Analysing India's Cyber Building Capabilities in the Global South

---

Table of Contents

1. Abstract

This paper dives into India's cybersecurity capabilities in the context of the Global South. It examines the prevalent cyber threats in developing nations, addresses challenges encountered, and dives into policy implications. The study analyses India's current cybersecurity landscape, with a focus on its infrastructure, technological investments, and efforts in human capital development. By analyzing India's cybersecurity policies and comparing them with peers in the Global South, the paper sheds light on policy frameworks and their efficacy. It stresses the significance of public-private partnerships in enhancing cybersecurity, suggesting incentives to encourage greater private-sector participation. The paper identifies regulatory reforms needed to strengthen cyber stability and reveals gaps in the existing regulatory setup. Collaboration and diplomacy at an international level are crucial in tackling cybersecurity issues. The research explores India's engagements on bilateral and multilateral platforms, along with its contributions to global cybersecurity governance. It also investigates potential collaborative opportunities with the European Union to reinforce cybersecurity frameworks. Drawing from these insights, the paper provides recommendations to improve India's cyber capabilities and adapt to a robust cybersecurity environment. In conclusion, it mentions the importance of unified efforts in protecting cybersecurity on a national and global scale.

KEYWORDS: cybersecurity, Global South, cyber threat, public-private partnerships, blockchain.

2. Introduction

Cyberspace holds the potential to profoundly impact human lives by facilitating connections, business transactions, community building, and access to essential services such as healthcare. However, the once envisioned equitable and empowering cyberspace is increasingly being exploited by both state and non-state actors for malicious purposes, including cyber espionage, viruses and malware, denial-of-service and botnet attacks on government servers, cyber assaults on critical infrastructure, cyber warfare (Stuxnet, Estonian cyber-attacks in 2007, Ukrainian Cyber-attacks in 2014 & 2022), and violations of individuals' privacy (Pegasus, Cambridge Analytica).

Digital technology forms the foundation for numerous social, economic, and political development objectives of donor countries and international organizations. Enhancing growth and stability in recipient countries through digitalization and cybersecurity capacity building will be crucial in future foreign policy decisions and government initiatives.

The future of cybersecurity is becoming a crucial element of international relations, emphasizing the growing dependence of nations on digital infrastructure and the internet.

This has led to new power imbalances, the advancement of offensive cyber capabilities by governments, and differing perspectives between liberal democracies and authoritarian regimes.

3. Cyber Threat Landscape in the Global South

3.1 Overview of Cyber Threats

As of January 2024, there were 5.35 billion internet users worldwide, which amounted to 66.2 percent of the global population. Of this total, 5.04 billion, or 62.3 percent of the world's population, were social media users. [1]The Global South is experiencing a rapid increase in internet users, increasing its vulnerability to cyber threats due to insufficient cyber capacity building. Developing countries face challenges in infrastructure, human resources, and expertise, leading to limited capacity-building efforts. Globally, cyberspace has evolved into a crucial high-stakes issue. Since the 1990s, the John Arquilla and David Ronfeldt paper "Cyberwar is Coming"[2] emphasized the importance of controlling cyberspace for military success, elevating it to a national security concern. This has started debates among major powers such as the US, China, and Russia from the global north, each aiming to shape cyberspace to align with their national interests. Countries with low performance in the Global Cybersecurity Index, as shown in Figure 1, are primarily the least developed and developing nations with a significant portion of their population offline. These countries require assistance to enhance their cyber capabilities and tackle cyber threats.

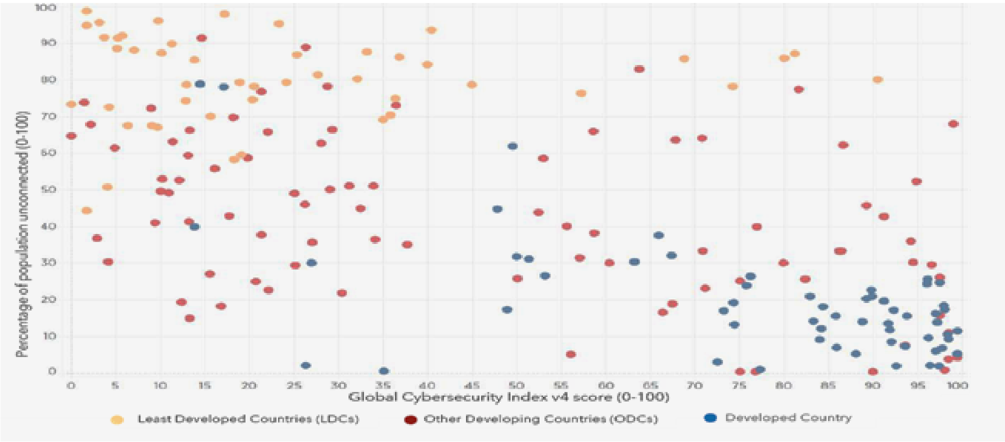

Figure 1 Source: Global Cybersecurity Index, ITU World Telecommunication /ICT Indicators

