International Journal of Education and Science Research Review
Volume-11, Issue-5 Sep-oct-2024 E-ISSN 2348-6457
(Peer-Reviewed, Open Access, Fully Refereed International Journal) P-ISSN 2349-1817
www.ijesrr.org Impact Factor - 7.02 Email- editor@ijesrr.org

INDIA'S APPROACH TO CYBER DIPLOMACY: NAVIGATING GLOBAL CHALLENGES IN A DIGITAL AGE

Fathimath Suhara Kadakkadan
Research Scholar, Glocal School of Art and Social Science
The Glocal University, Mirzapur Pole, Saharanpur (U.P).
Dr. Waseem Ahmad
Research Supervisor, Glocal School of Art and Social Science
The Glocal University, Mirzapur Pole, Saharanpur (U.P).

ABSTRACT

In the modern age of information, technology has become a cornerstone of global systems, influencing finance, trade, commerce, education, and other critical sectors that rely on efficient information exchange. Information and Communication Technology (ICT) has emerged as a driving force in the global economy and a vital tool in domestic governance, enabling nations to deliver better services and facilities. Even developing nations are embracing ICT, with applications ranging from smart cities to smart classrooms.Security, a core aspect of national politics, traditionally focused on military, weapons, and diplomacy, has expanded in the 21st century to include technology as an integral component. This shift reflects the universal role of technology, utilized not only by governments and individuals but also by terrorist organizations. In this era, technology is increasingly regarded as a powerful weapon, even by adversarial states. India has witnessed its share of challenges, from financial fraud and data breaches to cases of cyber harassment, all facilitated by digital platforms. Moreover, the borderless nature of cyberspace has enabled hostile entities and anti-social groups to exploit social media for spreading anti-national propaganda. While the indispensability of technology cannot be overstated, the growing dependence on it raises critical security concerns. Addressing these challenges is imperative, yet solutions remain elusive. IT companies are striving to enhance cybersecurity measures, but broader efforts are required at both national and international levels. Strict cyber laws are urgently needed to safeguard nations, while international cooperation and the development of robust cyber diplomacy can serve as partial remedies to this complex issue. Although such measures may not provide a definitive solution, they are essential steps toward mitigating the risks of cyber threats in today's interconnected world.

Key words: Cyber-security, International co-operation, laws, diplomacy, Nation-State, Politics, Technology,

1. INTRODUCTION

Cyber technology stands as one of the most significant advancements in our increasingly interconnected world. A single application can facilitate global interactions from within our own spaces. The entire globe is linked through cables and data, with network systems instigating transformative changes across economic,

political, and social landscapes. Computers, mobile devices, data, and applications serve as the backbone of this technological era. The post-globalization period is often referred to as the age of technology, characterized by the ability to connect the world through both wired and wireless means. Undoubtedly, the cyber age has enhanced comfort in daily life while raising expectations for further conveniences, leading to ongoing research and development in this field. Advanced technology has become a routine aspect of everyday existence, with civil society embracing it to improve quality of life. Additionally, politics has adopted technology as a governance tool, with significant initiatives focused on enhancing service delivery systems. Digitalization has refined government policy formation and execution, fostering a more people-centric approach to governance. In India, this evolution is often termed Digital Democracy. In the realm of politics, security is paramount. National interests hinge on effective security measures, and the complexities of international relations have intensified. The technological revolution of the post-globalization era has heightened reliance on technology, consequently increasing cyber security risks. Frequent incidents of cybercrime complicate the international political landscape. Merely enhancing cyber capabilities is insufficient to mitigate security threats; cyber security has emerged as a critical component of national security. The world faces ongoing security challenges due to the growing vulnerabilities associated with technology. The adoption of borderless and unfenced communication systems has propelled development to unprecedented heights, yet this expansive cyber space poses significant challenges to national security in international relations and domestic politics alike. The issue of cyber security has become a global concern.

