A COMPARATIVE ANALYSIS OF THE 2020 GLOBAL CYBERSECURITY INDEX SCORES OF INDIA AND PAKISTAN

IRTA FATIMA*

Abstract

This comparative analysis examines the 2020 Global Cybersecurity Index scores of India and Pakistan. The Global Cybersecurity Index (GCI) is a composite index that measures a country's commitment to cybersecurity based on five categories: legal measures, technical measures, organizational measures, capacity building, and cooperation. This study analyzes the GCI scores of India and Pakistan and identifies similarities and differences in their cybersecurity profiles. The GCI has published four editions till 2020, and according to the GCI of 2020, India scored 97.49 and became the 10th top scorer in the GCI, while Pakistan scored 64.88 on the index. The study highlights the areas where India and Pakistan have strengths and weaknesses in terms of cybersecurity measures and provides recommendations for both countries to improve their cybersecurity profiles. The study concludes that cybersecurity is becoming increasingly important in the digital age, and countries need to invest in cybersecurity measures to protect their critical infrastructure and citizens' data.

Keywords: *Global Cybersecurity Index, International Telecommunication Union, Pakistan-Cert, India-Cert, National security policy, Information, and Communication technology.*

---

* Ms Irta Fatima holds an MPhil degree in Peace and Conflict Studies from the National Defence University, Islamabad.

Regional Studies, 40:1, Summer 2022, pp.39-60

Introduction

The International Telecommunication Union (ITU) is the first international organization in the history of telecommunications. It was founded in 1865 to improve and enhance information and technology resources to ensure the standard of networks all over the world. In 1947, it was designated as a central agency of the United Nations. The goals of the ITU include promoting international cooperation in satellite orbital planning, enhancing telecommunications infrastructure in developing nations, and assisting in the creation and coordination of global technical standards.[1] The ITU is dedicated to bringing all the people of the world together, regardless of where they reside or how much money they have.[2] The ITU is aiming at efficiently, safely, easily, and affordably making the advantages of contemporary communication technology available to everyone. In addition to the ITU's 193 member states, including Pakistan and India, it has some 700 tech businesses and numerous prestigious academic institutions. The ITU is the only worldwide organization that includes all participants as member states in this dynamic and quickly expanding industry in a world that is becoming more and more interconnected.[3]

The ITU, the premier body for ICT regulations has launched the Global Cybersecurity Index (GCI) to establish a baseline of the level of cybersecurity globally to secure the cyber security of member states and to gauge the dedication of the ITU member states to cybersecurity to help them identify areas for improvement and motivate countries to take action by bringing attention to the state of cybersecurity globally.

Overview of the GCI

Indexes are frequently used as benchmarks to measure a portfolio's performance. Indexing involves passively striving to imitate an index instead of trying to perform it.[4] A measure or indicator of anything is called an index. The Global Cybersecurity Index (GCI) assesses a country's commitment to global cybersecurity to highlight

the significance and range of the problem. Each country's level of development or engagement is evaluated along the following five indicators:[5]

1. Legal Measures
2. Technical Measures
3. Organizational Measures
4. Capacity Building
5. Cooperation

The GCI has evolved to provide a more realistic picture of the cybersecurity measures implemented by member states as cybersecurity risks, priorities, and resources change. By highlighting gaps, promoting the adoption of best practices, and offering insightful recommendations, the GCI seeks to better understand the commitments of member states to cybersecurity.[6] The annual report of the GCI gives a broad picture of the world's cybersecurity environment, including the level of readiness for cybersecurity in each nation and the progress made in implementing cybersecurity paradigms. The report sketches a broad overview of the state of cybersecurity around the world, as well as the degree of preparedness for cybersecurity in each country and the progress made in putting cybersecurity measures into practice. The report also analyses the worldwide cybersecurity landscape and highlights important developments and difficulties.[7]

The GCI has published four editions so far. The first edition was published in 2014, the second in 2017, the third in 2018, and the fourth in 2020, which is the most recent one. This study highlights the GCI of Pakistan and India as per the fourth edition of GCI 2020, which gives Pakistan an overall score of 64.88[8] and India 97.49[9] (as mentioned in figure a). These scores are based on the key indicators mentioned above. India was placed 47th in the third version of the GCI published in 2018.[10] It has jumped to the 10th position in the ranking in 2020.[11] Pakistan was 94th[12] in the GCI report of 2018.[13] India has

improved its GCI score through improvements in indicators much faster than Pakistan.