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/

[2] https://apps.dtic.mil/sti/citations/tr/ADA485253

3.2 Challenges Faced by Developing Nations

The main challenge in cyberspace arises from the lack of understanding of various definitions, regulations, and laws, as well as the prosecution of offenders. Developed nations like the USA, Russia, and the UK are leveraging cyberspace vulnerabilities to assert dominance and influence over the Global South. Developing countries rely on developed nations for infrastructure and security frameworks, granting them access to developing countries' data, which can be misused in various ways. Private commercial companies commonly provide cybersecurity services, yet they might not fully consider the intricate cybersecurity requirements in developing countries. These nations encounter specific cybersecurity challenges due to limitations such as limited resources and inadequate infrastructure.

It is crucial to customize cybersecurity solutions to meet the distinct needs and limitations of developing countries. Collaborating with local experts and organizations in these regions can improve tailoring cybersecurity services to match their particular requirements. To ensure strong protection, it is vital to embrace a holistic cybersecurity strategy that addresses social, economic, and political factors in developing nations.

While cyberspace offers numerous benefits, it also poses drawbacks, notably the absence of physical boundaries. The anonymity provided by cyberspace enables criminals to engage in illegal activities with impunity. Cyber-attacks can hamper the economic progress of developing nations. The borderless nature of cyberspace and its anonymity factor hinder tracking culprits. Therefore, all nations must adopt robust cybersecurity policies to ensure a safe and secure online environment.

In 2012, countries like Pakistan, Egypt, the Philippines, and South Korea ranked in the top ten for hosting compromised computers and initiating malicious activities without consent, underscoring the need for stringent laws to safeguard global cyberspace. As discussed earlier, software, hardware, and control systems are dominantly manufactured in developed countries, leaving developing nations vulnerable. The Stuxnet virus incident[3] is an example of this vulnerability, where the virus took over machines involved in nuclear material production, causing massive disruptions. Instances of Kenya can be seen as it faces significant financial losses due to cybercrimes annually, with an increasing rate of cybercrime. Developing

[3] Stuxnet was the initial cyberweapon to impact physical infrastructure worldwide, targeting Iranian nuclear centrifuges. Consequently, it caused damage and destruction to vital military assets, resulting in substantial disruptions to Iran's nuclear program.

countries often rely on easily accessible templates for network security, making them accessible to cyber breaches.

3.3 Implications for Policy Formulation

In the Global South, various countries have implemented policies for data protection and regulation. Some of the examples are:

a. BRAZIL: The Internet Act (2014) and LGPD (2018) in Brazil focus on enhancing cybersecurity by emphasizing privacy, data security, and legal accountability. LGPD enforces penalties for violations, encouraging compliance. Both legislations emphasize user rights, including consent, transparent data handling, and prompt incident reporting. They require security protocols and governance frameworks, promoting proactive cybersecurity measures. These laws also regulate international data transfers to ensure data protection. Adhering to these regulations not only strengthens data security but also encourages organizations to implement robust cybersecurity practices, contributing to a safer digital landscape in Brazil.

b. PAKISTAN: The National Cyber Crime Policy 2021 marks a significant step forward in Pakistan's cybersecurity domain. Ratified by Parliament on July 27, 2021, this policy demonstrates a proactive stance towards addressing cybersecurity issues. Its approval highlights the government's acknowledgment of the changing digital landscape and the necessity for a holistic cybersecurity strategy. Serving as a guiding principle, the policy steers efforts toward establishing a secure digital environment in Pakistan. Prioritizing prevention, incident response, and legal accountability, the policy aims to strengthen the country's cybersecurity stance. As Pakistan enters the digital age, the National Cyber Crime Policy 2021 sets a promising path, emphasizing cyber resilience and protection against emerging threats.

c. CHINA: China's Cybersecurity Law (CSL), implemented on June 1, 2017, marks a significant milestone in establishing a standardized regulatory framework for cybersecurity and data protection. With a focus on a centralized, state-directed strategy, the CSL aims to harmonize control, security, privacy, inclusivity, and commerce. This policy showcases China's dedication to strengthening its digital infrastructure by adopting a comprehensive approach spanning various sectors. By promoting a consistent regulatory environment, the CSL cultivates a secure digital space while catering to the diverse needs of different industries. China's prioritization of state-led governance underscores cybersecurity as a national imperative, ensuring a cohesive and monitored cyber environment. The CSL not only enhances data security but also highlights China's resolve to navigate the complexities of the digital age with a strategic and unified method.

