecurity training, improving public awareness, and securing critical infrastructure sectors are critical. Budget allocations should be optimized to strengthen state-level projects and equip government systems with advanced, regularly updated technologies. Additionally, India should bolster international cybersecurity collaboration to address cross-border threats effectively.

Recommendation and Strategies

Security must be embedded in the creation of new systems through secure software development (SSD), continuous security assessment (CSAM), and incident response planning (IRP). Leveraging AI and machine learning can further enhance real-time threat detection and response capabilities. Additionally, governments should foster interdepartmental and public-private collaboration to counter transnational cybersecurity threats effectively.Based on the analysis of the sources and the key considerations discussed, this research paper recommends the following strategies for government agencies to effectively balance innovation with security. (Gordon et al. , 2015) ; Alshaikh, 2020)That is, the governments need to build a contextually sound, adaptive and developing cybersecurity governance framework that accommodates existing and emerging threats, new technologies, the requirement to shape the organizational culture and skills of its employees respectively. They should ensure that security is reflected as an inherent component of the creation of novel systems and applications, employing SSD, CSAM and an IRP(Ross et al. , 2016). To balance innovation with security, this research recommends that governments establish a flexible, contextually aware cybersecurity governance framework. This framework should adapt to evolving threats and technology, embed security from inception in systems through Secure Software Development (SSD), Continuous Security Assessment and Monitoring (CSAM), and Incident Response Plans (IRP). Leveraging AI and Machine Learning for real-time threat analysis, governments can improve proactive defense. Inter-agency and public-private collaboration will further strengthen resilience, addressing cross-border threats. Robust, adaptive policies promoting a culture of shared information and continuous improvement are essential for comprehensive cybersecurity.

Governments need to consider how they can leverage the certain new-age technologies which include AI and Machine learning in order to improve their cybersecurity posture in a manner that would allow them to better recognize, counter, and learn from threats in real time. Government should adopt structures where various government departments as well as other private industries work together and share information to fight the transnational threat indicated in this research. These following policies should adopt such as,

Adopt a Holistic Security Approach:

Governments should embed cybersecurity considerations in all stages of the technology life cycle during planning and design, to deployment and post implementation operations. That concept is simple: security must be built into all stages of the lifecycle of any technological solution, instead being tacked on at the end like a part to repair a washtub. This can help government be more proactive about addressing key vulnerabilities and

security risks before they even get to deployment, thereby improving the resiliency of their critical enterprise systems. (Release of SP 800-160 Volume 2 Developing Cyber Resilient Systems, 2019)

Implement Robust Policies:

National governments should implement and enforce guidelines for cybersecurity based on international norms, rules, and good practices (such as the National Institute of Standards and Technology Cybersecurity Framework or ISO/IEC 27001 Information Security Management System). These guidelines should be supported by appropriate policies that clearly assign roles and responsibilities to ensure consistency in implementation of security controls, risk management and ⎪ Cyber-security incident response. Regular revisions and update of these policies are a crucial element to make them relevant enough in the time facing new ground threats. (Ross, 2018)

Foster Public-Private Partnerships:

Work with cyber-security experts in the private sector and ICT-industry partners to help them better understand what you may lackacial knowledge is special cities which cannot yours. Participate in collective efforts to strengthen the threat detection, incident response and data sharing mechanisms. It creates a public-private partnership by blending the innovative solutions and real time threat intelligence from leading commercial company to strengthen overall cyber defense of government agencies. (CYBERSECURITY STRATEGY, n.d)

Invest in Workforce Training:

Provide ongoing cybersecurity guidance to Public Service workers, brief them on new threats they should be facing and remind them the relevance of vigilant mindset regarding security. Train people with wide-ranging modules that provide government personnel the information and the ability to identify, prevent as well as safeguard in case of an ever-changing cybersecurity threat landscape. Stress the importance of security for every employee, and cultivate a cybersecurity mindset across all levels within government. (Newhouse et al., 2017)

Promote a Culture of Security:

Develop a culture of security- by -design for all government employees and stakeholders, stressing the message that cybersecurity is part – but not an obligation– to address. Enable them for the larger goal that, is to engage in actions reducing the risks and always be on high alert of upcoming threats keeping security mindful practices a part of their daily routines. Instill an ongoing sense of shared responsibility for maintaining awareness on everyone's part and further bolstering cybersecurity at large. (Sadik et al., 2020) robust cybersecurity strategy for government agencies requires a proactive and integrated approach, embedding security throughout the technology lifecycle. Governments should implement internationally aligned policies with clear roles, foster strong public-private partnerships, and continuously invest in workforce training. Cultivating a security-conscious culture across all organizational levels is essential to maintain vigilance and shared responsibility for cyber resilience. Together, these strategies create a resilient framework to address emerging cybersecurity threats while supporting innovation and efficiency in public services.