Literature Gap: The GCI is a way of evaluating a country's cyber infrastructure's level of security. Notwithstanding, its ability to provide additional insight into the situation regarding worldwide global cyber security, the GCI has been overlooked in terms of academic research, as there is a lack of research in this particular domain of GCI comparison between India and Pakistan. There is a particular need for research that examines the index's accuracy and reliability, as well as its ability to predict future cyber threats. Research is also required to examine how the index might be applied to guide policy choices and tactics for enhancing global cyber security.

Methodology: Cyber Security Cooperation Framework (CCF)

As discussed above, the ITU is a United Nations agency that specializes in information and communication technologies (ICTs). It is in charge of establishing global standards and providing policy guidance on ICTs. The ITU has created a comprehensive framework for international cybersecurity cooperation based on the principles of collaboration, capacity building, and trust.

The ITU Cybersecurity Cooperation Framework (CCF) offers a comprehensive approach to international cybersecurity cooperation. It is founded on the tenets of collaboration, capacity development, and trust. The CCF is intended to promote the development of national cybersecurity strategies and the implementation of international standards by facilitating the sharing of knowledge and expertise.

The CCF is also used in the development of the Global Cyber Security Index. It is an international benchmarking tool that assesses the level of cyber security in countries around the world. It is based on a set of criteria that evaluates a country's legal, technical, and organizational safeguards against cyber threats to its residents and critical infrastructure. Moreover, it is used to identify areas for

improvement and to provide policymakers with information on how to better protect their inhabitants from cyber threats.

The data has been collected from a secondary source for instance an annual report of GCI 2020, where inductive reasoning is applied. The paper draws a comparative analysis between Pakistan's and India's GCI 2020 scores and also suggests the way forward to improve Pakistan's GCI score in the next edition of the GCI, which is likely to be published in 2023 by the ITU.

Figure (a)

Country Name	Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
Pakistan	64.88	15.7	12.26	11.01	17.25	8.38
India	97.49	20.00	19.08	18.41	20.00	20.00[14]

India's initiatives in the cyber domain till 2020

First pillar: India's legal measures in the cyber domain

1. **The Indian Penal Code, 1860:** This Act establishes penalties for online offences such as data theft, hacking, and cyber-terrorism.[15]
2. **The Information Technology Act, 2000:** This law gives electronic transactions and digital signatures legal status. Additionally, it calls for the creation of a Cyber Appellate Tribunal to settle issues resulting from online sales.[16]
3. **Following the Information Technology (Certifying Authorities) Rules, 2001:** These regulations offer instructions on how to issue digital signatures for certifying authorities.[17]
4. **The Information Technology (Security Procedure) Rules, 2009:** These rules offer recommendations for information system security.[18]

5. **The Information Technology (Procedure and Safeguards for Blocking for Public Access of Information) Rules, 2009:** These regulations offer principles for restricting public access to particular websites or information.[19]
6. **The Rules for the Use of Information Technology (Interception, Monitoring, and Decryption of Information), 2009:** These regulations offer guidelines for the government's information monitoring, decryption, and interception activities.[20]
7. **Rules for Information Technology (Intermediaries), 2011:** These regulations include recommendations for intermediaries, including internet service providers and search engines, to safeguard user interests and stop service abuse.[21]
8. **The Rules for Sensitive Personal Data or Information and Information Technology (Reasonable Security Practices and Procedures), 2011:** These regulations offer organizations instructions for safeguarding the personal information of their clients.[22]
9. **The Information Technology (Guidelines for Cyber Cafe) Rules, 2011:** These regulations offer criteria for cyber cafes to follow to protect the privacy and security of their patrons.[23]
10. **The Rules for the Delivery of Electronic Services in Information Technology, 2011:** These regulations offer instructions for how the government should deliver electronic services.[24]
11. **The National Cyber Security Framework (NCSF), 2013:** This is a comprehensive framework for the defence of vital information infrastructure and other information assets, has also been introduced by the Indian government.[25]
12. **The National Cyber Security Strategy (NCSS), 2013:** It was also introduced by the Indian government as a comprehensive plan for safeguarding other information assets as well as key information infrastructure.[26]