d. INDONESIA: Indonesia's cybersecurity policies, anchored in the Electronic Information and Transactions Law (EIT Law) and Government Regulation No. 71/2019, carry implications for the nation's digital landscape. While these regulations address offenses and enhance protections in electronic transactions, the limited coverage raises concerns. The EIT Law fails to encompass vital cybersecurity aspects, leaving gaps in safeguarding information, network infrastructure, and the need for cybersecurity expertise. The additional regulation, GR 71/2019, strengthens certain provisions but primarily focuses on cybercrimes related to electronic transactions. Furthermore, Regulation No. 82/2014 from the Ministry of Defence focuses mainly on cybersecurity guidelines for national defense, emphasizing military cyber defense capabilities. Consequently, other regulations are responsible for addressing non-military cyber threats. This highlights the need for a more flexible and comprehensive regulatory framework to efficiently combat various cyber threats, particularly those aimed at Indonesia's critical infrastructure and national security.

4. India's Current Cybersecurity Landscape

4.1 Infrastructure and Technological Investments

India has acknowledged the cyber crisis faced by the Global South and has adopted a unique approach focused on active engagement and collaboration, with a special emphasis on the Global South in cyberspace. The cyber strategy centers around enhancing cyber capacity in Global South countries. The country initiated economic liberalization in the 1990s, simplifying rules to attract foreign investment. While India is becoming more accessible from a regulatory and commercial perspective, challenges persist, such as privacy standards for outsourcing companies. Despite the absence of specific laws on privacy and Emerging Technologies in E-Government data protection, there are indirect safeguards offering sufficient protection to offshoring companies. To combat crimes, India enforces acts and regulations, including the Indian IT Act, Indian Copyright Act, Bharatiya Nyaya Sanhita[4], and Indian Contract Act. The country has witnessed substantial growth in its IT sector and telecommunications infrastructure, driven by the emergence of Next Generation Networks (NGN) to replace outdated networks. The convergence of IT and telecommunications presents regulatory and security hurdles that necessitate careful handling. India's telecom expansion and the rise of IP services and Broadband underscore the need to revisit regulatory frameworks. In response to global cyber threats, India prioritizes securing its ICT infrastructure to support social initiatives like rural empowerment, E-Governance, E-Commerce, and disaster relief. While the United States has the National Infrastructure Protection Plan (NIPP) and National Cyber Security Division (NCSD) under the Department of Homeland Security, India's National Disaster Management Authority (NDMA) focuses on creating a disaster-resilient nation through technology-driven strategies. Enhancing transparency and establishing an organization akin to the NCSD

[4] Earlier known as Indian Penal Code

would enhance India's cybersecurity efforts. Addressing critical infrastructure vulnerabilities requires a comprehensive approach recognizing the interdependence of various sectors.

4.2 Human Capital Development Initiatives

The passage emphasizes the vital role of the Indian government in ensuring cybersecurity within the nation. It outlines various responsibilities undertaken by the government, such as policy development, enforcement of regulations, conducting training programs for capacity building, coordinating incident responses, issuing advisories, and fostering international cooperation. It also delves into the functions of key government entities like the National Critical Information Infrastructure Protection Centre (NCIIPC), Indian Computer Emergency Response Team (CERT-In), National Cyber Security Coordinator (NCSC), and Indian Cyber Crime Coordination Centre (I4C). Furthermore, the passage sheds light on the significant contribution of Indian academia in the field of cybersecurity. It elucidates how educational institutions play a crucial role in cybersecurity education, research endeavors, innovation, and collaborations with various stakeholders. Notable contributions from institutions like the Indian Institutes of Technology (IITs) and other research facilities are highlighted.

Additionally, the passage underscores the involvement of cybersecurity think tanks in India, including the Cybersecurity and Privacy Foundation (CSPF), CyberPeace Foundation, Centre for Internet and Society (CIS), Observer Research Foundation (ORF), Data Security Council of India (DSCI), and India Smart Grid Forum (ISGF). These organizations focus on research activities, policy formulation, leading discussions, and enhancing cybersecurity capabilities through training programs. Lastly, we see diverse initiatives undertaken by the Government of India, academia, and cybersecurity think tanks to bolster cybersecurity through policy frameworks, education, research, and collaborative efforts.

