FTI CONSULTING

AMCHAM INDIA

A WHITE PAPER ON INDIA'S NATIONAL CYBERSECURITY STRATEGY 2020

PREPARED FOR THE OFFICE OF THE NATIONAL CYBERSECURITY COORDINATOR (NCSC), GOVERNMENT OF INDIA

APRIL 2020

EXPERTS WITH IMPACT

FOREWORD

Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. Increasingly, there is evidence that critical national infrastructure is being probed by cyber agents from other nation states. In sectors where competitive intensity is high, cyber criminals now operate with both espionage and criminal intent. In the past, cyber criminals focused on stealing information and threatening corporates, but now, they are weaponizing software by installing malicious scripts and disrupting work.

In an uncertain time like such, India's positioning in building a strong cybersecurity policy along with a strategy to implement the same at the grassroot levels becomes imperative. The American Chamber of Commerce (AMCHAM) along with FTI Consulting has consulted its members upon getting a recommendation for the upcoming Cybersecurity Policy of 2020. It looks into six critical infrastructure sectors and has provided a detailed structure in consultation with the industry and feedback received by the National Cybersecurity Coordinator (NCSC) task force committee. AMCHAM would like to thank Gen Rajesh Pant, Brigadier Manjeet Singh, and the NCSC team for the opportunity to deliberate on the suggestions made by AMCHAM Member companies.

Ranjana Khanna

Director General and CEO, AMCHAM

The American Chamber of Commerce in India (AMCHAM India) is an association of American businesses in India, established in 1992, with 500 members. The US Ambassador to India is the Honorary President. AMCHAM works closely with the Indian government for facilitating ease of doing business in India.

FOREWORD

The role of information and communication technology (ICT) in India's economic growth and social development cannot be overemphasized, accounting for one-fifth of the GDP by the time the latter reaches five trillion US dollars. Whether it is education and healthcare, governance and citizen engagement, entrepreneurship and innovation, or for that matter, agriculture and climate change, the government's ambitious "Digital India" programme envisages leveraging ICT for all these and then some.

The attack surface of the cyberspace is also growing with hyper-connectivity across devices and services. Whether we look at data from companies, consulting organizations, or even the government itself, cybersecurity threats are on the rise in India. In fact, according to the Global Cybersecurity Index published by the UN agency International Telecommunication Union (ITU), India's global rank slipped to 47 in 2018 from 23 in 2017, indicating a decreasing level of cybersecurity engagement across the country. Complicating the matter even further, cybersecurity is also becoming a geopolitical issue.

Hence, India needs a national cybersecurity strategy for comprehensive readiness and responsiveness, ultimately leading to resilience while also ensuring that fundamental rights, like privacy, are preserved. It should span critical information infrastructure protection, capacity building, and crisis management. However, the government cannot do it all alone and must coopt and collaborate with the private sector, where much of the design, development, and deployment happens, as recognized in the US-India bilateral cyber cooperation framework signed in 2016.

AMCHAM members include leading cybersecurity solution providers with innovative technologies and organizational capability that India can and must leverage. This report is a humble contribution in this regard. I would like to place on record our sincere appreciation for the guidance of National Cybersecurity Coordinator Lt. Gen. (Dr.) Rajesh Pant and other members of the Task Force; AMCHAM members for their inputs; Amrit Singh Deo, Prasanto Roy, and Subhodeep Jash at FTI Consulting for their research; and Ranjana Khanna and Ishita Sengupta at AMCHAM secretariat.

Valsa Williams

Advisor, AMCHAM India

Kishore Balaji

Co-Chair, AMCHAM India Cyber Committee and Director- Govt Affairs & Public Policy (South Asia), Intel

Rajnish Gupta

Co-Chair, AMCHAM India Cyber Committee and Regional Director-India and SAARC, RSA Security

Deepak Maheswari

Chair, AMCHAM India Cyber Committee and Director – Government Affairs, India, ASEAN & China, Norton LifeLock

FOREWORD

As India prepares to refresh its National Cybersecurity Policy, it must move in sync with present day technological and ecosystem realities. India's cybersecurity framework should be able to adapt and be resilient to protect against intrusions at all levels – in the public sector, including critical infrastructure, and citizen services, enterprise systems, and public and private data assets.

A spate of recent incidents ranging from a malware attack on Kudankulam nuclear plant that led to a significant data breach on its administrative network to a recent financial data breach reported by the Singapore-based IB group affecting more than 1.3 million card users, underscore the security vulnerabilities in our cybersecurity apparatus.

This FTI Consulting-AMCHAM white paper takes an ecosystem view and outlines the cybersecurity imperatives for India while considering all of the developments that have taken place since the 2013 Cybersecurity Policy. We undertake a stock-taking approach in first reviewing the progress, both domestically, and in the context of other jurisdictions, such as the United States and the European Union (that coincidentally published its first Policy around the same timeframe), along with the UN-backed ITU Global Cybersecurity Index to identify parameters where India can improve significantly and emerge as a cyber mature nation.

This paper then proceeds to make the case for a sense of urgency to address existing gaps, raise the level of cybersecurity preparedness and response capacity to bring it on par with cyber mature nations, and the need for closer coordination between private and public sectors, as the challenge requires pooling of resources while making specific recommendations to meet these objectives. This roadmap, we believe, can elevate India to a global cybersecurity economy that will be featured in the top 10 cyber-mature economies on the UN Index within the next three years.

We would like to express our deep appreciation for AMCHAM's Cybersecurity Committee and especially its Chair Deepak Maheshwari, Advisor Valsa Williams, and its Director General Ranjana Khanna for their strategic guidance on this paper.

Amrit Singh Deo

Senior Managing Director, FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. Individually, each practice is a leader in its specific field, staffed with experts recognized for the depth of their knowledge and a track record of making an impact. Collectively, FTI Consulting offers a comprehensive suite of services designed to assist clients across the business cycle – from proactive risk management to the ability to respond rapidly to unexpected events and dynamic environments.

Contents

PART 1
Executive Summary 6

PART 2
Background 8
2.1 Cybersecurity Imperative for India 8
2.2 Recent Breach incidents 8
2.3 Security Fraud in BFSI 9
2.4 Governing Data Flows 9

PART 3
Insitutional Framework 10
3.1 National Cybersecurity Policy 2013 and Key Policy Developments 10
3.2 Review of the NCSP 2013 12

PART 4
Global Trends 13
4.1 International Best Practices 13
4.2 Global Cybersecurity Norms and Framework 14
4.3 Global, Regional, and Bilateral Partnerships with India 15

PART 5
Assessment of India's Cybersecurity Ecosystem 18
5.1 Critical Information Infrastructure Protection 18
5.2 Securing E-governance Ecosystem 19
5.3 Building Cyber Deterrence Capabilities 20
5.4 Emerging Technologies and Their Security Implications 21
5.5 Cybersecurity Talent and Research 23
5.6 Cybersecurity Standard Setting, Testing, and Certification 23

PART 6
Recommendations For Indian Cybersecurity Policy – 2020 Onwards 25
6.1 Cybersecurity Governance 25
Recommendation 1 25
Recommendation 2 26
Recommendation 3 27
6.2 International Cooperation on Cybersecurity 28
Recommendation 4 28
6.3 Cybersecurity Risk Management 29
Recommendation 5 29
Recommendation 6 30
6.4 Cybersecurity Legislation and Regulations 31
Recommendation 7 31

INDIA'S NATIONAL CYBERSECURITY STRATEGY 2020

WHITE PAPER PREPARED FOR THE OFFICE OF THE NATIONAL CYBERSECURITY COORDINATOR (NCSC), GOVERNMENT OF INDIA

EXECUTIVE SUMMARY

Cyber risks are not bound by definitions of geography or ownership – rendering public and private assets equally vulnerable and without discrimination – and can render a vulnerable system useless in the blink of an eye. Or worse, mask the vulnerability in a system, slowly crippling it to destruction. We believe that the issue of cybersecurity starts with system vulnerabilities, which is at essence a human issue when broken down into its constituents[1], that aggregates and manifests quickly into a geopolitical issue. This is the reason national cybersecurity policies should move in close coordination with global efforts to secure critical assets, both in public and private sectors.

India is uniquely positioned to leverage its expanding influence as a rising economic power and global consumption hub to play an agenda-setting role in the global cybersecurity ecosystem. Over 1.17 billion people own a mobile phone in India, which is over 90 percent of the population[2]. Many of these mobile phone users also own a bank account. With a significant portion of the new Internet users emerging from rural India, digital inclusion needs to have security considerations embedded. The first step towards this ambition would be to address existing gaps in the current context, raise the level of cybersecurity preparedness and response capacity to bring it on par with cyber mature nations, and work in close coordination with other global regulators and cybersecurity frameworks.

This white paper makes the case for a sense of urgency to address these vulnerabilities and the need for closer coordination between the private and public sectors, as the challenge requires pooling of resources and taking an ecosystem view while making specific recommendations. FTI Consulting (FTI) has reviewed the UN-backed International Telecommunication Union (ITU) Global Cybersecurity Index to identify parameters where India can improve significantly and emerge as a cyber mature nation.

We place our recommendations along the pillars of (a) Secure India (b) Strengthen India and (c) Synergise India that you've highlighted in the call for submissions.