Cyber Security and Politics

Cyber space has also used to disturbed the domestic political peace of a nation. Hate speech, communal violence, disruption of privacy are the main areas for concern. Political parties for the sake of their narrow political interest utilizing the media platform. Public sentiments some -times working based on post truth factors. Catchy tagline attracts millions of viewer without knowing the actual truth. Terrorist activities also fabricated and executed in this way. Using cyber space without government vigilance is a good example of liberal democratic government order, misusing this is an example of misguided civil society. Observing these issues manifest that government initiatives for improve the system , empowering people, ensure socio-political and economic growth, improving the innovation system, development in a sustainable nature through technology has no alternative except strong cyber security policies.Cyber security is an operation of protecting computer software, mobile device, data, electronic system and network system from hostile strike. In cyber security the major objective is the development of protection measures from any unwanted encroachment or design a technology to assured safety of networking system from surface threats. Cyber security is now an important security aspect for domestic politics and international relations[4]. National politics is now technologically dependent. Holistic development is an essential aspect for national politics and development, which is now refine and enhanced with the support and application of Information and Communication Technology. Global political system also attached in comparatively. Therefore Technology is dominating factor in contemporary world politics[7].

Types of cyber security

1. Security on communication system

2. Security of Cloud.
3. Develop tricky security infrastructure
4. Software security

National Security implies that protection of nation from any kind of external threats and justifying the application of force[6]. According to Harold Lasswell "the distinctive meaning of national security means freedom from foreign dictation"[17]. After the cold war with the emergence of new nations, issues of national security took new dimensions because of the end of bipolar system. Besides the two super powers, other nations are also in rate race for attained rank the of global super power like China and Russia. The paramount factor has risen after the World War second when the issues took place about the differences between North and South. Northern part of the globe is the combination of economically developed countries and Southern part is least developed. International political Economy has emerged as a sub-discipline of International relations to discuss the issues of poverty, inequalities and development among the states. Therefore, the definitions of security for the development nations are not now similar for the developing nations. For the developing nations national security is not only the defense and military security but social security also. National Defense College of India defines "National Security is an appropriate and aggressive blend of political resilience and maturity, human resources, economic structure and capacity,technological competence, industrial base and availability of natural resources and finally the military might."

The transformation of world politics, conveyed the Security aspects into boarder angle. Concept of Security shifts from its traditional militarily domain to other areas including the technology for national human and economic development and better Social security. The important parts of National Security are:

- Political security
- Economic Security
- Human Security
- Environmental Security
- Cyber security.

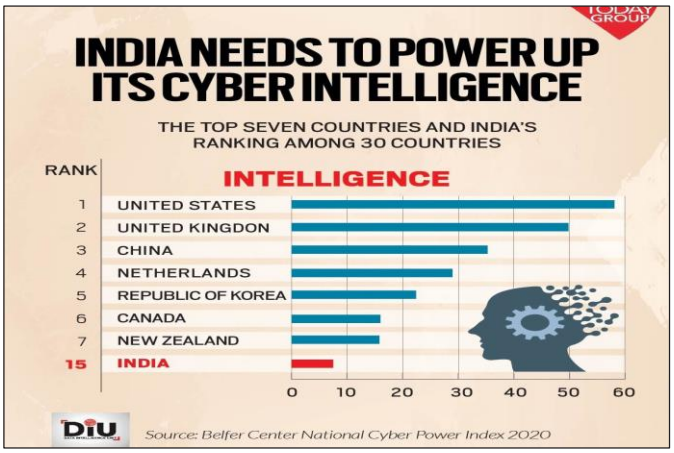

Fig. 1: Manpower availability in the field of Cyber and IT Security (Copied from India Today)

Cyber Security in India

To address the complexity of Indian security matters, the Ministry of External Affairs explained that "India's external environment remains complex and challenging. We are living in a world in transition, not just in geo-political terms-covering trade, financial flows, financial trends, demographic changes and participation in a globalized economy. Globalization comes with its concurrent global threats- terrorism, proliferation of weapons of mass destruction, piracy and other threats to maritime security, environmental challenges, threats to space and cyber security and access to water, among others." Global politics is depended now in Information and Communication Technology. Countries like United States of America and China are holding the top position in this field. Past history of several attack on cyber space has raised many question relating to cyber security. Present dependence on cyber world is increasing the situation further complicated. Application based global economic system can be destroyed with a help of single touch. India's global ranking on Information and communication Technology is not in a higher position[12]. As Fig. 1 has demonstrate that USA holds the 1st ranking followed by united Kingdom and China but gradually India is improving in the Technological field. India has now known as Digital India. This process of digitalization constructs strong economic relation globally and builds domestic government activities more trouble free. Emphasis has been giving mainly on public service sector, where citizen will entitle the effortless services and will ensure the transparency. India is now not totally well equipped in technology for domestic sector but application of technology is also an important strategy for India in military field. India's security challenges are very troublesome situations from very beginning of the inception of the country. India's economic prosperity and military strength helps the nation to fight with all odds. The goal of cashless transaction, better known as digital transaction to provide corruption free maximum services generate cyber risks every day. Even the digitally advance countries with high percentage of literacy has been suffering after their declared digital dependency. India is also not exception.