4.3 Public-Private Partnerships

India's advancement in digitalization has been accompanied by a surge in cyberattacks across various sectors, resulting in significant financial losses. Security concerns have reached a critical level in businesses in the United States, with a growing apprehension at the management level due to the complexity and consequences of cyber threats. The financial implications of these attacks, along with the anticipation of data breaches, are pressing issues that need to be addressed. This detailed report was prepared by DSCI in partnership with SEQRITE, analyzing a vast number of malware instances and identifying numerous SEQRITE locations in India. The global shift towards Industry 4.0 has led to extensive digitalization across industries, including the automotive sector, which is facing escalating cyber risks. India is particularly susceptible to state-sponsored threat actors, with government and defense agencies being prime targets. Healthcare providers, manufacturing companies, logistics firms, as well as banking and financial sectors are also at risk of cyberattacks in India. Challenges facing India's cybersecurity efforts include insufficient funding, lack of coordination between states' cybersecurity strategies, and inadequate software auditing by government agencies. Notably, the Ministry of IT's cybersecurity budget in 2015 was less than $20 million, while attacks on Indian websites surged by approximately 500% between 2010 and 2014. The IT Act 2000 allows governments to designate any computer resource affecting critical information infrastructure as a protected system.

5. Policy Framework Analysis

5.1 Existing Cybersecurity Policies in India

Indian Computer Emergency Response Team (CERT-In) handles all kinds of matters related to cybercrime in India. There are no cybersecurity regulations that have been updated in the current year, 2024. The following are the already existing policies undertaken by the Indian Government:

a. Formation of CERT-In in 2004,
b. Information Technology (IT) Act, 2000,
c. National CyberSecurity Policy, 2013,
d. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) in 2017,
e. Data Protection and Privacy Regulations in 2017,
f. National Critical Information Infrastructure Protection Centre (NCIIPC),
g. Cybersecurity Cooperation and International Engagements,
h. Skill Development Initiatives,
i. Sector-Specific Regulations,
j. Cybersecurity Awareness Initiatives

Numerous cybersecurity regulations incorporate measures for transferring data between nations to guarantee the safe and legal transfer of personal information across borders. These provisions are designed to safeguard individuals' privacy rights and ensure adherence to legal requirements during data transmission. In India, the National Critical Information Infrastructure Protection Centre (NCIIPC) is responsible for safeguarding Critical Information Infrastructures (CIIs). The NCIIPC identifies and classifies CIIs, establishing protocols and regulations for their protection.

Through the above-mentioned policies, we have seen that the cyber security regulations that have been implemented throughout the years in the country are very effective and have helped a lot to all common users. In addition, we can learn all the fundamentals of cyber security with the help of many courses designed especially for dealing with this problem.

5.2 Comparative Analysis with Global South Peers

The National Cybersecurity Strategy (NCSS) serves as a crucial framework to assess a country's readiness to safeguard cyberspace. However, its intricate nature, encompassing technology, industry, economics, and defense, poses challenges for systematic evaluation. Analyzing the text provides a new approach to unveiling the abundance of information within NCSS documents. Greger's (2010) research highlights the significance of Computer Emergency Response Teams (CERT) or Computer Incident Response Teams (CIRT) in handling cyber incidents. India, positioned 17th globally, faces digital obstacles despite its progressive government and prominent IT-enabled service sectors. The nation grapples with infrastructure deficiencies, limited digital economic practices, and inadequate cybersecurity regulations. CERT-In managed an impressive 674,000 cybersecurity incidents in the first half of 2022, marking a substantial increase from the previous year. This surge has prompted discussions on establishing national cybersecurity laws and a dedicated ministry, in areas where India lacks structured frameworks. In contrast, most countries, excluding the United States, deploy response teams during cybersecurity incidents. France raises concerns about the lack of clear guidance or assistance for victims, including the public, SMEs, and other stakeholders. While India contemplates establishing a national support system for cyber attack victims, the effectiveness of this initiative remains uncertain. This comparative analysis highlights the urgency for India to enhance its cybersecurity infrastructure, revealing global and regional differences in preparedness and response strategies. Addressing these challenges will be pivotal for India to successfully navigate the evolving digital landscape.

6. Public-Private Partnerships in Cybersecurity

6.1 Role of the Government

Governments are tasked with overseeing and mitigating national security risks, even though they may not directly control privately owned critical infrastructure, which makes up a significant portion of the essential assets in the United States, estimated at over eighty percent. To address this challenge, establishing partnerships between government authorities and private infrastructure owners and operators is a strategic approach to boost the stability and availability of crucial information and communication technologies. These collaborations enable the efficient sharing of vital security information, coordination of incident responses, and insights into infrastructure resilience for the government. Simultaneously, industry stakeholders can access critical threat information and vulnerabilities, enhancing their risk management capabilities. In a recent podcast, Sam Merrell and John Haller from CERT's Resilience Enterprise Management team, along with Philip Huff, Manager of Security and Compliance at the Arkansas Electric Cooperative Corporation, discuss the essential steps required to develop strong public-private partnerships between government and industry. The conversation underscores the importance of these alliances in strengthening national cybersecurity efforts through cooperation, information sharing, and collective risk management.