A. Secure India

1) Framing a critical information infrastructure (CII) protection plan: An updated national incident response plan can provide guidance to enable a unified whole-of-nation and internationally coordinated approach to response and recovery during a significant cybersecurity incident affecting critical infrastructure. Vulnerability reporting (by product/service vendors, agencies, as well as third parties), identifying and notifying critical systems and reporting of action taken by vendors/service providers, needs special attention. An updated national CII plan can supplement the broader 2020 Strategy.

2) Resilient frameworks at an enterprise (public or private) level: The Securities and Exchange Board of India (SEBI) has prescribed a cyber resilience framework for stock exchanges. This has five core principles similar to those in the National Institute of Standards and Technology's (NIST) framework: Identify, Protect, Detect, Respond, and Recover. Similarly, good IT governance at the agency level, whether public or private, must ensure consistency with internationally-endorsed standards such as ISO:27001, the NIST framework, and outcome frameworks frameworks at the European Telecommunications Standards Institute (ETSI), to integrate within the government and strategic public

[1] See FTI Consulting's 2018 Connected Risk paper https://www.fticonsulting.com/insights/articles/connected-risks
[2] Telecom Regulatory Authority of India, https://main.trai.gov.in/sites/default/files/PR_No.101of2019.pdf

enterprises. For example, the NCSC can look at a common minimum resiliency framework, and the Ministry of Electronics and Information Technology (MeitY) could develop a network security regime around 5G and the Internet of Things (IoT), along with industry stakeholders.

B. Strengthen India

3) 'Whole-of-nation' approach driven in project management mode by NCSC: This would lead to better alignment with strategic intent and ensure that cybersecurity principles enshrined in the National Cybersecurity Strategy 2020 are followed, and efforts across various ministries home, electronics and IT, etc.) are in coordination with state-level IT agencies, resolve any inter and intra-agency coordination gaps.

4) Developing state capacity and cyber readiness index for states: Any state-level security framework for ensuring responsive cyber federalism should be in alignment with the National cybersecurity Strategy, with no overlaps or misalignment with the central vision. For building stronger capacities at the local level, we should develop a cybersecurity Readiness Index (suggestion: in partnership with MeiTY and Niti Aayog) along the lines of the Government's similar effort to measure e-governance readiness in 2008.

C. Synergise India

5) Instituting a public private working group: A public-private cybersecurity working group constituted with members from Indian and global companies and government agencies should take forward the previous JWG mandate into specific tangible outcomes: the establishment of four to five Centers of Excellence (CoE), a cybersecurity skills action plan on capacity building and training programmes co-developed with industry bodies, such as AMCHAM and NASSCOM, and support to small and medium-sized enterprises and startups (similar to the UK's Cyber Aware programme.

6) Setting up new sectoral information sharing centres focusing on critical sectors: New Information Sharing and Analysis Centers (ISACs) are required for designated critical sectors (transportation; power and energy; telecom; government; banking, financial services, and insurance; and strategic/public enterprises). This will enable a central resource for gathering information on cyber threats and allow two-way sharing of information between the private and the public sector. Six sectoral ISACs for the critical sectors could be formed under the command of the National Critical Information Infrastructure Protection Centre (NCIIPC),, which could also set up a governing council to allow and oversee information exchange.

These recommendations are suggestions for the consideration of the NCSC so that India is more like Arjun rather than Abhimanyu in this modern-day rendition of the ancient Mahabharat war. Abhimanyu, Arjun's son, fought bravely but was slayed in battle as he had an Achilles heel – he did not know how to break out of the 'Chakravyuh' battle-formation. India must act to eliminate any such weakness if it is to emerge as a world-leading economy and geopolitical power in this twenty-first century.

BACKGROUND

2.1 CYBERSECURITY IMPERATIVE FOR INDIA

The ubiquity of smartphones, popularity of social media, and thriving digital inclusion projects have been key drivers in the success story of India's digital economy thus far. However, minimal digital literacy or low thresholds of educational attainment and awareness among India's Internet users can create significant risks for cyber crime and data misuse.

Additionally, cyber attacks continue to pose risks to critical infrastructure as can be seen with the July 2018[3] incident in the United States, when hackers gained access to the control rooms of utility companies, as well as the September 2019 drone attacks on the Saudi Aramco refineries. The vulnerability of critical technological infrastructure is a growing national security concern.

Since the 2013 National Cybersecurity Policy (NCSP), there have been major paradigm shifts that include the push for digital financial inclusion and next generation technological shifts, such as artificial intelligence, Internet of Things (IoT), and the Smart Cities Mission. In 2015, Prime Minister Narendra Modi outlined the risks that the world faces from a "bloodless" cyber war threat[4]. The criticality of information and communication technology (ICT) and allied areas, such as cybersecurity, is increasing with threats that can be propagated by cyber terrorism, military espionage, corporate espionage, and financial fraud. The Hon'ble Prime Minister observed that, given that India is a major service provider in global technology, solutions around the global problem should emerge from India, not only to enhance cybersecurity in the country, but also to make India a global leader in this realm.

The World Economic Forum (WEF) Global Risks Report 2019[5] notes that malicious cyber attacks and lax cybersecurity protocols led to massive breaches of personal information in 2018 – ranging from a security incident at T-Mobile affecting 2 million users' data to a personal data breach affecting 150 million users of the MyFitnessPal application[6]. In February 2019, India's MeitY outlined India's digital vision of unlocking the potential of a USD 1 trillion digital economy by 2025 from its current value of around USD 200 billion[7]. To realize this potential and build a stable digital economy, it is imperative that all government and private digital systems are safe, secure, and resilient.

As India prepares to refresh its National Cybersecurity Policy, it must move in sync with present day technological and ecosystem realities. India's cybersecurity framework should be able to adapt and be resilient to protect against intrusions at all levels – in the public sector, including critical infrastructure, and citizen services, enterprise systems, and public and private data assets.

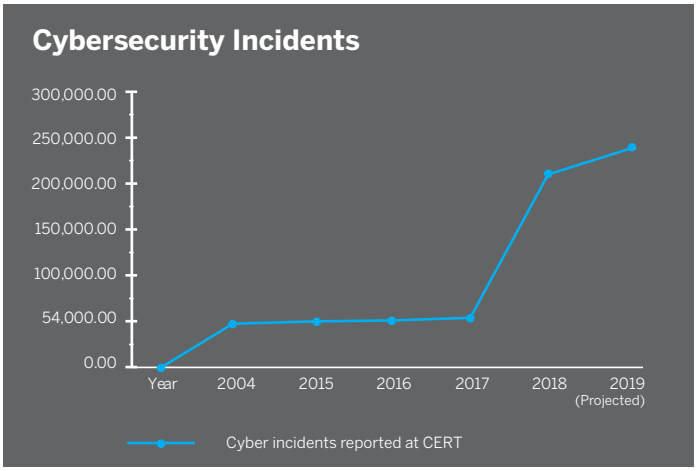
A NATIONAL CYBERSECURITY POLICY MUST BE IN SYNC WITH MODERN TECHNOLOGICAL AND ECOSYSTEM REALITIES AND MUST ADAPT TO FUTURE CHANGES AND DISRUPTIONS, WITH A SYSTEM OF ANNUAL ASSESSMENT AND REVIEW.

2.2 RECENT BREACH INCIDENTS

The Indian Computer Emergency Response Team (CERT-In) has reported a rapid increase in the number of cybersecurity incidents in recent years: a steep four-fold rise of incidents from 53,117 in 2017 to 208,456 in 2018. For 2019, between January and May, there were 105,849[8] such incidents.

The WannaCry and NotPetya incidents showed that attacks targeting the digital elements of utility infrastructure such as power plants, assets such as banks' or hospitals' servers, and devices including mobiles and personal computers, have damaged critical national assets. In March 2017, hackers took advantage of a bug in the Unified Payment Interface (UPI), leading to losses of around INR 250 million for Bank of Maharashtra customers[9]. Other threats to digital payments include malware installations, phishing attacks, SIM card swap attacks, and unreliable devices and infrastructure.

The breach and fraud perpetuated in February 2016 at the Central Bank of Bangladesh, where an estimated USD 81 million loss occurred as it was siphoned off into Manila casinos within a few hours, is the sort of incident that nobody wants. The vulnerability in the system was not technological – it was human error – the failure to change passwords on the system.



[3] Smith, R. "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say". The Wall Street Journal. 23 July 2018. https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110?mod=e2tw&page=1&pos=1

[4] PM remarks at the launch of Digital India week, July 1, 2015, pmindia.gov.in.

[5] The Global Risks Report 2019 – World Economic Forum. https://www.weforum.org/reports/the-global-risks-report-2019

[6] https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#18-t-mobile-about-2-million-4

[7] "India's Trillion Dollar Digital Economy," Govt. of India, 2019, accessed 2 August 2019, https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

[8] Cybersecurity breaches, answer to Lok Sabha question number 1848, 3 July 2019.