13. **The National Cyber Security Policy, 2013:** The policy has been introduced by the Indian government as a framework for safeguarding various information assets as well as key information infrastructure.[27]

Second Pillar: Technical measures

1. The **Digital India Program**, which aims to encourage the use of digital technologies across the economy, was established by the Indian government.[28]
2. The Indian government has recently unveiled a network for automated and technical tools called Cyber Swachhta Kendra.[29]
3. The **National Cyber Security Portal (NCSP)**, a one-stop shop for all information and technical services relating to cyber security, has also been launched by India.[30]

Third pillar: Organizational Measures

1. To safeguard the country's vital information infrastructure from online attacks, India established the **National Critical Information Infrastructure Protection Centre (NCIIPC)**.[31]
2. The **Indian Computer Emergency Response Team** (CERT-In) organization was established to address cyber security issues and offer enterprises support[32] and to track, identify, and address cyber security glitches.[33]
3. The **National Cyber Security Policy (NCSP)** which is a software private limited, defines the steps to be done to safeguard the nation's cyberspace against cyber-attacks and was introduced by the Indian government.[34]
4. The Digital India institute, the **SANS foundation**,[35] was started by the Indian government to encourage the usage of digital technologies there.[36]
5. To track and assess cyber threats in real time, the Indian government also built the **National Cyber Coordination Centre**

(NCCC).[37] It is an active cybersecurity and electronic surveillance organization in India.

6. The **Indian Cyber Crime Coordination Centre (IC4)** was also set up by the Indian government to work with law enforcement organizations to combat cybercrime.[38]
7. To encourage research and development in the area of cyber security, the Indian government also established the **National Cyber Security Research and Development Centre (NCSRDC)**.[39]

Fourth Pillar: Capacity Development measure

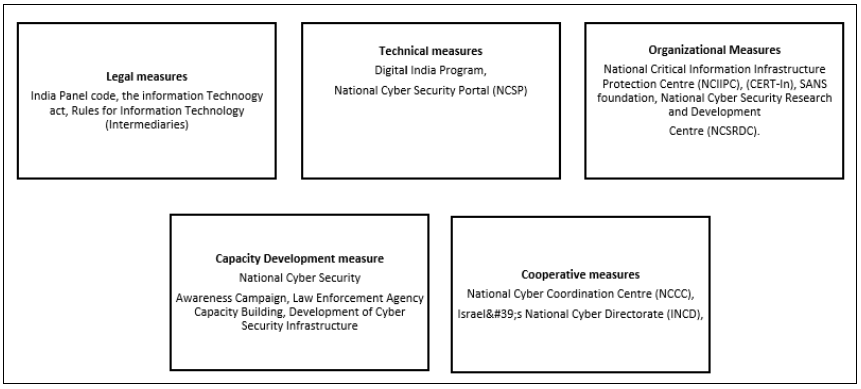
1. To educate citizens about cybersecurity, the Indian government has also started the **National Cyber Security Awareness Campaign**.[40]
2. To increase Cyber Security Education and Consciousness: India has launched several initiatives to increase cyber security education and awareness. These include the introduction of the Indian Computer Emergency Response Team (CERT-In) to monitor, detect, report, and respond to cyber security issues, as well as the 2013 unveiling of the National Cyber Security Policy, which aims to build a secure cyberspace in India.[41]
3. **Law Enforcement Agency Capacity Building:** The Indian government has taken several measures to increase the ability of law enforcement organizations to combat cybercrime. These include the NCCC to coordinate cyber Security initiatives and a National Cyber Crime Reporting Portal to make it easier for victims of cybercrime to come forward.[42]
4. **Reinforcement of Guideline:** The Indian government has also acted to make the country's cybersecurity regulations stronger. Incorporating the Information Technology Act, (mentioned above in legal measure) which offers a legal framework for policing online transactions and cybersecurity, is one example of this.