India has faced numerous security challenges from her neighboring countries[18]. Pakistan is always a great threat for India and interrupted the every effort to establishing peace full relation with the neighbor countries

and an uninterrupted functioning of domestic politics by Influencing the radical fundamentalist culture and also fuelling anti national hate speech with the help of Social media. The Cross border terrorism and proxy war initiated by government of Pakistan has already established. Now instead of using heavy artilleries Pakistan is planning to jeopardize the whole system with Hackers. Cyber Attack is now a matter of serious concern[20].

India's another security threat is China[15]. From the Chicken neck corridor China is only 4 hours distance from India by road. But China except some minor military confrontation avoids hard power. China is expert in using its financial diplomacy and cyber space to sabotaget he enemy nation. China's dis-trustful relation with neighbors and their growing cyber capacity is creating huge security threats for India, especially soft attack for example cyber attack. India has recognized 261 percentages of cases related with cyber crime has increased in last one year. Chines Cyber department's different bureau are researching since many years how to use ICT as a tool of soft weapon. Without hampering single life which can collapsed the whole system. One report has estimated that by 2030 China becomes a Cyber Super Power in AI.

India loosed the battle of cyber attack in many times due the lack of knowledge in proper application and mishandling the technology on computer and poor awareness on operation[2]. Complicated and advanced cyber strikes are coming from well organized terrorist groups, state sponsor's hackers groups who has engaged for spying and developing technics to derailed the whole IT system of the nation or targeting particular corporate house for those purpose to demand ransom. Corporate sectors are failed to play a definite role to stop these kinds of attacks. Recently huge number of cases are pending in different police stations , majority of them are connected with financial fraud and violation of right to privacy or sexual hassle.

In cyber security index, India ranked 37 in 2020. The Week news desk reported in January 2021 that Cyber Security is very common and India near about 11,5,000 incidents of cyber attacks were traced and outlined by Indian Cyber crime experts. Energy sectors, banking sector, telecommunication sector, medical labs,air lines industry, railway system, hotel business are the target of cyber criminals. To deal with the challenges of Cyber security the only measure is protection. Total military system can collapsed through the use of single computer key. Development of Strong counter security strategy is urgently need. Critics are against to adopting the counter attack because it is against the policy of national sovereignty and democratic values. But whether breach of morality for the sake of national interest is permissible or not it istill a debatable issue. Dealing with unknown-unseen enemies created the situation difficult. This is quite untroubled to dealing with the local pettycyber crime. Cyber space when has used with an objective to immobilize the national activities then it is working as a weapon. It is now known fact that non-state actors played crucial roles in present world politics. These non-state actors are emerged due to create monopoly of the rich nations over the other. Growing importance of non-state actors are increasing the risk of security from unknown organization because of their easy access of national territory. Now Cyber space is also considered as non-state actor and the technology is the driving force of it. Victims of the cyber crime and cyber terrorism are mostly developing countries. Digitalization is the popular demand of the policy makers without knowing the maturity level of civil society. People become trapped under the cyber-crime web. But because of advantages of technology, government bound to promote the maximum use of technology.