Governments play a pivotal role in safeguarding their citizens through legislation and infrastructure enhancements, while businesses should align with governmental goals to protect individuals and their data. Raising public awareness is crucial; just as the government issues warnings about road safety during accidents, similar alerts should be issued for cybersecurity threats. These notices can be disseminated through newspapers or radio broadcasts to educate a wide audience on cybersecurity best practices. Improving security measures not only safeguards data but also protects physical infrastructure. For instance, the Stuxnet computer worm, discovered in 2010, disrupted centrifuges in Iran's nuclear program, illustrating the tangible physical consequences of cyber threats. Cybersecurity is a shared responsibility where individuals should be aware of online risks, businesses must enhance security measures, and governments need to enforce relevant regulations. Through collaborative efforts, the impact of cyber incidents can be minimized, emphasizing the importance of cybersecurity.

6.2 Incentives for Private Sector Involvement

Public-private partnerships offer many benefits to both the public and private sectors when it comes to cybersecurity. For the public sector, public-private partnerships allow them to benefit from the expertise of the private sector as well as share resources and information. This creates an environment where both entities can develop better strategies and solutions to fight cyber threats.

For the private sector, public-private partnerships allow them unprecedented access to government and public entities, creating new opportunities to innovate and develop new solutions. Furthermore, private sector companies can benefit from public sector resources such as grants and assistance, allowing them to better invest in their cybersecurity solutions. It allows both sectors to create a collective, holistic approach to tackling cyber threats. By working together, both sectors can create more effective solutions and foster stronger cybersecurity initiatives.

7. Regulatory Reforms for Cyber stability

7.1 Current Regulatory Structure

In a broad sense, privacy refers to an individual's lawful right to choose how much of himself he wants to reveal to others, as well as the information regarding the time, place, and circumstances under which he communicates with others.

Developing countries are facing major cyber threats that can impede their growth in all aspects. Comprehensive cooperation between all stakeholders, industry, private sector, state, and citizens, and international coordination, can lead to a safer and more secure cyberspace, especially for migrants to ICT, as he said in his speech in 2020 in New Delhi in the Republic Day. This will allow the government the will to adopt new laws, regulations, and policies on information and data exchange and investigation for maximum social benefits.

7.2 Identified Gaps and Challenges

To effectively battle the growing frequency and severity of cyber threats, organizations must prioritize adopting strong mitigation and resilience methods. Businesses that remain proactive and alert can better protect their sensitive data and vital systems from potential breaches and attacks. Embracing an integrated strategy that includes regular security assessments, personnel training, and cutting-edge cybersecurity solutions will allow firms to stay ahead of cyber threats and mitigate their effects. We need to remember that investing in cybersecurity is about more than simply protecting your data; it is also about ensuring your reputation, consumer trust, and overall business continuity in an increasingly digital world.

National Crime Records Bureau reports cases for publication of sexually explicit content online are increasing by 110% from 6,308 to 3,076, with a total of 306 cybercrime cases registered against children in 2019 increasing to 1,102 cases in 2020:

a. [5]Ladies and Children – confront cyber stalking which is online badgering, an extension of cyberbullying leading to badgering, torment, physical dangers, stigmatizing to spilling private information or morphed photographs of casualties or data to hurt the notoriety of ladies, Online Sextortion, circulating delicate fabric on the web in request of looking for sexual favors coming about as online mishandle, Morphing of photos ladies, youthful observing clueless ladies or children in changing or toilets, Online Child Preparing to mishandle them and Computerised Assault embeddings objects or human parts separated from penis within the vagina, ass or mouth of casualty mightily without consent.
b. Senior Citizens – face Shopper phishing and online fakes, these sorts of cybercrimes which are unlawful get to to their individual secure information through computer

[5] https://ncrb.gov.in/

systems, online or telecaller fakes, character robbery to get financial picks, fake charity commitments, Life protections/ reserve funds, sentiment fakes and vandalism.

8. International Collaboration and Diplomacy

8.1 Bilateral and Multilateral Engagements

Governments across the globe are striving for international cooperation to achieve their cybersecurity objectives through various forums and agreements. However, reaching a consensus on multilateral agreements can be challenging, especially when implementing them across decentralized cybersecurity organizations. While regional organizations offer flexibility, they may need more enforceability. The cybersecurity initiatives of the Shanghai Cooperation Organization, which emphasize state sovereignty, could potentially control cyberspace and raise concerns about freedom of expression, contrasting with the multistakeholder model and posing a dilemma for global collaboration and cybersecurity standards. The lack of clear definitions highlights the difficulty in establishing universal cybersecurity norms and raises issues regarding individual liberties.