5. **Development of Cyber Security Infrastructure:** To make India's cyber security infrastructure stronger, the government has taken many actions. To safeguard vital information infrastructure, these initiatives include the creation of the National Critical Information Infrastructure Protection Centre (NCIIPC) and the National Cyber Security Coordination Centre (NCSC), which serve to coordinate various cyber security initiatives.[43]
6. **Advancement of Research and Development:** India has also initiated steps to advance cybersecurity research and development. It also entails the creation of the National Cyber Security Innovation Centre (NCSIC) to foster innovation in cybersecurity and the National Cyber Security Research and Development Centre (NCSRDC) to foster research and development in cybersecurity.[44]
7. To educate citizens about cyber security, and protect their personal information, the Indian government has also started the National Cyber Security Awareness Campaign (NCSAC).[45]

Fifth Pillar: Cooperative measures

1. To track and assess online threats in real time, India built the **National Cyber Coordination Centre (NCCC)**, which was approved by the Ministry of Home Affairs (India) in 2018.[46] NCCC was established to provide appropriate information exchange for proactive, preventative, and protective measures by individual entities and to generate situational awareness of current and forthcoming cybersecurity threats that is required.
2. On 15 July 2020, Israel and India reached an agreement to increase their collaboration at the international level in the area of cybersecurity. Yigal Unna, the director general of **Israel's National Cyber Directorate (INCD)**, and Sanjeev Singla, India's ambassador to Israel, signed a Memorandum of Understanding (MoU).[47]

- India has enhanced its alliance with hi-tech industries, such as Microsoft to speed up India's digital transformation and National Association of Software and Services Companies (NASSCOM)[48] and IBM to hasten the adoption of innovative technologies and cooperation.[49]



Pakistan's initiatives in the cyber domain till 2020

First pillar: Pakistan's Legal measures in the cyber domain

1. The Federal Investigation Agency's (FIA) Cybercrime Wing (CCW) is governed by the **Prevention of Electronic Crimes Act (PECA),** which addresses the growing threat of cybercrimes. This was established in 2007 to recognize and address the problem of electronic exploitation in society. In Pakistan, it is the sole unit of its sort that collects complaints directly and pursues legal action against cybercriminals.[50]
2. In 2016, **the Prevention of Electronic Crimes Act (PECA), Electronic Transactions Ordinance 2002,** and **Electronic and Cyber Crime Bill 2007**, were introduced by the government as part of efforts to make cyber laws and regulations stronger.[51]

Second pillar: Technical measure

1. The Pakistan Computer Emergency Response Team **(Pak-CERT)** is a private entity founded in 2020 to offer organizations technical support and assistance in response to cyber incidents.[52]

Third pillar: Organizational measures

1. The **National Response Centre for Cyber Crime (NR3C)** institution was formed in 2007 to look into cybercrime.[53] The Federal Investigation Agency (FIA) added NR3C to its portfolio, especially to address technology-based crimes in Pakistan.
2. The Pakistani government started work on establishing the National Centre for Cyber Security (NCCS) in June 2018. The Higher Education Commission (HEC) and Planning Commission collaborated on the **NCCS** project. The Centre is made up of Research and Development (R&D) Labs in reputable Pakistani universities (NUST-Air) that were chosen after HEC issued an open request for proposals in the first quarter of 2018. These universities were given the authority to construct NCCS-affiliated Labs under the secretariat of the centre in various specialized fields of cybersecurity.

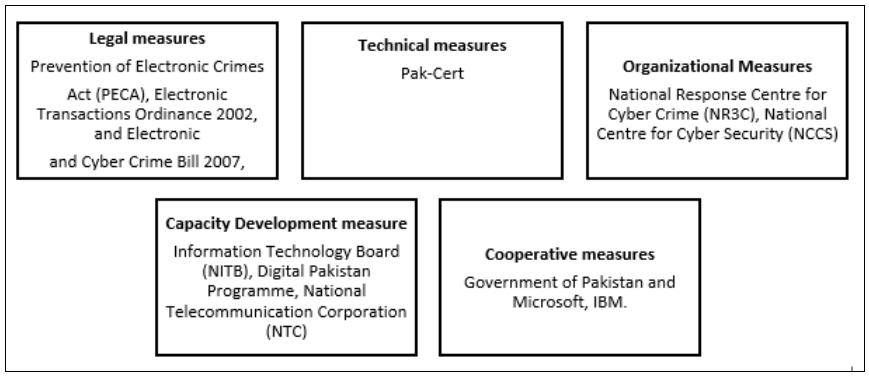
Fourth Pillar: Capacity development measure