Cyber area allowed friendship and hostility both. Fully digitalized globalized world actors are empowered to utilize technology for their financial development and negative use can paralyzed the whole system at the same time. Cyber criminals are targeting single entry but operating on larger number of victims. Dark Web is very common word in this regard. Cyber criminal's basic objective to rob the database, for

instance intellectual data, professional data,occupational data, data related to trade and commerce, personal information etc.[11]. Main motive is financial gain. These Cyber criminals when are operating their activities for personal interest or any other related psychological reasons is not created threat for a nation's security as a whole but when it has been working by the instruction from any nation's top authority then it is created havoc threat for national security. Politically influenced cyber criminals are the real threat for a country. The politically hacktivists groups are using the dark web to attacking the different government sites, stealing money from financial institutions for funding their militant groups and indoctrinate their ill ideology through the social media. They are using websites as safe passage for spreading their propaganda. Rioting, different of violence activities,stimulate young generation for joining their groups are the basic motto of these groups. To disrupt the national digital functions the common actions are computer virus generating, data beaches, denial of particular services etc. In Kashmir and North East India has been experiencing these kind of issues since long time. National Security Agencies have collected numerous prove that how the radical groups are exploiting the technology for their ambitions. Even world terrorist organisations are applying technology for their financial flow like hacking,demanding ransom, stealing data. This trend leds politics towards the new idea of warfare, that is the cyber warfare[19].

And the arms are better technology and strong cyber policies. There is debate over the word of Cyber- War, the reason is that absence of face to face retaliation. Most of the cyber attacking cases retaliation is missing. International co-operation is urgent necessity in this regard. Cyber-war treaty is also an important initiative from future security perspectives[5]. It is clear that non-state actors played a vital role in international politics to secure their host nation's economic interest so denial of using cyber space as their national interest is not possible. National politics demands increasing of resilience in armature. Militarization of cyber space can be a best answer for counter attack. Government of India now put emphasis over the mechanism for stronger Cyber Security. The Security agencies are identified the stable links between the local terrorist organization with the international terrorist groups. The local groups are working on regional base but helps to funding the international organizations. In a conventional war it's not too difficult to identify the enemy but in case of cyber attack, identification is not an easy task. The bigger challenges of cyber space are in the area of economy and security. India has already experienced. Cyber Security forum and focus in India is showing in Fig. 2.

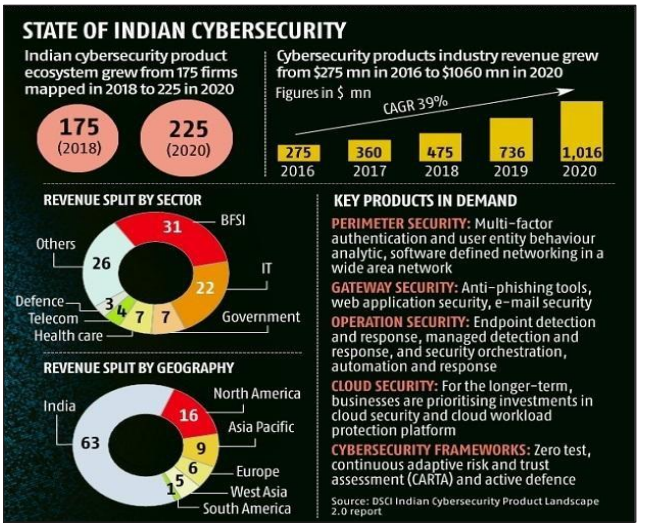

Fig. 2: Cyber Security Sectors, key product demand (*Source:* Business Standard)

This is the details of India's present position on Cyber Security. This image shows that how India splitted the funds in different sectors to ensuring the Cyber security. In recent past Pakistan sponsored cross border terrorism, Chinese encroachment of Indian territory are raising the security threat repeatedly. Accordingly the cyber attack can not be unexpected. Exchange of information by the cyber space can be utilize to fulfill the unlawful and unethical purposes by the across the enemy state and non-state actors. India has developed the National Cyber Security Policy. The ambition is that to preserve and encouraging the computing protection and building trust in technology. It is urgent to identified the mechanism to curb the damage possibilities expecting from cyber space with a team work and the members are people, policy and technology[21]. Ministry of Communication and Information Technology of India declared the basic objectives of Cyber Security. Primary task is to build protected cyber eco-system which will be produce proper confidence in IT sector and will increase people's trust in IT for financial sectors in near future. Create a mechanism for every seconds observation on national cyber space. Indian External Affairs Minister S. Joysankar has stated in the Melbourn Quad Summit, 2022 that "India is looking at a holistic Cyber Security policy that will cover various verticals of potential attacks or situation, both external and external, as it evaluates the policies ruled out by the United Kingdom and Australia, people familiar with the matter"[22].