The International Cybersecurity Cooperation Dataset (ICCD) is a valuable resource for researchers and analysts interested in international cybersecurity accords. Rather than focusing on countries or organizations, the dataset concentrates on individual agreements, providing comprehensive information in an accessible format. It categorizes agreements into bilateral and multilateral/multistakeholder sections, facilitating detailed comparisons between these approaches and helping researchers identify trends and relationships in international cybersecurity cooperation.

In analyzing bilateral agreements, the dataset considers factors such as the political gap between participating nations, shedding light on the political dynamics influencing cybersecurity collaboration. On the other hand, multilateral/multi-stakeholder agreements are evaluated within a broader framework that acknowledges the diverse political systems involved. Researchers can use the dataset to assess how different agreement types effectively tackle cybersecurity challenges. By incorporating relevant variables and metadata, the dataset enables a thorough examination of how these agreements impact cybersecurity practices, information sharing, and collaborative endeavors. Ultimately, the ICCD enhances understanding of bilateral and multilateral/multi-stakeholder strategies, facilitating well-informed decision-making in international cybersecurity cooperation.

8.2 India's Role in Global Cybersecurity Governance

India's global cybersecurity governance strategy emphasizes practicality and subtlety, steering clear of aligning with ideological factions. Amid the polarised discussions on cybersecurity norms at the UN, India positions itself as a crucial "digital decision-maker" from a neutral standpoint. Viewing cybersecurity as a top strategic priority, India concentrates on securing critical infrastructure and bolstering cybersecurity capabilities. However, there is limited coordination between bureaucratic bodies like the Ministry of External Affairs (MEA) and the Ministry of Electronics and Information Technology (MeitY), with cyber norm negotiations not being a primary focus.

In the multi-stakeholder tech policy landscape, involving civil society, academia, media, and the private sector, these entities play a passive role in shaping India's global cybersecurity stance. This approach grants the government flexibility in decision-making, particularly in addressing immediate strategic and security requirements. Rather than engaging in ideological debates, India showcases leadership globally by sharing successful domestic practices and proposing practical models like the "Digital Public Infrastructure."

India's nuanced, results-driven strategy, coupled with its focus on tangible outcomes, positions the nation as a significant player in the evolving field of global cybersecurity governance. By advocating for the Global South's interests and engaging in non-controversial issues aligned with its objectives, India contributes to shaping cybersecurity norms and fostering global collaboration.

8.3 Taking strength from the EU

It is crucial to develop a new vision and strategy for cybersecurity within the EU at this moment for the key reasons:

a. The increasing connection of critical services and everyday objects to the Internet has led to a rise in sophisticated cyber-attacks. Success in the Green Digital transformation, a top EU priority, relies on integrating security into all planned investments to establish trust in the technology.

b. The global cyberspace has become a battleground for geopolitical influence, challenging the concept of an open global Internet and international norm-setting frameworks.

c. The pandemic has accelerated our reliance on digital tools and services, making it essential to invest significantly in cybersecurity. To ensure strategic autonomy, Europe must lead in secure technology development throughout the digital supply chain.

d. The EU Cyber Shield comprises AI-driven Security Operations Centres to detect cyber threats early. It includes a Joint Cyber Unit for collective response and European solutions for global Internet security. The strategy involves enhanced cyber dialogues, a UN Program of Action, and a robust EU cyber diplomacy toolbox. Additionally, there will be an EU External Cyber Capacity Building Agenda and an interinstitutional Cyber Capacity Building Board to enhance external cyber capacity-building efforts.

e. Investments in the entire digital technology supply chain, aimed at facilitating the digital transition or addressing related challenges, are projected to reach a minimum of 20%, equivalent to €134.5 billion, of the €672.5 billion Recovery and Resilience Facility comprising grants and loans.
f. Cybersecurity funding is planned under the Digital Europe Programme in the EU funding for the 2021-2027 Multiannual Financial Framework. Additionally, cybersecurity research funding is anticipated under Horizon Europe, with a particular emphasis on supporting SMEs. Altogether, this could total €2 billion, in addition to investments from Member States and industry.
g. The European Defence Fund (EDF) will support European cyber defense solutions as part of the European defense technological and industrial base. Cybersecurity is integrated into external financial instruments to aid partner countries, particularly through the Neighbourhood, Development, and International Cooperation Instrument.