1. To develop and carry out e-governance policies and plans, and for IT training Pakistan's National **Information Technology Board (NITB)**[54] was established.
2. To digitize the economy, the state has also started the **Digital Pakistan Programme.**[55]
3. To assure quality assurance and secure the establishment of digital products and services, the government has started the **Digital Pakistan Certification Programme.**[56]

4. The **National Telecommunication Corporation (NTC)**[57] was founded to encourage the expansion of Pakistan's telecom industry.

Fifth Pillar: Cooperative measures

1. A Memorandum of Understanding (MoU) between the **Government of Pakistan** and **Microsoft** has been signed in 2016 to improve the government's cybersecurity capabilities.[58]
2. To support the growth of the country's entire IT infrastructure, agriculture sector, cloud computing, and artificial intelligence, the government of Pakistan signed a Memorandum of Understanding (MoU) with **IBM** in 2018 at the international level.[59]



Comparative Analysis of the 2020 GCI Scores of India and Pakistan GCI-2020

As mentioned above, India scored 97.49 and was ranked among the top 10 in the ITU's GCI 2020. India has fulfilled the parameters on which the GCI scores its member states, as compared to the GCI of Pakistan.

Relating to India's legal measures, India has taken enough jurisdiction measures in the cyber domain but in the cyber laws' domain of Pakistan, a gap is found in cooperation

between the Ministry of Information Technology and policymakers in Pakistan. Mentioning technical measures of the cyber domain in India, the GCI 2020 found that India had worked a lot in technical terms to secure cyberspace such as the Indian Computer Emergency Response Team (Cert-In), Digital India Programme, and the National Cybersecurity portal to secure technical infrastructure of India. Correspondingly, in the context of Pakistan, Pak-Cert is a private entity offering technical support. The struggle to launch a national Cert to secure cyberspace in Pakistan is still enduring due to a lack of collaboration between the private and public sectors. As mentioned above, the organizational measures taken by India depicted that India has ensured cyber security with the help of the formation of organizations discussed above. Pakistan has taken very few organizational measures like NR3C and the National Cybersecurity Academy to promote the education of cyber security and some universities such as the National University of Science and Technology (NUST) and Air University are offering facilities for research and development in cybersecurity. However, the Higher Education Commission of Pakistan has only shown concern from 2021 onwards to including the course of cybersecurity in universities to promote cyber education. In the same way, India has taken enough steps in capacity development measures in the cyber domain. For instance, awareness campaigns and facilitation centres to create coordination and cooperation between the Ministry of Home Affairs and the citizens of the country. Pakistan has not achieved enough unless awareness campaigns or training programmes are initiated by NITB (elaborated above). In cooperative measures, India has signed an MoU with hi-tech Giants such as

NASSCOM and so on but Pakistan has not maintained assistance at domestic and international levels. With the exception of Mircrosoft, Pakistan has not signed MoUs with the likes of Amazon and other hi-tech giants such as Meta.

This research shows that Pakistan has not taken enough steps to strengthen Pakistan's score in the GCI 2020, whereas India has tried to achieve the key indicators of the GCI.