[9] https://www.livemint.com/Industry/8HUcQEUGBn0CcPOD6cbfJP/Bank-of-Maharashtra-accounts-lost-Rs25-crore-due-to-UPI-bug.html

SIGNIFICANT DATA BREACHES

2019 Jun	106m credit card customer data (of Capital One) compromised through a firewall breach.	**2018 Jan**	Cosmos Bank in Pune suffers a cyber breach with North Korean hackers stealing USD 13.5m via unauthorized withdrawals and illegal transfers on SWIFT Network.	**2017 Jun**	NotPetya ransomware attack shut down the port of Maersk for 2 days, causing USD 300m in estimated losses. The US and UK attributed it to Russia.
2017 May	E-commerce company Zomato suffers a breach comprising 17m digital records. It discloses in a transparent manner and advises users.	**2016 Oct**	Malware injection on Hitachi's system compromising 3.2m debit cards.	**2014 Nov**	Sony Pictures (in the US) hacked with malware. FBI investigation reveals North Korea to be behind it.

2.3 SECURITY FRAUD IN BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI)

India has seen an exponential growth of digital payments with the use of mobile wallets and apps and net banking and a ten-fold rise in transaction volume in the past four years: from 202 million a month in 2013-14 to 2.03 billion a month in 2017-18. This could lead to increased vulnerability to cyber attacks ranging from phishing and malware to consumer fraud. Greater financial inclusion has brought hundreds of millions of people into the global financial system, but it is concurrent with the challenge of a new generation of Internet users with limited cybersecurity awareness and limited access to security products and services.

Countries such as Brazil, Canada, and Japan have explicitly highlighted identity theft and fraud in relation to "Card Not Present" transactions as a primary threat to their digital payment frameworks. Between March and December 2017, the number of such cases for credit card, debit card, ATM, and net-banking transactions rose to 22,740[10]. In October 2019, Singapore-based IB Group also unearthed a startling revelation on how the dark web[11] hosted a database of credit and debit card details of more than 1.3 million users. Of the total accounts, 98 percent belonged to Indian banks. This is the biggest card database encapsulated in a single file that's been uploaded to underground markets in a single instance, thus highlighting the gravity of ever-increasing skimming and fraud-related threats.

HITACHI ATM INCIDENT

In one of the largest data breaches in India's banking system, 3.2 million debit cards were affected by a malware injection in Hitachi's payment systems. The breach occurred in 2016 between May and July and was reported in October. Hitachi later issued a statement to say that the malware and the penetration into the network had been traced and deciphered, but the amount of data breached during the period could not be ascertained due to secure deletion by the malware. The breach was first detected after some banks raised an alarm over the fraudulent use of their customers' cards in China and the United States, even as these customers were physically in India.

The handling of the incident raised concerns, especially as it was believed that Hitachi (i.e., the entity controlling the concerned infrastructure) failed to inform India's designated Computer Emergency Response Team (CERT-In). Inadequate coordination, incident response, and information -sharing protocols contributed to the breach.

2.4 GOVERNING DATA FLOWS

By harmonizing data privacy laws across Europe, GDPR protects and empowers all EU citizens. In the event of a cybersecurity breach that compromises EU citizens' data, an organisation may face fines of up to 4 percent of their annual global turnover, or €20 million – whichever is greater. GDPR shifts the balance of power to the citizen to whom the personal data belongs, and away from organisations that collect, analyse, and monetise such data (GDPR also applies to data brokers, processors, and controllers).

GDPR protects the privacy of EU citizens while allowing cross-border flow of data. Cross-border data flows enable certain cybersecurity features, allowing for companies to reduce network latency and maintain redundancy for critical data.

As India finalizes its Personal Data Protection Bill, it should align national data protection policies to global practices to harmonize with global standards on data and cybersecurity and bear in mind the tests of legality (existence of law), legitimate goal (law or regulation seeking to achieve a legitimate state aim), proportionality (rationale nexus between objects and means adopted to achieve them), and procedural guarantees (to safeguard against excessive State interference) as laid down by the Supreme Court in its landmark privacy judgement.

The recent revelations from WhatsApp on a targeted Pegasus spyware intrusion by Israel-based NSO Group that led to a number of journalists, academics, and activists being surveilled via their mobile devices (including visibility into private data, such as passwords, contact lists, and text messages) highlights that pernicious tools can affect individual citizens even as the NSO Group has claimed that it only licenses products to vetted state agencies across the globe.

[10] http://164.100.47.190/loksabhaquestions/annex/14/AU6084.pdf.
[11] https://www.deccanherald.com/specials/13-million-indians-bank-card-details-put-on-dark-web-772112.html

3. INSTITUTIONAL FRAMEWORK

The Information Technology Act 2000 continues to be the omnibus legislation that governs cybersecurity policy in the country, and it includes provisions for digital signatures, e-governance, e-commerce, data protection, cyber offences, critical information infrastructure, interception and monitoring, blocking of websites, and cyber terrorism. Rules under the Act are issued from time to time.

In addition to this legislation, regulatory guidelines are issued by sectoral regulators, such as the banking regulator Reserve Bank of India (RBI), telecom regulator Telecom Regulatory Authority of India (TRAI), capital markets regulator Securities and Exchange Board of India (SEBI), and insurance regulator Insurance Regulatory and Development Authority (IRDA), for organizations under their purview.

The Indian Computer Emergency Response Team (CERT-IN), established within the Ministry of Electronics and Information Technology (MeitY), issue alerts and advisories regarding the latest cyber threats and countermeasures on a regular basis, and has published guidelines for securing IT infrastructure.

3.1 NATIONAL CYBERSECURITY POLICY (NCSP) 2013 AND KEY POLICY DEVELOPMENTS

The National Cybersecurity Policy (NCSP) 2013 document was prepared by the Ministry of Communications and Information Technology to facilitate the creation of a secure cyberspace ecosystem and strengthen the existing regulatory frameworks. The mission was to protect information infrastructure systems, build capacities for preventive and response functions to rising cyber threats, and mitigate vulnerabilities and damage from cyber incidents through a mixture of institutional structures, people, processes, technology, and cooperation.

- The Office of the National Cybersecurity Coordinator (NCSC) was established under the National Security Council Secretariat as the nodal agency for cybersecurity. The office coordinates with the central government arms, the states and union territories, and global law enforcement agencies (LEAs) abroad.

- The National Cybersecurity Policy 2013 document is in the nature of a basic framework and provides an initial approach on cybersecurity from the perspective of protecting data of enterprises and individuals. It references protection of strategic digital assets and critical information infrastructure, without significant details of implementation.

Post the NCSP 2013, numerous initiatives to build a strong national cybersecurity ecosystem were launched:

- Critical Information Infrastructure Protection: The National Critical Information Infrastructure Protection Centre (NCIIPC) was established for the protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology Act 2000. It released the first version of its guidelines for protection of critical sectors of the Indian economy in 2013. The second version of was released in 2015. The guidelines specify five levels of control: planning, implementation, operational, disaster recovery/business continuity planning, reporting, and accountability.

- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules 2013): The Rules outline proactive measures for cybersecurity, including forecasts and alerts on security incidents and the prediction and prevention of future incidents. The guidelines, however, lack regulatory accountability in terms of treatment and quality of response to security incidents.

- National Information Security Policy: The Ministry of Home Affairs (MHA) developed the National Information Security Policy and related guidelines in August 2014 for securing classified information in all government organizations.

- Draft IoT Policy: This was released (in two versions) by MeiTY in 2014-15 with a view to solicit inputs from the industry and others on cybersecurity concerns in the IoT ecosystem.

- Draft M2M (Machine-To-Machine) Telecom Roadmap: Developed by the Department of Telecommunications and released on May 12, 2015 discusses cybersecurity issues in M2M interactions.

- SEBI Circular on Cybersecurity and Cyber Resilience of Stock Exchanges: Securities regulator SEBI, as a member of International Organization of Securities Commissions (IOSCO), issued a circular in July 2015 adopting the Principles for Financial Market Infrastructures (PFMIs) laid down by the Committee on Payments and Market Infrastructures (CPMI) at IOSCO. Principle 17 of PFMI requires that systemically important market infrastructure institutions "should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through use of appropriate systems, policies, procedures, and controls. The framework adopts the five functions approach laid down by the US-based standard settings organization, National Institute of Standards and Technology (NIST), comprising of "Identify, Protect, Detect, Respond, and Recover."

- A Draft National Policy on Encryption under Section 84A of the Information Technology Act 2000 was published on September 21, 2015, and invited comments from the public, but was withdrawn two days later due to its unfeasible and unclear provisions with respect to the usage of encryption technologies.

- RBI Security Framework for Banking: The Reserve Bank of India in a June 2016 advisory on "Cybersecurity Framework in Banks" advised banks to improve and maintain customer awareness and education with regard to cybersecurity risks. Banks were also asked to educate customers on the downside and risk of sharing their login credentials / passwords, etc. with any third party or vendor, and the consequences thereof. Banks were asked to strengthen their cybersecurity protocols and asked them to report incidents of security breaches. The circular advised banks to evaluate the controls on various aspects including information sharing arrangements with CERT-In, RBI, and the Institute for Development and Research in Banking Technology (IDRBT).