9. Recommendations

Given the importance of cybersecurity in today's digital landscape, organizations, and governments must collaborate to enhance defenses and safeguard sensitive data, we should prioritize implementing strong mitigation and resilience strategies to combat cyber threats effectively, and we can use some of the regulatory reforms ;

a. Utilize Blockchain Technology to Boost Data Security: Blockchain provides decentralized and unchangeable ledgers, enhancing resistance against tampering and unauthorized entry. There are already existing laws in India for the same but they haven't been up to the mark.[6]

   Section 17 of the Personal Data Protection Bill might need adjustments to specify blockchain as the preferred method for ensuring the security and confidentiality of health data. To put this into action, the Ministry of Health and Family Welfare could partner with standardization bodies to develop guidelines for utilizing blockchain in healthcare data management. It could be made compulsory for healthcare providers to document patient consent on a blockchain ledger for each data transaction in line with the Electronic Health Records Standards for India. Furthermore, hospitals and clinics that follow blockchain standards for storing and sharing patient health records could be eligible for tax benefits. The Union and State Ministries of Health, in collaboration with the Indian Council of Medical Research (ICMR), are tasked with overseeing the necessary technological advancements. By integrating blockchain technology, India's healthcare sector can enhance data security. Initially, a collaboration between healthcare and technology experts is crucial to establish clear regulations. Following this, pilot programs could be initiated in hospitals to demonstrate the benefits of blockchain. Educating healthcare professionals about

[6] Information Technology Act, 2000, Medical Council of India Act, 1956, Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002

blockchain is vital, and a dedicated team can ensure compliance and monitor regulatory adherence. Additionally, offering incentives such as tax benefits to hospitals that implement blockchain can safeguard patient data and improve healthcare services for all.

b. Promoting Cybersecurity Insurance for Businesses: Advocate for businesses to consider investing in cybersecurity insurance policies to reduce financial losses linked to cyberattacks and data breaches. Such insurance can cover legal expenses, data recovery costs, and reputation management fees. IRDAI oversees insurance in India and likely has guidelines for cybersecurity insurance. These can be adapted for healthcare. SEBI regulates financial markets and may offer insights into cybersecurity practices. Though not healthcare-specific, SEBI's guidelines can inform cybersecurity insurance strategies.

Implementing a comprehensive cybersecurity strategy in India involves several key elements, including:

I. Legislative requirements and government directives
II. Financial incentives and industry cooperation
III. Innovative insurance solutions and risk assessment tools
IV. Incident response strategies and legal advocacy

Advocating for updates in laws, such as the Information Technology Act, to mandate cybersecurity insurance for businesses handling sensitive data provides legal backing and promotes proactive risk management. Collaborating with government bodies to establish clear guidelines and offering incentives like tax advantages encourages the adoption of cybersecurity insurance. Partnerships between industry associations and regulatory agencies facilitate knowledge sharing through workshops and seminars. Tailored cybersecurity insurance plans developed in collaboration with insurers cater to diverse business needs, while risk assessment tools empower strategic decision-making. Well-defined incident response plans, created with experts, help mitigate financial losses and protect reputation. By implementing these measures, businesses in India can enhance their cybersecurity defenses, mitigate risks, and cultivate a secure business environment.

c. Establishing a National Cybersecurity Task Force: In India, the Ministry of Electronics and Information Technology (MeitY) plans to establish a cybersecurity task force with a focus on protecting digital data from cyber threats. This task force will collaborate with key sectors such as energy, transportation, and telecommunications across the country. It will consist of cybersecurity experts, government officials, industry professionals, and law enforcement officers, under the supervision of MeitY. Together, they will develop strategies aligned with the country's cybersecurity goals to strengthen online data security. Adequate government funding will support skill development, system improvements, and fair compensation for team members. By fostering collaboration between the public and private sectors, the task force aims to encourage information sharing and joint actions against online risks. The task force's effectiveness and structure will be guided by specific government directives and granted authority. The potential for the newly formed Cybersecurity Task Force within India's Ministry to enhance effectiveness surpasses current initiatives across various fields.

The task force can provide specialized guidance to critical sectors such as energy, transportation, and telecommunications to help them defend against cyber threats specific to their operations. It can establish a system for rapid information exchange on cyber threats among governmental bodies and businesses to ensure prompt responses. By promoting cooperation across sectors, it can streamline responses to cyber attacks to reduce their impact. Moreover, it can focus on educating individuals in all sectors about cybersecurity to increase awareness and preparedness. Additionally, it can advocate for new policies and collaborate with other countries to strengthen global cybersecurity efforts.

By implementing these improvements, the Cybersecurity Task Force can significantly enhance India's cybersecurity readiness and resilience. It can assist organizations in understanding and complying with cybersecurity regulations and standards by guiding best practices and risk mitigation strategies. It can support regulations and policies that boost cybersecurity resilience, innovation, and collaboration at national and international levels. It can coordinate responses to incidents across sectors, enabling swift and coordinated reactions to cyber events to minimize their impact on critical infrastructure and services. It can establish channels for organizations to report cyber incidents and conduct post-incident analyses to identify trends, vulnerabilities, and crucial insights for future prevention.

d. Public-Private Partnerships :

Public-private partnerships can work towards the important goal of improving cybersecurity in many ways. Here are just a few examples of the ways public-private partnerships can facilitate better cyber defense:

I. Data Sharing – Private sector companies can share timely cyber threat information and intelligence with public sector entities and vice versa. This allows for a more comprehensive understanding of the nature of cyber threats and can help entities to develop better defensive strategies.