Pakistan's Cyber Pathway from 2021 Onwards

1. The adoption of Pakistan's first comprehensive policy, the **Pakistan Cybersecurity Policy 2021**, by the Federal Government of Pakistan. The goal of the strategy is to address the changing nature of cyber threats and the requirement to safeguard the country's digital infrastructure.[60]
2. The establishment of **Pakistan Cyber Security Authority (PCSA)**, to counter the nation's increasing cyber threats, the Pakistan Federal Government formed the Pakistan Cyber Security Authority (PCSA). The PCSA is entrusted with creating a thorough cybersecurity framework and strategy as well as advising and assisting organizations from the public and private sectors with the execution of the policy.[61]
3. The Federal Cabinet of Pakistan approved **Pakistan's first-ever Cloud First Policy** in February 2022 with the goal of reformation and rationalization of the public sector's information and communication technology (ICT) environment.[62]

Proposed Way Forward to Enhance Pakistan's Score in the Fifth Edition of the GCI:

1. To improve technical measures in the next fifth edition of GCI, an official Pakistan Cert is required. Which could be regulated by the **Ministry of Information Technology and Telecommunication (MoITT)**, Pakistan. For this, cooperation

between the private and public sectors is important, because Pk-Cert was made in 2000 by a private entity. Correspondingly, India has made one uniform entity named as Cert-In, launched by the Ministry of Electronics and Information Technology of the Government of India.

2. The formation of the **National Cyber Security Authority** by MoITT is needed, to coordinate and manage the application of cybersecurity policy 2021 and plans. To make sure that such establishment/authority is held responsible for cybersecurity practices. This institution ought to be responsible for creating and enforcing cybersecurity laws as well as advising and assisting both public and private sector enterprises.
3. Think tanks such as the Institute of Regional Studies (IRS), can collaborate with MoITT, to introduce new platforms or opportunities to reinforce cooperative and capacity development measures. Although the **National Technology Board** (NITB) has initiated an IT training program, it could be more beneficial if the NITB collaborates with think tanks such IRS and others to spread IT education by conducting workshops.
4. Creation of a **National Cybersecurity Strategy** by MoITT is a prerequisite for outlining the country's goals, priorities, and measures for safeguarding its vital infrastructure, technical assets, and data against cyber-attacks.
5. The **Pakistan Telecommunication Authority** (PTA) and **NR3C** need to create a **single accessible portal** for the citizens of Pakistan to register cyber-attacks or to identify cyber threats for undertaking counter-measures against them.
6. In terms of cooperative measures, in which Pakistan's progress is very less. The MoITT and PTA can collaborate with the **Ministry of Foreign Affairs (MOFA)** to establish cyber alliances with developed countries such as China, Australia, and Russia. These institutions can provide a favourable and secure environment to

enhance international collaboration with hi-tech giants such as Meta, Amazon, Google, and Apple, including establishment of their offices in Pakistan. They could also coordinate for new cybersecurity initiatives and seek assistance from hi-tech giants from emerging global powers such as China and Russia. MOFA can act as a mediator through dialogues, table talks, and confidence-building measures to promote cooperation. As mentioned above, India has already made a cyber alliance with Israel.

Conclusion

Pakistan's cyber evolution is quite vulnerable, even though Pakistan has taken a few steps such as Pakistan-Cert, the National Cybersecurity Policy 2021, etc. Pakistan has adopted initiatives in technical, organizational, capacity development, and legal domains but very little progress is found in cooperative measures. Unfortunately, Pakistan is susceptible to the lowest GCI. India's score in the *GCI 2020 Report* shows that it became the 10th country in cybersecurity. This is an indication that India is advancing in the cyber domain. Pakistan should keep an eye on the developments in the cyber domain. Warfare has become non-traditional in the 21st century, where cyber-warfare has taken place between India and Pakistan. A 'cyber-alliance' could be a game changer for Pakistan, by enhancing its cybersecurity paradigms through mutual collaboration at the international level. This can help Pakistan to compete with the Global Cyber Security Index of India, in the next (fifth) edition, which would likely be published in 2023 by the International Telecommunication Union.

Notes and References

1 Jamal Shahin, "The International Telecommunication Union", *Research Gate* (2010), 11.

2 Yoshio Utsumi, "The International Telecommunication Union", *ITU,* August 2002, available at https://www.itu.int/itudoc/gs/promo/gs/81150.pdf.

3 Charles Glass, "An Overview of the Structure and Functions of the International Telecommunication Union", *International Spectrum Policy Division,* 25 September 2019, available at https://ustti.org/wp-content/uploads/2019/11/Day-7-1_ITU_Overview.pdf.