- CERT-In Advisories & Circular on CISOs: CERT-In advised all banks, Pre-paid Payment Instrument (PPI) issuing agencies, and other stakeholders to report cybersecurity incidents without delay to the Indian Computer Emergency Response Team. In March 2017, CERT-In issued guidelines for assigning roles and responsibilities of Chief Information Security Officers (CISOs) in ministries/departments and related agencies managing ICT operations. The core functional aspects of the officers lay in securing applications or infrastructure and compliance.

- Guidelines on Information Security for Insurers: The insurance regulator, Insurance Regulatory and Development Authority of India (IRDAI), issued "Guidelines on Information and Cybersecurity for Insurers" in March 2017 for providing responsibilities of insurers in ensuring that adequate mechanisms are put in place on issues relating

to information and cybersecurity, including requirements related to CISOs.

- Proposed CERT-Fin: The CERT-IN Director General in 2017 led a Working Group that looked at the proposed creation of a separate CERT for the financial services sector and invited public comments. The entity is yet to be constituted.

- Creation of Centre of Excellence for Cybersecurity, IB-CART at IDRBT: CERT-IN has created a Centre of Excellence (CoE) for cybersecurity within IDRBT in Hyderabad. IDRBT works closely with government-owned banks and other public agencies on cybersecurity related research and issues. The IB-CART, established within IDRBT, is intended to be a common platform for sharing breach information amongst banking entities, on the lines of the FS-ISAC in the US and elsewhere.

- National Digital Communications Policy 2018: In tune with the advancements in the digital communications ecosystem, the National Telecom Policy has now been rechristened as the National Digital Communications Policy (NDCP) wherein the Telecom Commission has been now re-designated as the Digital Communications Commission. The central strategic objectives of the policy are to achieve by 2022 (a) broadband for all and (b) propel India to top 50 countries on the International Telecommunication Union (ITU) ICT Development Index. On the three missions to achieve these objectives, "Secure India" outlines a focus on ensuring individual autonomy and choice, data ownership, privacy, and security, while recognizing data as a crucial economic resource.

- Ministry of Finance Report on Fintech: In September 2019, a Ministry of Finance committee submitted its final report on fintech-related issues. The Committee report also looks at fintech for cybersecurity and fraud control. The report recommends that fintech firms specializing in this field should be encouraged to set up their businesses in India and provide necessary regulatory approvals for expanding their services in the country.

- Creation of Power-Sector CERTs: Four power sector CERTs have been created to oversee power generation, transmission, and distribution parts of the electricity value chain. This is the only sector with a developed ecosystem of functioning CERTs for sharing breach information.

- Creation of ReBIT within RBI: The central bank RBI created ReBIT as its IT subsidiary in 2018, focused primarily on the issue of data and cybersecurity across the institution and to advise it on cyber risks in the banking sector.

- CERT-In Training and Capacity Building with Government Agencies: CERT-IN conducts regular training programmes for network / system administrators and CISOs of government and critical sector organizations regarding securing IT infrastructure and mitigating cyber attacks (24 such training programs were conducted in 2018). Cybersecurity mock drills and exercises are being conducted regularly to enable assessment of cybersecurity posture and preparedness of organizations in government and critical sectors. 43 exercises have so far been conducted by CERT-In where organizations from different sectors such as finance, defence, power, telecom, transport, energy, space, and IT participated.

- National Cyber Coordination Centre (NCCC): The NCCC was set up to generate necessary situational awareness of existing and potential cybersecurity threats and enable timely information sharing for proactive, preventive, and protective actions by individual entities. Phase-I of NCCC has been made operational.

- MeitY Initiatives: 84 security auditing agencies have been empaneled to support and audit implementation of Information Security Best Practices. The government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) that provides detection of malicious programs and free tools to remove them. MeitY has also set up a Cyber Lab at National Law School of India University (NLSIU) Bangalore for creating cyber crime awareness and cyber forensic training.

- Cyber crime Awareness Amongst Law Enforcement Agencies (LEAs): MeitY has engaged with the Data Security Council of India (DSCI) for creating cyber crime awareness among law enforcement authorities through workshops at different cities across India. For security awareness and capacity building, MeiTY has also set up Cyber Forensics Training Labs at policy headquarters in (i) all north-eastern states in collaboration with CDAC[12], (ii) cities of Mumbai, Pune, Bangalore, and Kolkata, with the help of DSCI for creating Cyber Crime Awareness and Cyber Forensics Training for both LEAs and judiciary (included judges, judicial officers, and public prosecutors).

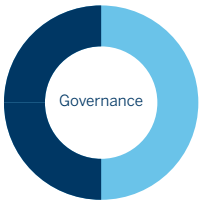
[12] Centre for Development of Advanced Computing

Key Cybersecurity Agencies	Notes
National Cybersecurity Coordinator (NCSC)	The central agency coordinating with different agencies in the national level on cybersecurity.
National Critical Infrastructure Information Protection Centre (NCIIPC)	Statutory nodal agency for the protection of critical information assets, excluding the armed forces and a few strategic sectors.
Computer Emergency Response Team (CERT-In)	Established under MeiTY. It reports to the NCSC on security incident handling and prevention as well on security assurance frameworks.
National Cyber Coordination Centre (NCCC)	Looks at situational awareness of existing and potential cybersecurity threats.
Cyber and Information Security Division	Deals with cyber and information security at the Ministry of Home Affairs (MHA) level.
Indian Cyber Crime Coordination Centre (I4C)	A Ministry of Home Affairs (MHA) approach to combat cyber crime in a coordinated manner, with components such as a threat analytics unit, crime reporting portal, forensic lab, training center, etc.
Defence Cyber Agency (DCA)	Setup to work in conjunction with National Cybersecurity Coordinator to look at cyber issues in the military context. [13]
Cyberspace Agency	Expected to be formed soon.

3.2 REVIEW OF THE NCSP 2013

The National Cybersecurity Policy 2013 document was India's first formal policy document dedicated exclusively to cybersecurity. From 2013 to 2019, the policy has served India well.

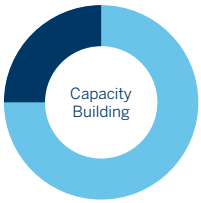
FTI Consulting reviewed the NCSP 2013 and identified the following areas for improvement:



Area of Action
- Core institution
- Supporting pillars
- International cooperation

Comments

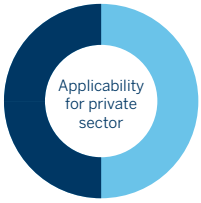
International cooperation and advocacy need more prominence – the policy does not articulate a leadership role for India in the global cybersecurity arena.



Area of Action
- Education and training
- Building trust in law enforcement

Comments

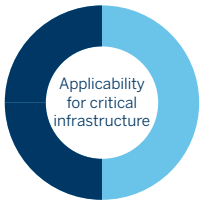
The policy envisions creating a workforce of 500,000 security professionals without a clear roadmap.



Area of Action
- Public-private partnerships
- Awareness efforts
- Investments in creating secure cyber environment

Comments

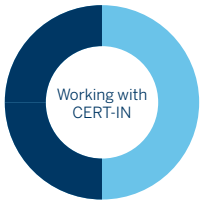
Initial Joint Working Group was set up with a public-private partnership mechanism. Barring creation of a security testing lab, no other significant achievements.



Area of Action
- Building a robust critical infrastructure
- Partnerships with other sectors

Comments

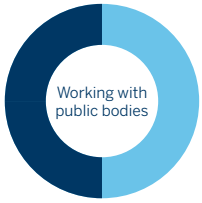
Established NCIIPC to oversee critical sectors such as transport, power and energy, telecom, govt., banking and financial services as well as strategic and public enterprises. No sectoral Information Sharing and Analysis Centre (ISAC) mechanism yet for these areas.



Area of Action
- Collaboration with the public and private sector
- Building a CERT network

Comments

Enforceability of CERT-IN mandated notification is unclear, in terms of awareness and frequency of such incident reporting from private sector entities.



Area of Action
- Awareness raising campaigns
- Education and training
- Establish a culture of cybersecurity and resilience

Comments

CERT conducts capacity building programmes (24 of them in 2018). Stronger "culture of security" needed, incl. standard operating procedures around protecting against data misuse; use of public e-mail (Gmail, etc) at government agencies. (A 2015 email policy has not been strictly implemented.)