Conclusion

Governments must diligently pursue a balanced approach to leverage technological advancements while safeguarding cybersecurity. By establishing a comprehensive security agenda and formulating supportive policies, agencies can create a resilient framework capable of addressing evolving threats. Collaborating with private organizations enhances resource sharing and innovation, while continuous workforce training ensures employees are equipped to navigate the complexities of the cyber landscape.

Moreover, promoting a culture of security within government entities fosters a proactive mindset among all personnel, encouraging vigilance and responsibility in maintaining cybersecurity practices. This multifaceted strategy not only enables government agencies to effectively counter dynamic cyber threats but also protects critical systems and sensitive information. Ultimately, these efforts aim to deliver safe, efficient, and trustworthy public services, fostering confidence and resilience among citizens in an increasingly digital world. By prioritizing cybersecurity alongside technological innovation, governments can ensure that advancements benefit society without compromising security.

 ISSN: 3048-5320 (Online)

Reference:

Alenezi, M. (2022, January 1). Understanding Digital Government Transformation. Cornell University. https://doi.org/10.48550/arxiv.2202.01797

Alshaikh, M. (2020, November 1). Developing cybersecurity culture to influence employee behavior: A practice perspective. Elsevier BV, 98, 102003-102003. https://doi.org/10.1016/j.cose.2020.102003

CYBERSECURITY STRATEGY. (n.d). https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

Ghaffar, H N A A. (2020, March 23). Government Cloud Computing and National Security. Emerald Publishing Limited, 9(2), 116-133. https://doi.org/10.1108/reps-09-2019-0125

Gordon, L A., Loeb, M P., Lucyshyn, W., & Zhou, L. (2015, November 26). Increasing cybersecurity investments in private sector firms. Oxford University Press, tyv011-tyv011. https://doi.org/10.1093/cybsec/tyv011

Gürkaynak, G., Yılmaz, İ., & Taşkıran, N P. (2013, October 31). Governmental Efforts and Strategies to Reinforce Security in Cyberspace. Canadian Center of Science and Education, 2(1). https://doi.org/10.5539/ilr.v2n1p185

Lasisi, R O., Menia, M., Farr, Z., & Jones, C. (2022, May 4). Exploration of AI-enabled Contents for Undergraduate Cyber Security Programs. George A. Smathers Libraries, 35. https://doi.org/10.32473/flairs.v35i.130615

Melaku, H M. (2023, June 30). A Dynamic and Adaptive Cybersecurity Governance Framework. Multidisciplinary Digital Publishing Institute, 3(3), 327-350. https://doi.org/10.3390/jcp3030017

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017, August 7). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://doi.org/10.6028/nist.sp.800-181

Perumal, S., Pitchay, S A., Samy, G N., Shanmugam, B., Magalingam, P., & Albakri, S H. (2018, October 7). Transformative Cyber Security Model for Malaysian Government Agencies. , 7(4.15), 87-87. https://doi.org/10.14419/ijet.v7i4.15.21377

Release of SP 800-160 Vol 2 Developing Cyber Resilient Systems. (2019, November 27). https://csrc.nist.gov/News/2019/sp-800-160-vol2-developing-cyber-resilient-systems

Ross, R R., McEvilley, M., & Oren, J C. (2016, November 1). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. https://doi.org/10.6028/nist.sp.800-160

Ross, R S. (2018, December 20). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. https://doi.org/10.1002/10.6028/nist.sp.800-37r2

Sadik, S., Ahmed, M., Sikos, L F., & Islam, A N. (2020, September 17). Toward a Sustainable Cybersecurity Ecosystem. Multidisciplinary Digital Publishing Institute, 9(3), 74-74. https://doi.org/10.3390/computers9030074

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation. (n.d). https://www.gao.gov/assets/700/694355.pdf

Ministry of Electronics and Information Technology. (2013). National Cyber Security Policy. Government of India. Retrieved from

https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

Maharashtra State Government. (n.d.). Maharashtra Cyber Security Project. Retrieved from https://www.maharashtra.gov.in

Karnataka State Government. (n.d.). Karnataka Cyber Security Policy. Retrieved from https://www.karnataka.gov.in

Telangana State Government. (n.d.). Telangana Cyber Security Policy. Retrieved from https://www.telangana.gov.in

Kerala State Government. (n.d.). Kerala Cyber Security Policy. Retrieved from https://www.kerala.gov.in

Tamil Nadu State Government. (n.d.). Tamil Nadu Cyber Security Policy. Retrieved from https://www.tn.gov.in