India has succeed the plan of cyber-security in an innovative way. In India the techno stakeholders are government of India, civil society, private sectors, academic world and international political field and the cyber security researchers. Domestic Minister of External Affairs, Prime Minister Office (NSA)are the sub-branch of government of India. For successful working on the security field some technical co- operations are essential from Authorities as CERT and NCIIPC, from domestic area developing molality, ethics and determines the weaknesses of the protection measures. Fortune of this approach is very much depending on international co-operation with domestic politics. Some legal policies also incorporated within the security commitments in particularly strong IT laws, introduction of Data protection Bill along with inclusion of Technology safe guard related acts in the statute book of India and inclusions of such safety cap in International Laws also. The expecting benefits of the Government initiatives have different dimensions[23].

These dimensions are:

- *Geo-political:* Identify the threats and stabilize it.
- *National-Sate:* Build security from financial hazards, preserving of complicated information framework, Preventive measures for electoral process.
- *Civil:* Concentration on virtual economy, expansion of computerized structure.
- *Personal:* Safe keeping of digital system, Guidance for safety from commercial duplicity, preservation of private information from violation.

The major advantages of the government initiatives are Attributions of Cyber attacks or deterrence, Existing talent in the country, Lack of awareness (institutional and individual lavel), Lack of international consensus, Balancing cyber security with privacy. News Paper The Hindu reports in December, 2021 that according to a Parliament report at-least 26,000 India websites were hacked in last few months. The news agency also reported that the Computer Emergency Response Team identified 17,560 in 2018, 24,768 in 2019, 26,121 in 2020 and 25,870 in 2021 are the total reported cases of Indian Website hacking. Fig 3 is showing the global scenario of cyber crimes.

India has been progressing in a good manner to manage the security threats. Like creating a technical mechanism to early detection of upcoming threats[10]. Preparing a team for which will work for twenty- four hours nationwide to produce emergency services and also will work for better facilities. A strong approach is important to deal with crisis of technology because it is related with public safety and national safety both. E-Governance is now a key of national development programmes. To ensure people's best participation and involvement in the political process, E-governance is an essential tool and these tools are based on technology, hence risk are there. Therefore, government should initiative to build a crisis management team to control the cyber emergency to uninterrupted flow of public service programmes thorough the help of technology[14]. Make this plan success it is crucial to employ maximum experts.

Last few incidents and new incidents of breach of security in cyber space, people lost trust. Government programme implementation can use as antidote of this problems.

Fig. 3: Cyber Security scenario in different countries (*Source*: Aegonlife)

Security improvements programme shall be organise under the ages of Research and Development wing. Research and Development wing shall be courage for developing cost effecting, detect some pure and original security gel so wider area would be cover, would be helpful national purpose and marketing for business purpose. Private – public joint partnership work will also produce some positive results in this area. Academic society of the country should be involved in this purpose too[13].

The present problem of cyber space and its intensity, International political world understands that they are not safe anymore. It is urgently needed a strong global initiative to tackle the present cyber security problems. Office of Drug and Crime of United Nation Organization has been taking about international response after realizing the complexity nature of the problems."General Assembely resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8, the Global Programme Cyber Crime is mandated to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance"[24]. BRICS member states in their summit in 2017 discussed the challenges of economic co-opration where they found the cyber security is an issue of treat[16].Another initiative has taken from the platform of "Council of Europe". The Cybercrime Convention has been discussing about the building of strong legal framework and given emphasis over the international co-operation[25]. Cyber Diplomacy could be a vigorous step for handling the tricky and difficult nature of the Security. India assumes heavy security threat from Pakistan and China but the region of South Asia is not secure[5]. International Political platform should find out the solutions to deal with the hurdle of fighting with unseen enemy. In majority times nations have faced the proxy war,where cyber-space is an useful weapon attack, to deal this kind of security environment diplomacy could be an effective tools. Developing countries like India, who are economically booming the world market are always facing cyber-attack frequently to jeopardize the whole system without a single living casualty. Therefore international organizations, nation-state and

Private organizations should function collectively and collaborately, Cyber Diplomacy might be a strong step. India definitely take steps about the cyber diplomacy with the neighboring states like Pakistan and China, from where country expects maximum security threats[9]. Fig. 4 has defined India's cyber security plan accurately regarding manpower development with academic programs, training and skill development.