[13] https://economictimes.indiatimes.com/news/defence/india-in-final-stages-of-setting-up-defence-cyber-agency/articleshow/67540186.cms?from=mdr

4. GLOBAL TRENDS

4.1 INTERNATIONAL BEST PRACTICES

Area of Action	United States	Europe	Singapore
Governance	• The National Security Council's **Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC)** in the White House is the primary policy coordinator. • ICHPC is co-chaired by the Homeland Security Council and **Cybersecurity Coordinator (CSC)** at National Security Council's Cybersecurity Office. CSC leads interagency development of national cybersecurity strategy and policy and oversees agencies for implementation of policies.	• **European Union Agency for Cybersecurity (ENISA), CERT-EU and EC3 (Europol)** are the leading agencies in Europe – there is a fragmented approach with no one central point of reference. • The EU adopted its first cybersecurity strategy in 2013 (similar timeframe as India). It has been proactive in ensuring periodic reviews and updating elements of its framework. In 2019, the European Parliament adopted the EU Cybersecurity Act which gave a permanent mandate to ENISA, created EU's cybersecurity certification framework, set up a rapid emergency response framework and established EU-wide cyber research competence centres.	• A recently introduced **Cybersecurity Act of 2018** authorized the **Cybersecurity Agency of Singapore (CSA)** to prevent and respond to cybersecurity threats and incidents. The CSA's powers may be exercised according to the severity of the cybersecurity threat or incident and measures the required response. • A light-touch licensing framework for cybersecurity service providers exists - one of a few countries with legislation for a licensing scheme.
Cyber Incident Response and Information Sharing	• The Department of Homeland Security (DHS) works closely with local governments, through interstate information sharing arrangements, such as the multi-state information sharing and analysis centre. • Government-monitored information sharing platforms for anonymous disclosures exist. The US Cybersecurity and Information Sharing Framework (2015) offers incentives and liability protections for voluntary disclosure.	• The Network and Information Security Directive (NIS) has cybersecurity requirements and breach reporting obligations for energy, transport, and healthcare sectors, deemed critical national infrastructure. • Member states, under NIS, have to adopt national cybersecurity strategies and create national authorities.	• The National Cybersecurity Centre (NCSC) monitors the cyber threat landscape to maintain cyber situational awareness and anticipate future threats. • In the event of large-scale cyber incidents involving multiple sectors, NCSC coordinates with the sector regulators to provide a national level response and facilitate quick alerts to cross-sector threats.
Critical Information Infrastructure (CII) Protection	• The DHS releases monthly toolkits for CII protection and identification. • Sector-specific plans to supplement its National Infrastructure Protection Plan. They have identified private-sector engagement, development of sector-specific plans, and collaboration with sector-specific agencies as pillars for CII protection.	• The European Commission (EC) identifies 11 critical sectors. Critical services should be tailored to the needs of jurisdictions and that effective collaboration with the private sector is fundamental to identifying and protecting CII assets.	• The Cybersecurity Agency (CSA) is responsible for 11 critical sectors. Any computer system directly providing "essential services" is CII. • Obligations fall on CII owners to protect systems against attack, with a "whole-of-government" exercise to test cyber incident emergency response frameworks across critical sectors.
Budget	• FY 2020 President's budget is USD 17.4 billion for cybersecurity activities, a 5 percent increase[14] from FY 2019. There are some undisclosed components and amounts outside of this budget amount.	• In July 2016, the EU announced a public-private partnership, whereby it invested EUR 450 million and encouraged private industry to bring total investment to EUR 1.8 billion.	• Singapore had announced[15] that it would spend 8 to 10 percent of its IT budget on cybersecurity in line with similar practices in Korea (10 percent spend) and Israel (8 percent spend) across government.
Standards Setting	• Cybersecurity Enhancement Act of 2014 gives National Institute of Standards and Technology (NIST) the authorization and support to develop voluntary standards to reduce the risk of cyberattacks to critical infrastructure.	• ENISA has rolled out a joint initiative for the EC and industry on cybersecurity certification that embodies a "duty of care" principle to reduce products, services, and systems vulnerabilities while putting the onus of cybersecurity for all connected devices on the private sector.	• Public and private sectors work together. In 2013, InfoComm Media Development Authority (IMDA), Enterprise Singapore, and industry players developed the world's first multi-tiered cloud computing standard to address security of cloud services by government agencies and private sector. • The Singapore Standards Council is developing new standards for autonomous vehicles and IoT security.

[14] https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf
[15] https://www.csa.gov.sg/news/speeches/min-opening-speech-at-govware2015

4.2 GLOBAL CYBERSECURITY NORMS AND FRAMEWORKS

The OECD's report, Cybersecurity Policymaking at a Turning Point[16], reveals that cybersecurity strategies developed by different nations share some common elements. Shared approaches include four elements:

1. States' need for enhanced internal operational coordination;
2. Reliance on private-public partnerships;
3. Interest in improved international coordination; and
4. The need to protect fundamental values in cyberspace.

GLOBAL CYBERSECURITY NORMS AND FRAMEWORKS

There have been multiple global forums such as the Global Commission on the Stability of Cyberspace. The appeals tend to rarely go into the conceptual contours of what the specifics of these norms would comprise of and how it would be implemented. As a result, policy discussions and media coverage often apply the term to policy instruments that are not, in fact, norms. Simply solving the puzzle of what substantive normative prescriptions might address given a cybersecurity problem and announcing this to the world does not create a norm. Others need to buy in and recognize that the norm's behavioural prescriptions apply to them (or to other actors who can be held accountable)[17].

The US government saying that commercial cyber espionage is bad did not create a norm countering cyber espionage. Only when China, the UK, and other G20 countries signed on did a norm start to take shape. Widespread adoption of the National Institute of Standards and Technology (NIST) voluntary cybersecurity framework, which includes an array of norms, helped actors signal their intentions and build trust in supply chains (and with governments).

It is important to evaluate some of the key directions on global frameworks in the past few years:

• ITU Global Cybersecurity Agenda & Global Cybersecurity Index (GCI): The ITU GCI identifies five strategic pillars: legal, technical, organizational, capacity-building, and cooperation[18]. The Global Cybersecurity Index (GCI) is a product that emerges from the ITU Plenipotentiary Resolution 130 on strengthening the role of ITU in building confidence and security in the use of information and communication technologies. The goal is to foster a global culture of cybersecurity and its integration at the core of information and communication technologies. The first GCI survey was conducted in 2014. A snapshot of key findings from the GCI reports is further outlined in the section below.

• Tallinn Manual 2.0: The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations[19], authored by 19 international law experts, is a considerably expanded second edition that was unveiled in 2017. It is an influential resource for legal frameworks around cyber issues developed at NATO's Cooperative Cyber Defence Centre of Excellence. The manual details four sections comprising general legal principles in the cyber domain as well as specific specialized legal regimes.

• UN Group of Governmental Experts (UN GGE): The UN GGE focuses on developments in the field of information and telecommunications in the context of international security and is comprised of 20 nations equitably distributed based on geography. It includes nation states regarded as leaders in cyber areas. The UN GGE released a consensus report in 2015 which proposes norms of responsible behaviour and includes commentary on applicable principles of international law in the cyberspace. A final consensus could not be reached due to its rejection by a few states including Cuba and, reportedly, Russia and China. Three points were flagged as contentious issues:

  – the right to respond to internationally wrongful acts (a veiled reference to countermeasures);

  – the right to self-defense; and

  – international humanitarian law, clearly applicable to cyber activities.

Equally clearly, the failure of the GGE was partly caused by the politicisation in the cyber context of well-accepted international law norms.

• The UN General Assembly adopted two resolutions on cyber[20], one creating a working group to study cyber norms and possible dialogues, and another setting up a working group of government experts to study applicability of international law to states in cyberspace. UN Secretary General Guterres created a high-level panel on digital cooperation, bringing together public and private sector stakeholders.

  – The resolution tabled by the Russian Federation entitled "Developments in the field of information and telecommunications in the context of international security"[21] was passed by a vote of 109 in favour to 45 against, with 16 abstentions. The resolution encapsulated the Sino-Russian view.

  – The UN General Assembly also approved the draft resolution "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" tabled by the United States, with 139 in favour to 11 against, with 18 abstentions[22].

  – India voted for both resolutions. This is synchronous with India's strategic autonomy exercised through positive relations with both the US and Russia. The rationale for this vote is to provide an approach to a position that suits a developing economy's context.

• Paris Call for Trust and Security in Cyberspace: This was launched by French President Emmanuel Macron in November 2018, as a high-level declaration for cooperation endorsed by 64 countries, international NGOs, universities, and hundreds of private companies.

• Open Ended Working Group (OEWG) at UN: The UN General Assembly established the OEWG on informational security that convened for the first time in 2019 around consultative meetings with industry, NGOs, and academia on developing norms of responsible state behaviour in cyberspace.

• Cybersecurity Tech Accord: Around 34 global technology and security companies came together in the 2018 RSA Conference to sign a Cybersecurity Tech Accord to advance online security and resilience around the world. The signatories of the Tech Accord pledge to "protect and empower civilians online and to improve the security, stability, and resilience of cyberspace."

[16] http://www.oecd.org/sti/ieconomy/cyber security%20policy%20making.pdf
[17] https://carnegieendowment.org/2017/11/30/cyber security-and-concept-of-norms-pub-74870
[18] https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cyber security-matters.html
[19] https://ccdcoe.org/research/tallinn-manual/
[20] https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/
[21] https://undocs.org/A/C.1/73/L.27
[22] https://www.un.org/press/en/2018/gadis3619.doc.htm

ITU GLOBAL CYBERSECURITY INDEX (GCI)

The ITU framework for international multi-stakeholder cooperation in cybersecurity aims to build synergies between current and future initiatives, and focuses on following five pillars:

1. LEGAL: Measures based on existence of legal institutions and frameworks dealing with cybersecurity and cyber crime.

2. TECHNICAL: Measures based on existence of technical institutions and framework dealing with cybersecurity.

3. ORGANISATIONAL: Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

4. CAPACITY BUILDING: Measures based on the existence of research and development, education and training programmes, certified professionals, and public sector agencies fostering capacity building.