4 Andrew W Lo, "What is an index?", *Research Gate,* January (2019), available at https://www.researchgate.net/publication/291359536_What_Is_an_Index.

5 Doreen Bogdan-Martin, "Global Cybersecurity Index 2020", *International Telecommunication Union Development Sector*, (2021), available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

6 Ibid.

7 Ibid.

8 Doreen Bogdan-Martin, "Global Cybersecurity Index 2020", *International Telecommunication Union Development Sector*, (2021), 95.

9 Ibid., 87.

10 "Global Cybersecurity Index 2018", *International Telecommunication Union*, (2019): 63.

11 Doreen Bogdan-Martin, "Global Cybersecurity Index 2020", *International Telecommunication Union Development Sector, (2021)*, available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

12 "Global Cybersecurity Index 2018", *International Telecommunication Union*, (2019): 65.

13 "Global Cybersecurity Index 2018", *International Telecommunication Union*, (2019): 65.

14 Ibid.

[15] "The Indian Penal Code," *Arrangement of sections,* available at https://www.iitk.ac.in/wc/data/IPC_186045.pdf.

[16] Ramanbir Bindra, "Information Technology Act, 2000," *Gargicollege,* (2020), available at https://gargicollege.in/wp-content/uploads/ 2020/03/Information-Technology-Act.pdf.

[17] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary*, available at https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[18] Ibid.

[19] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary*, available at https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[20] Ibid.

[21] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary,* available athttps://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[22] The Personal data protection bill", *Minister of Law and Justice, Communications and Electronics and Information Technology),* available at https://www.dataguidance.com/sites/default/files/personal-data-protection-bill-2019.pdf.

[23] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary*, available at https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[24] Ibid.

[25] Lt Gen D S Hooda, "India's national security strategy", *assuming our rightful place in global affairs*, available at https://manifesto.inc.in/pdf/national_security_strategy_ gen_hooda.pdf.

[26] Ibid.

[27] "National Cyber Security Policy (NCSP) 2013. National Cyber Security Policy (NCSP) 2013", *InstaPdf,* available at https://files.instapdf.in/wp-content/uploads/pdf-thumbnails/2020/01/national-cyber-security-policy-ncsp-2013-2780.webp.

[28] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary*, available at https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[29] M Shahnawaz, "Cyber security: crying need of the day," *Global Journal for research analysis*", October (2020): 71, available at https://www.worldwidejournals.com/global-journal-for-research-analysis-GJRA/recent_issues_pdf/2020/October/cyber-security-crying-need-of-the-day_October_2020_2662471012_2809316.pdf.

[30] Ibid.

[31] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary*, available at https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf.

[32] Gulshan Rai, "Cyber Security & Role of CERT-In", *Cert-IN,* available at https://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/rai-role-of-cert-in-sept-09.pdf.

[33] Udbhav Tiwari, "Cyber Security & the CERT-In A Report on the Indian Computer Emergency Response Team's Proactive Mandate in the Indian", *Cyber Security Ecosystem*, available at https://cis-india.org/internet-governance/files/cert-ins-proactive-mandate.pdf.

[34] D S Hooda, "India's national security strategy", *assuming our rightful place in global affairs*, available at https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf.

[35] SANS provides industry-leading community initiatives, training, and events to empower present and future cybersecurity professionals around the world with information and skills.

[36] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary*, available at https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guide

lines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

[37] "National Cyber Security Policy (NCSP) 2013. National Cyber Security Policy (NCSP) 2013", I*nstaPdf*, available at https://files.instapdf.in/wp-content/uploads/pdf-thumbnails/2020/01/national-cyber-security-policy-ncsp-2013-2780.webp.

[38] Indian Cyber-crime coordination Centre", *Journals of India*, available at https://journalsofindia.com/indian-cyber-crime-coordination-centre/?print=pdf.

[39] National Cyber Security Research and Development Challenges, "*An Industry, Academic and Government Perspective",* available at https://www.fbiic.gov/public/2009/feb/i3pnationalcybersecurity.pdf.