II. Assessments & Audits – Public-private partnerships allow for joint assessments and audits of the measures that the public and private sectors have implemented, allowing both sectors to identify gaps or weaknesses in their current cybersecurity strategies.

III. Incident Response & Emergency Management – Public-private partnerships allow for more effective and coordinated incident response and emergency management plans, allowing for a better response to cyber emergencies.

IV. More Resources – Joint public-private partnerships provide access to more resources, both financial and personnel than would otherwise be available to either the public or private sector alone.

Overall, public-private partnerships offer the opportunity for valuable collaboration between public and private sector entities, with many resources and strategies combined to improve the cybersecurity of both sectors and better protect against cyber threats.

10. Conclusion

In conclusion, the evolving cybersecurity landscape requires a multifaceted approach to protect individuals and nations. Practices like strong and unique passwords, two-factor authentication, regular updates, and cautious online behavior are essential for personal cybersecurity. The Government of India has taken commendable steps, including awareness campaigns, collaboration with experts, and capacity-building initiatives. Challenges remain, like balancing privacy and security and keeping pace with fast-changing technology. As India tackles these challenges, cooperation between citizens and the government is vital for a secure online environment. The Government has shown dedication through public awareness campaigns and partnerships, leading to successful crackdowns on cybercrime. Balancing privacy and security and keeping up with technological advancements pose challenges. International regulatory alignment is key for a robust cybersecurity framework, encouraging collaboration and regulatory consistency. As India moves forward, a unified approach at personal and governmental levels is essential to navigate the cybersecurity landscape, ensuring a secure digital environment for the nation.

11. References

1. (n.d.). Wikipedia. Retrieved March 25, 2024, from https://www.researchgate.net/publication/311188828_Cyber_security_capacity_building_digitalization_and_the_Global_South
2. Wikipedia. Retrieved March 25, 2024, from https://www.reddit.com/r/IndiaSpeaks/comments/oaeufc/india_jumps_to_no10_on_global_cyber_security/
3. Wikipedia. Retrieved March 25, 2024, from https://arxiv.org/ftp/arxiv/papers/2303/2303.13938.pdf
4. (2023, February 27). India has Started to Emphasize the "Global South" | List of Articles | International Information Network Analysis | SPF. Retrieved March 25, 2024, from https://www.spf.org/iina/en/articles/toru_ito_05.html
5. Ahmar, M. (2023, April 20). *Cybersecurity: How does India perform on the global stage?* ET CIO. Retrieved March 25, 2024, from https://cio.economictimes.indiatimes.com/news/digital-security/cybersecurity-how-does-india-perform-at-the-global-stage/99628852
6. Author, G., Parasnis, S., Maitra, R., Mathi, S., & Johari, S. (2024, February 3). *How Does India see the global cybersecurity norms debate?* MediaNama. Retrieved March 25, 2024, from https://www.medianama.com/2024/02/223-india-global-cybersecurity-norms/
7. *Distinguished Lectures Details*. (2018, April 4). Ministry of External Affairs. Retrieved March 25, 2024, from https://www.mea.gov.in/distinguished-lectures-detail.htm?743

8. *India And Global South, Significance, Challenges, Initiatives*. (2023, December 23). StudyIQ. Retrieved March 25, 2024, from https://www.studyiq.com/articles/india-and-global-south/

9. *INDIA CYBER*. (n.d.). Data Security Council of India. Retrieved March 25, 2024, from https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

10. *Multilateral Agreements to Constrain Cyberconflict*. (n.d.). Arms Control Association. Retrieved March 25, 2024, from https://www.armscontrol.org/act/2010-06/multilateral-agreements-constrain-cyberconflict

11. *Placing India's cyber security in the global scenario: The Global Cybersecurity Index (GCI) 2020.* (n.d.). Indian Institute of Public Administration. Retrieved March 25, 2024, from https://www.iipa.org.in/cms/public/uploads/496841643884987.pdf

12. Saraswat, V. (n.d.). *Cyber Security*. NITI Aayog. Retrieved March 25, 2024, from https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

13. Singh, A. (2022, November 6). *(PDF) Cyber Crime, Regulations, and Security - Contemporary Issues and Challenges*. ResearchGate. Retrieved March 25, 2024, from https://www.researchgate.net/publication/365172688_CYBER_CRIME_REGULATION_AND_SECURITY_CONTEMPORARY_ISSUES_AND_CHALLENGES