5. COOPERATION: Measures based on the existence of partnerships, cooperative frameworks, and information sharing networks.

4.2.1 MAPPING INDIA'S PROGRESS ON THE CYBERSECURITY INDEX

Mapping India's progress on the five pillars of the ITU GCI, we found the following shifts from 2017 to 2018:

Country	2018 Rank	2018 GCI Score[23]	2017 Rank	2017 GCI Score
United States	2 =	0.926	2	0.919
United Kingdom	1 ▲	0.931	12	0.783
Singapore	6 ▼	0.898	1	0.925
India	47 ▼	0.719	23	0.683
Total Countries Surveyed	193		134[24]	

In 2017, the global commitment level had a distribution in all the six regions of ITU, eliminating geographical theories of commitment. However, in 2018, only three regions are represented having the most level of commitment: six countries from the Europe region, three from the Asia-Pacific region, and two from the Americas region.

While India displays a slight improvement in the overall score from 0.683 to 0.719, we find that India slips 24 places on the overall ranking of progress. A major reason is that only 21 countries were considered to be in a leading stage of development in 2017, compared to 54 countries in 2018 that were considered as having high levels of national cybersecurity commitment.

> A PRIMARY REASON FOR INDIA'S SLIP IN RANK FROM 5 TO 47 IN FOUR YEARS IN THE ITU GLOBAL CYBERSECURITY INDEX WAS ITS WEAK COLLABORATION BETWEEN PUBLIC AGENCIES, GOVERNMENT, AND INDUSTRY.

LIKELY REASONS FOR INDIA'S UNDERPERFORMANCE AS A MATURING CYBERSECURITY STATE

The 2018 report does not provide any breakdown on the individual pillars (legal, technical, organizational, etc.) for India. We can, however, reference the 2017 report to look for the areas of shortcomings in India's position as a maturing[25] cybersecurity state:

- India's score is weak on parameters of public-private partnerships as well as intra-agency partnerships.
- On standards, both at the organizational level and professionals' level, India has a medium score.
- There were no major incentive mechanisms (e.g. toward improving competitiveness in related areas, or towards creating an adequate domestic ecosystem)

4.3 GLOBAL, REGIONAL, AND BILATERAL PARTNERSHIPS WITH INDIA

Shared notions of cyber governance have yet to bear fruit due to three key factors:

1. The philosophical divide on the nature of cyberspace with two groups, one driven by the United States (and backed by G7 and EU countries) which sees the Internet as a free-flowing entity to be driven by market competition and light-touch regulation.

2. The difficulties of tracing back and attributing a cyber attack to the original perpetrator incentivises states and non-state actors to continue engaging in low-intensity cyber attacks against states who retain military and strategic advantages in traditional domains of warfare. This is because the attacker sees the benefits of mounting cyber attacks as outweighing the risks of getting caught.

[23] The Score is measured on a scale of 0 to 1.

[24] Participated in the GCI survey

[25] The gradations in the GCI are initiating, maturing and leading stages, where initiating indicates countries that start to make commitments in cyber security whereas leading signifies countries that demonstrate high commitment across all five pillars of the index.

3. There has been increasing participation of heterogeneous non-state actors in the global cybersecurity architecture – both as perpetrators of cyber attacks and norm-entrepreneurs*. This heterogeneity in needs, motivations, and ideologies of these actors poses an obstacle to developing a uniform and cohesive approach to cyber regulation.[26]

MULTI-STAKEHOLDER PARTNERHIPS

These, below, are some notable efforts to form multi-lateral partnerships around cybersecurity:

- In an effort to defend Indian political parties and campaigns against cyber attacks ahead of the country's elections in spring 2019, the International Republican Institute (IRI) and the National Democratic Institute (NDI) partnered with Microsoft and Defending Digital Democracy (D3P)—a project of the Harvard Kennedy School's Belfer Centre— to launch the Belfer Centre's Cybersecurity Campaign Playbook in India[47].

- In January 2018, the World Economic Forum announced the creation of its Global Centre for Cybersecurity (C4C). The C4C has been set up through a network of partners comprised of global companies (such as Accenture and Palo Alto Networks), intergovernmental organizations (such as Europol, ITU, Israel National Cyber Directorate), and research institutions (such as Observer Research Foundation, UC Berkeley). The C4C is setting out to foster global governance, stimulate efforts to reduce cybercrime, facilitate global cyber crisis management, anticipate future threats and risks, and develop a global cybersecurity workforce. The first year of the C4C's operation looks promising, with an agreement signed with Interpol on capacity building and public-private coordination and steps taken to expand cooperation with China's Cyberspace Administration[28].

- In April 2019, the United States and international cybersecurity officials called for greater international cooperation to combat Internet crime and align cyber activity during the Atlantic Council's 8th annual International Conference on Cyber Engagement (ICCE). David Koh, chief executive of the Cybersecurity Agency in Singapore, called for like-minded nations to establish "a rules-based cyberspace based on applicable international law and the adoption of voluntary operational norms[29]." He argued that what has been achieved for physical domains, such as the maritime and aviation sectors, must be sought for cyberspace as well.

- The Global Commission on the Stability of Cyberspace (GCSC) was established as result of the Global Conference on Cyberspace (GCCS) held in the Netherlands in 2015 and was inaugurated in 2017[30]. It aims to promote mutual awareness and understanding among the various communities working on issues related to international cybersecurity. The Commission intends to support policy and norms coherence related to security and stability in and of cyberspace. The Commission is comprised of 27 commissioners representing a wide range of geographic regions as well as government, industry, technical, and civil society stakeholders. Latha Reddy, former Deputy National Security Adviser of India has been one of the commissioners. Within the Commission, a research advisory group conducts scientific research to support the deliberations and publications of the commissioners. The group's core interaction is founded on four email lists dedicated to areas that the Commission works on: international peace and security of cyberspace, Internet governance, law, and technical and information security. The primary partners of the GCSC are the Government of The Netherlands, Microsoft Corporation, and the Government of Singapore.

BILATERAL PARTNERSHIPS: INDIA-US

- The India-US cyber relationship is enmeshed in a broader discourse around the global governance of common digital spaces. This was aptly illustrated in 2015, when India signaled its willingness to endorse the rules of the road set by the United States with a "multi-stakeholder" Internet governance model.

- In a Track 1.5 Cyber Dialogue of 2016, with involvement of the top cybersecurity brass from both countries, the need for multi-stakeholder dialogue was underscored. Data sharing requests and Mutual Legal Assistance Treaties (MLATs) have typically been the key priority areas in this stream with an agreement on the need for a more streamlined process in addressing law enforcement concerns.

- Cooperation on cyber issues is a key component of the bilateral relationship between India and the United States. The two countries have created a wide-ranging strategic partnership that reflects their shared values, democratic traditions, national security and economic interests, and common vision and principles for cyberspace via the US India Cyber Framework Agreement signed in 2016. The core elements of the agreement[31] included:

  – Identifying and cooperating on implementation aspects of cybersecurity best practices;

  – Information sharing in line with existing bilateral arrangements ;

  – Developing joint mechanisms for cooperation to mitigate cyber threats likely to affect the security of ICT infrastructure and information systems ;

  – R&D and security standards setting related to cooperation

[26] https://cis-india.org/internet-governance/files/cyberspace-and-external-affairs
[27] https://www.iri.org/resource/iri-partners-ndi-and-harvard-belfer-center-indian-cyber security-campaign-playbook
[28] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/advancing-global-cyber security-five-questions-for-the-world-economic-forums-global-centre-for-cyber security/
[29] https://www.atlanticcouncil.org/blogs/new-atlanticist/international-engagement-key-to-building-cyber-resilience
[30] https://dig.watch/actors/global-commission-stability-cyberspace
[31] https://in.usembassy.gov/framework-u-s-india-cyber-relationship/

– Improving capacities of LEAs through joint training initiatives; and

– Promoting voluntary norms on responsible state behaviour including norms identified by the UN Group of Governmental Experts in the field of information and telecommunications.

Indian companies and users stand to benefit from cutting-edge products and services offered by US operators in the development of testing criteria and technical protocols. If security reasons have compelled India—whose electronics supply chain relies almost entirely on foreign products—to develop its own unique standards, there is also room to re-examine them. The conversation on standards is both a bilateral and plurilateral one. As the International Telecommunications Union has lent itself to government participation at the exclusion of other stakeholders, multi-stakeholder bodies, like the Internet Engineering Task Force, should make their platforms accessible to the private sector in India and other emerging economies.

> INDIAN COMPANIES AND USERS BENEFIT FROM CUTTING-EDGE PRODUCTS AND SERVICES FROM GLOBAL TECH PIONEERS. SECURITY-DRIVEN POLICIES AND ACTIONS, WHILE CRITICAL, SHOULD AVOID DISRUPTING ELECTRONICS SUPPLY CHAINS, OR DATA FLOWS CRITICAL TO OUR TECH INDUSTRIES.