[40] Andrew Facini, "The Cybersecurity Campaign Playbook", *Defending Digital Democracy Project Belfer Center for Science and International Affairs*, March (2019), available at https://www.iri.org/wp-content/uploads/2022/01/2019.3.11_indian_cybersecurity_playbook.pdf.

[41] Gulshan Rai, "Cyber Security & Role of CERT-In", *Cert-IN*, available at https://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/rai-role-of-cert-in-sept-09.pdf.

[42] "National Cyber Security Policy (NCSP) 2013. National Cyber Security Policy (NCSP) 2013", *InstaPdf,* available at https://files.instapdf.in/wp-content/uploads/pdf-thumbnails/2020/01/national-cyber-security-policy-ncsp-2013-2780.webp.

[43] "IT (Intermediary Guidelines and Digital Media Ethics Code) Rules", *The gazette of India: Extraordinary*, available at https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf.

[44] National Cyber Security Research and Development Challenges, "*An Industry, Academic and Government Perspective*", available at https://www.fbiic.gov/public/2009/feb/i3pnationalcybersecurity.pdf.

[45] Facini, "The Cybersecurity Campaign Playbook."

[46] "National Cyber Security Policy (NCSP) 2013. National Cyber Security Policy (NCSP) 2013", *InstaPdf,* available at

https://files.instapdf.in/wp-content/uploads/pdf-thumbnails/2020/01/national-cyber-security-policy-ncsp-2013-2780.webp.

47 "India and Israel sign agreement to expand cooperation in cyber security", *The Hindu news*, available at https://www.thehindu.com/news/national/india-and-israel-sign-agreement-to-expand-cooperation-in-cyber-security/article32102730.ece.

48 "Industry-Performance2018-19-and-what-lies-ahead", available at https://nasscom.in/ *sites*/default/files/Industry-Performance2018-19-and-what-lies-ahead_0.pdf.

49 "IBM and IIT Delhi collaborate to advance AI research in India" *IBM*, available at https://in.newsroom.ibm.com/2018-11-29-IBM-and-IIT-Delhi-collaborate-to-advance-AI-research-in-India.

50 Ibid.

51 "As passed by the Majlis.e.Shoora (Parliament)", *A Bill*, available at https://na.gov.pk/uploads/documents/1470910659_707.pdf.

52 Taimur Tufail, "Comparing the national cyber security framework of Pakistan with India and United kingdom", *TUT Center for Digital Forensics and Cyber Security*, (2018): 43, available at https://digikogu.taltech.ee/en/Download/56aa279d-3c19-4610-b25d-a33defc6d149.

53 "Cyber-crimes Risks, Prevention and Legal Remedies", *Ministry of Interior Government of Pakistan*, available at https://www.fia.gov.pk/ files/publications/860464251.pdf.

54 On August 11, 2014, the National Information Technology Board was created by merging the Pakistan Computer Bureau (PCB) and the Electronic Government Directorate (EGD). To establish e-governance to enhance the public's access to high-quality information and services delivered by ICT practically and economically.

55 "Digital Pakistan Policy", *Ministry of IT & Telecom,* available at http://moib.gov.pk/Downloads/Policy/DIGITAL_PAKISTAN_POLICY%2822-05-2018%29.pdf.

56 Ibid.

57 To provide secure and dependable telecom services, NTC was established under Pakistan Telecom.

[58] "Microsoft to open new training, development center in Pakistan", *The Nation, 2 February 2016,* available at https://www.nation.com.pk/02-Feb-2016/microsoft-to-open-new-training-development-centre-in-pakistan.

[59] 'Telenor Pakistan Collaborates with LMKT to Provide IBM's Accurate Weather Forecast to Local Farmers", *LMKT,* available at https://www.lmkt.com/telenor-pakistan-collaborates-lmkt-provide-ibms-accurate-weather-forecast-local-farmers/.

[60] "National cyber security policy", *Digital Pakistan,* July (2021): 2, available at https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf.

[61] Ibid.

[62] "Pakistan cloud first policy", *Digital Pakistan,* February (2022), available at https://moitt.gov.pk/SiteImage/Misc/files/Pakistan%20Cloud%20First%20Policy-Final-25-02-2022.pdf.