Fig. 4: Cyber Security skill development and plans (*Source:* Digital Learning Magazine)

CONCLUSION

In the final analysis, it can be said that nations such as India are technologically immature, particularly when it comes to applications. Many computer companies develop their products in a very complex way for safety reasons due to the growing awareness about cyber security risks. However, consumers in developing countries were unable to try the product. Therefore, these products are useless in less developed nations. Developing countries need to prioritize research aimed at strengthening their information technology infrastructure. It is evident that hostile nations or terrorist organizations are constantly looking for ways to exploit vulnerable cyberspaces. Therefore, nations such as India should establish robust IT units to effectively address any potential threats. Information and communication technology has become an essential aspect of modern life; thus, it is crucial to incorporate both the benefits and drawbacks of IT into academic curricula. This should be a key focus within the national education framework.

REFERENCES

1. Paul, P.K., Chatterjee, D., Bhuimali,A., Atarthy, A. 2016. Cyber Crime: An Important facet for promoting Digital Humanities—A Short Review in *Saudi Journal of Humanities and Social Science*, **1**(1): 13-16.

2. Paul, P.K. 2013. Cyber Crime and its Challenges with Special Reference to Solution. *International Journal System Simulation,* **7**(2): 77-82.

3. Schafer, J., Ragsdale, D.J., Surdu, J.R. and Carver, C.A. 2001. The IWAR range: a laboratory for undergraduate information assurance education. *Journal of Computing Sciences in Colleges*, **16**(4): 223-232.

4. Schepens, W., Ragsdale, D., Surdu, J.R., Schafer, J. and New Port, R.I. 2002. The Cyber Defense Exercise: An evaluation of the effectiveness of information assurance education. *The Journal of Information Security*, **1**(2): 1-14.

5. Caballero-Anthony, M. and Cook, A.D. (Eds.). 2013. *Non-traditional security in Asia: Issues, challenges and framework for action*. Institute of Southeast Asian Studies.

6. Devi, S. and Rather, M.A. 2015. Cyber Security in India: Problems and Prospects. *IITM Journal of Management and IT*, **6**(1): 59-68.

7. Ebert, H. 2020. Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. *India Review*, **19**(4): 376-413.

8. Gupta, A. 2018. *How India manages its national security*. Penguin Random House India Private Limited.

9. Malik, M.B. 2018. Architecture of cyberspace as an evolving security paradigm in outh Asia: Pakistan-India cyber security strategy. *Institute of Regional Studies, Islamabad*, **36**(2): 3-35.

10. Kumar, S. 2003. *India's National Security*. Taylor & Francis.

11. Kumar, S.R., Yadav, S.A., Sharma, S. and Singh, A. 2016. Recommendations for effective cyber security execution. In *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)* (pp. 342-346). IEEE.

12. Kshetri, N. 2013. Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research*, **13**(1): 41-69.

13. Patil, S. 2021. *Securing India in the Cyber Era*. Routledge India.

14. Paul, P.K. and Aithal, P.S. 2019. Information Assurance and IT Management: The Key Issues, Solutions in Indian Scenario based on International Trends. *World Academics Journal of Management*, **7**(1): 12-17.

15. Subrahmanyam, K. 2003. External security. *India: Vision, 2025*. Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. *India Review*, **19**(4): 376-413.

16. Wanglai, G. 2018. BRICS cyber-security cooperation: Achievements and deepening paths. *China Int'l Stud.*, **68**: 124.

17. https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=6172&lid=4236

18. https://timesofindia.indiatimes.com/readersblog/the-seeker/threat-perception-for india-and-its-neighbourhood-33225/

19. https://www.sciencedirect.com/topics/computer-science/cybercriminals

20. https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security

21. https://vikaspedia.in/e-governance/national-e-governance-plan/national-cyber-security-policy

22. https://www.hindustantimes.com/india-news/india-looks-to-redraw-plan-for-cybersecurity-policyofficials-101644601423461.html

23. https://cis-india.org/internet-governance/cyber-security-mapping.

24. (https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

25. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html