BILATERAL PARTNERSHIPS: INDIA-EU

The EU outlined a partnership for sustainable modernisation and rules-based global order in a joint communication last year that aims to strengthen the strategic partnership at a plurilateral level[32]. The strategy recognizes India as an important service provider to the EU, and cybersecurity is a joint priority. The EU and India should engage more with each other to stabilize cyberspace and develop global norms underpinned by a shared commitment to a free, secure, stable, peaceful, and accessible cyberspace. Proposed action items include:

- Exchange expertise on cybersecurity and hybrid threats.
- Conclude working arrangements to foster cooperation between Europol and Indian law enforcement institutions.
- Develop an EU branding in India with more targeted public and digital diplomacy initiatives by systematically reaching out jointly with EU Member States at national and regional levels.
- Promote common understanding of underlying global, regional, and bilateral trends, as well as socio-economic issues, through regular think-tank exchanges, track 1.5 and 2.0 dialogues, including the EU Institute of Security Studies.
- Promote common approaches and standards to digital transformation, promote data protection values, and facilitate data flows by supporting India's efforts to develop its legislation with a view towards adopting a data adequacy decision by the European Commission.

BILATERAL PARTNERSHIPS: INDIA WITH SINGAPORE AND ISRAEL

- India and Singapore had signed a Memorandum of Understanding (MoU) in January 2016, to focus on the establishment of a formal framework for professional dialogue, CERT-CERT related cooperation for operational readiness and response, collaboration on cybersecurity technology and research related to smart technologies, exchange of best practices, and professional exchanges of human resource development.
- India and Israel signed a MoU in January 2018 on cybersecurity cooperation. It envisages cooperation in the field of cybersecurity to develop, promote, and expand cooperation in the field of human resource development through various platforms and arrangements, such as training programmes, skill development, and simulator-based hands-on training. It also envisages collaborating in the field of cybersecurity resilience, promoting B2B cooperation in cybersecurity and facilitating industrial summits.

[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:028:FIN

5. ASSESSMENT OF INDIA'S CYBERSECURITY ECOSYSTEM

5.1 CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

The National Critical Information Infrastructure Protection Centre (NCIIPC) is designated as the national nodal agency in respect of critical information infrastructure protection (CIIP), in the identified areas of transport, power and energy, telecom, government, banking and financial services as well as strategic and public enterprises. Some of the critical functions of the NCIIPC encompass the following:

- National nodal agency for all measures to protect the nation's critical information infrastructure.
- Protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare, and other threats.
- Identification of all critical information infrastructure elements for approval by the appropriate government for notifying the same.
- Provide strategic leadership and coherence across governments to respond to cybersecurity threats against the identified critical information infrastructure.
- Coordinate, share, monitor, collect, analyze, and forecast national-level threats to critical information infrastructure (CII) for policy guidance, expertise sharing, and situational awareness for early warning or alerts. The basic responsibility for protecting a CII system shall lie with the agency running that CII.

The active participation of governmental regulatory agencies from sectors such as aviation, communications, offshore oil and gas, and banking are of prime importance. In this regard, the following considerations are imperative to bear in mind:

RECOMMENDATION: Self-organized, self-run, and self-governed private sector councils, known as Sector Coordinating Councils, are required to facilitate discussion and representation of owners and operators of critical infrastructure. Cross-sector coordination is also essential. The new strategy must look at "criticality" as a measure to identify the critical elements within the infrastructure to allocate utmost priority. Such a qualitative/quantitative approach would aid policymakers in India to focus on priority areas.

- IDENTIFYING CRITICAL ASSETS/ PROCESSES/ SYSTEMS: The identification of critical assets, processes, and systems within critical infrastructure sectors is the foundation of an effective CIIP strategy. This exercise begins with every department or unit being involved, in providing an assessment of the assets. There is a general acceptance of two facts: (a) not all the elements of critical infrastructure are critical; and (b) it is practically impossible to secure each and every element of critical infrastructure, all the time, from all probable threats, and that is due to various technical and financial constraints.
- DETANGLING INTERDEPENDENCIES: One of the primary reasons for critical infrastructure being so complex is the cascade of dependencies and the web of interdependencies. Innovative simulations or software tools to model the flow of entities, services, and materials are a direct outcome of the national policies marking interdependencies as a priority area for advanced research.
- FOCUS ON CRITICAL INFRASTRUCTURE RESILIENCE: Despite having the best of technology, management, or security policies and practices at one's disposal, it is practically impossible to secure all critical elements of infrastructure against all eventualities. The evolving trend now is to heighten the resilience of the CII to such an extent that the critical business functions or services are restored as early as possible, and cascading effects are mitigated. This is a significant departure from the earlier notions of security centred on building defences. Resilience is commonly embedded in processes, rather than individual physical assets.
- BUSINESS CONTINUITY AND CRISIS MANAGEMENT PLANS: Plans at the organizational level are the building blocks for sectoral and national resiliency of critical infrastructure; therefore, the responsibility and execution lie with the owners and operators of critical infrastructure.
- ADOPTING AN "ALL-HAZARDS" APPROACH: The probability of a threat actor being able to execute an attack exploiting a vulnerability is a desired input for quantitative risk assessment. Preparedness encompasses a broad range of both manmade and natural hazards, which also includes acts of terrorism. From an operator's perspective, the source or cause of the incident is secondary, while the continuity of service and the mitigation of unanticipated cascading effects is the primary task at hand.
- AMALGAMATION OF REGULATORY AND PARTNERSHIP MODELS: Critical infrastructure owners and operators are unevenly spread across the governments, private, and public sectors. With deregulation of sectors such as energy, transportation, and communication, multiple players with varying degree of maturity in security practices are now part of the critical infrastructure. At a strategic level, governments are inclined to enforce supervision over the best practices and guidelines issued for the critical infrastructure sectors.

[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:028:FIN

• STRATIFIED INFORMATION SHARING: Once a strategy and an executive apparatus are in place, information sharing is the key driver of an effective CIIP policy initiative. The scope of information is wide: it encompasses threat information, incident reporting/analysis, best practices, protective measures, advisories, vulnerability or audit notes, crisis management, alerts, and warnings. Information sharing is vital to communication, situational awareness, policy implementation, collaboration, and coordination. Graduating from the hierarchical model, information sharing now works like a network, and there are multiple agencies, strata, and channels, both formal and informal.

> THERE IS A NEED FOR NEW SELF-GOVERNING 'SECTOR COORDINATING COUNCILS' TO REPRESENT MULTI-STAKEHOLDER VIEWPOINTS. STRATEGIES FOR SECURING CRITICAL INFRASTRUCTURE SHOULD INVOLVE OWNERS AND OPERATORS OF SUCH INFRASTRUCTURE.

For incident reporting, there must be SOPs that clearly define timeframes for reporting and resolution of incidents, including action taken reports and notifying users/entities of any follow-up actions. There is a special need to outline a clear process for third parties (including white hat hackers or whistle-blowers) to report vulnerabilities, both to private and public sector organizations, such that:

- The report is noted and acknowledged.
- Action is taken and reported to a regulator or concerned CERT/NCIIPC.
- There is no fear of reprisal for a bonafide reporting party.

As an example, if a third party detects a vulnerability in an automotive system, they should be able to report it to the manufacturer (who must have relevant contacts clearly published online) as well as to the Transportation CERT (or CERT-IN, or NCIIPC). The concerned CERT should mention on its website that a vulnerability has been reported concerning the specified vendor, without details of the product, and vendor response and/or a fix for the vulnerability, if applicable, is awaited. Subsequent to the vendor's report, the product name, nature of vulnerability, and fix may be updated.

The Policy should require all concerned manufacturers or service providers in the six critical infrastructure areas to publish contacts on their websites for reporting product vulnerabilities of any kind, including cybersecurity vulnerabilities.

RECOMMENDATION: Informed by global benchmarks, India must frame a CII protection plan that articulates the roles and responsibilities and coordinating structures that support how a nation will respond to and recover from significant cybersecurity incidents affecting critical infrastructure. A national incident response plan provides guidance to enable a unified whole-of-government, whole-of-nation, and internationally coordinated approach to response and recovery during a significant cybersecurity incident affecting critical infrastructure. Vulnerability reporting (by product/service vendors, agencies, as well as third parties) and reporting of action taken by vendors/service providers, needs special attention.

5.2 SECURING E-GOVERNANCE ECOSYSTEM

The Digital India Mission and the National AADHAAR Biometric Identity Authentication System have made cybersecurity an imperative for secure delivery of e-governance projects managed by various state-owned agencies and extended third parties. E-governance itself is comprised of two interfaces: the citizen interface and the back-end interface. Both need to be adequately secured to deliver services in a safe manner, and the government has taken some measures.

• The MHA had issued its National Information Security Policy & Guidelines which could be taken as a reference by all the central ministries, state governments, and public sector undertakings (PSUs) for developing their own information security and control mechanism. However, these were broad-level guidelines, and government agencies need to understand their specific requirements, processes, and functions in driving implementation frameworks. These considerations could entail: (a) the government's user lifecycle; (b) the type of data accessed and processed; and (c) the lifecycle of this data. An ideal cybersecurity framework should also not be constrained by changes in the nature and shape of evolving technologies. Specific functional responsibilities can be outlined with functional entities – for instance RBI set up Reserve Bank Information Technology Private Limited (ReBIT) to take care of information technology requirements for the RBI, and to an

extent its regulated entities. One of the four verticals for ReBIT is to enhance the trust and reliability of RBI's infrastructure for assurance and resilience.

- The Government could look at further efforts around implementing its Cyber Crisis Management Plan (CCMP). CERT-In had outlined that the purpose of this plan was to establish the strategic framework and guide actions around recovering from a cyber incident. The plan is especially designated for protection of critical information assets across various government ministries in countering cyber attacks and cyber terrorism. However, sectoral strategies and playbooks should be in place as well to handle crisis response management in this regard, such as the one developed by the ReBIT in the context of banking and financial services.

- MeitY has initiated a project entitled, Information Security Education and Awareness (ISEA) Project Phase-II, in 2014, with the objective of capacity building in the area of information security, training of government personnel, and creation of mass information security awareness targeted towards various user segments. The project envisages training 114,000 persons in various formal/non-formal courses and more than 13,000 government officials by March 2020.

RECOMMENDATION: Risks associated with cyberspace must be protected in various databases - Aadhaar, Census, National Health Registry, and others. India's Internet registry is not designated as a protected system and numerous policy stakeholders use Gmail and other public email systems for official communications (including listing them in official directories). These are critical gaps and vulnerabilities that affect national and citizen security and should be addressed on priority.

5.3 BUILDING CYBER DETERENCE CAPABILITIES

Deterrence does not easily adapt itself to the domain of cyberspace and state conflicts. For deterrence to be credible, threats of severe retaliation require attribution and a quick response. Factors inhibiting the use of the deterrence concept in cyberspace include the proliferation of actors with different risk appetites, and the fact that cyber weapons are very different compared to conventional weapons, which can be precisely quantified in terms of tonnage as well as in terms of the physical damage or adverse effects they can cause[33].

The recent malware attack[34] on Kudankulam nuclear power plant wherein a significant data breach on its administrative network highlighted the risks associated with the physical effects of such an attack, ranging from facility sabotage to a full-fledged reactor meltdown. In this event, while that risk may have been subverted as it has been contended that the core networks were air gapped or isolated from the Internet, it is not always a fail-safe solution safeguarding critical networks, such as a nuclear facility. A new deterrence strategy must encompass more rigorous policy instruments than air gapped systems.

A deterrence strategy for cyberspace should address four broader sets of threats, emanating from terrorism, crime, espionage, and asymmetric attacks targeted at critical infrastructure. The actors behind these threats have different capabilities to impose harm, and varying degrees of tolerance for risk to their own operations or infrastructure. For instance, a nation state is more prone to risks from retaliatory attacks on its own critical infrastructure which could endanger its populace, while a terror group is immune to those risks as it does not hold territory, infrastructure, or have a population to defend against retaliatory attacks. In retrospect, non-state actors are the most difficult adversaries in cyberspace to deter, as they do not have territory, population, or political constraints, which are extremely valuable for nation states, and also happen to be the key determinants of a deterrence strategy.

- ADOPTING AN "ALL-HAZARDS" APPROACH: The probability of a threat actor being able to execute an attack exploiting a vulnerability is a desired input for quantitative risk assessment. Preparedness encompasses a broad range of both manmade and natural hazards, which also includes acts of terrorism. From an operator's perspective, the source or cause of the incident is secondary, while the continuity of service and the mitigation of unanticipated cascading effects is the primary task at hand.

- AMALGAMATION OF REGULATORY AND PARTNERSHIP MODELS: Critical infrastructure owners and operators are unevenly spread across the governments, private, and public sectors. With deregulation of sectors such as energy, transportation, and communication, multiple players with varying degree of maturity in security practices are now part of the critical infrastructure. At a strategic level, governments are inclined to enforce supervision over the best practices and guidelines issued for the critical infrastructure sectors.

- STRATIFIED INFORMATION SHARING: Once a strategy and an executive apparatus are in place, information sharing is the key driver of an effective CIIP policy initiative. The scope of information is wide: it encompasses threat information, incident reporting/analysis, best practices, protective measures, advisories, vulnerability or audit notes, crisis management, alerts, and warnings. Information sharing is vital to communication, situational awareness, policy implementation, collaboration, and coordination. Graduating

[33] https://idsa.in/system/files/book/book_indias-strategic-options-in-cyberspace.pdf
[34] https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/#click=https://t.co/WePv1sBGrr

from the hierarchical model, information sharing now works like a network, and there are multiple agencies, strata, and channels, both formal and informal.

- DETERRENCE BY DENIAL: Deterrence by denial means to strengthen defences in such a manner that the efforts, resources, and costs required for a successful attack are enormous. There are different methods and approaches used to do this.

- ENHANCED CYBERSECURITY: Enhanced cybersecurity is more like a security ring which fends off a majority of the attacks before they can achieve their goals. The approach to cybersecurity generally includes stringent authentication and password management, encryption of data and communication channels, analysis and assessment of viruses or malware, and the timely update or patching of software for known vulnerabilities.

- ACTIVE CYBER DEFENCE: Active defences in the form of network monitoring or surveillance for the swift identification of and counter measures against cyber attacks are gaining prominence since the ways and means used are typically moving beyond traditional cybersecurity practices. These include monitoring network traffic, blocking hostile packets, and deploying honeypots. Active defence for network security also helps in unveiling the identity of the perpetrators of an attack, as well as facilitating justice and prosecution in accordance with the respective legal frameworks.

- REDUNDANCY AND RESILIENCE: Redundancy in infrastructure ensures the sustainability of operations in the case of attacks or other disasters/ accidents which degrade infrastructure. Redundant assets remain functional under such contingencies, containing the propagation of failure or disruption. Although building redundancy and resilience into network systems adds to the costs and architectural complexity, they are quite effective in mitigating operational risks to a larger extent. Well defended and resilient information systems and computer networks can reduce the perceived gains from a cyber attack for the adversary. Enhanced defence mechanisms could be further reinforced or supplemented by multilateral arrangements for acceptable behaviour or norms in cyberspace.

- PROJECTION: The projection of power by building robust systems, such as seen in the US context of its Transportation Command building a deployment and distribution system that is strong, can be an effective counter-power projection built into a deterrence strategy.

- INTERNATIONAL NORMS OF STATE BEHAVIOUR FOR CYBER SPACE, CONFLICT PREVENTION, AND CONFIDENCE BUILDING: Diplomatic measures to prevent conflict and build confidence among the stakeholders in cyberspace are a cornerstone of stability in this domain. Such activities are actively being pursued at global and regional levels such as in the United Nations, the International Telecommunication Union, the ASEAN Regional Forum (ARF), and OECD, etc. with a focus on practical measures to build confidence among member states or pave the way for norms of behaviour in cyberspace. However, diverging interests, varying cultures of norms and behaviour, in addition to the practical challenges of verification, make treaties extremely difficult to negotiate and enforce.

- ENTANGLEMENTS: Economic, political, social, or other spheres of interactions and engagements lead to entanglements. These interwoven dependencies make the attacker question the very necessity or attractiveness of the attack as it may result in severe damage for the attacker himself. Entanglements mould the attacker's perception of the targeted system, as emanating interdependencies might significantly impact his own infrastructure – or assets which the attacker values.

RECOMMENDATION: Assessment of cyber deterrence, beyond the above observations, requires intensive investigation bringing in a wider set of experts from global and national cyber defence stakeholders. Our view is that a Cyber Defence Policy, while entwined with the National Cybersecurity Policy, should be dealt with separately.

5.4 EMERGING TECHNOLOGIES AND THEIR SECURITY IMPLICATIONS

The Internet of Things (IoT) is aggravating the security threat for both consumers and businesses alike with the number of IoT devices expected to increase from 23 billion worldwide now to 31 billion in 2020 and 75 billion in 2025, according to Statista. In 2018, a Symantec study[35] reported an average of 5,200 attacks per month on IoT devices. As IoT increasingly pervades our private and public environments, its vulnerabilities may favour severe security and safety from threats.

The United Kingdom is leading efforts on enforcing standards, with its Department for Digital, Culture, Media, and Sport last year publishing a Code of Practice for Consumer IoT Security[36] that has been translated into seven languages.

5G TELECOM TECHNOLOGIES

High-speed broadband services over 5G networks is expected to result in expansion of IoT applications, in the consumer and industrial space. This enables organisations to integrate more

[35] https://www.symantec.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse
[36] http://www.mobilenewscwp.co.uk/2019/05/29/feature-advent-of-5g-and-iot-looks-set-to-ramp-up-uk-cyber security-threat/

processes as well as allow more information to be collected and communicated via networks. The need for safety and resilience in network and device security becomes critical levers in this regard.

As the US presses ally to impose restrictions on a Chinese telecom firm, European countries are drafting stricter 5G security requirements. In December 2018, the Czech National Cyber and Information Security Agency (NCISA) issued a warning against hardware and software produced by the Chinese companies such as ZTE Corporation. According to the Czech NCISA, the use of hardware and software supplied by these companies constituted a threat to national security. Businesses designated as critical national infrastructure, important information systems, and essential providers are obliged to take note of this warning and to implement adequate countermeasures.

About half a dozen countries are now leading the charge to shape an EU-wide regime on 5G security, which would include a mixture of security checks and procedures, certifications, and instruments to potentially interfere in telecom deal-making in the case of strategic or national security concerns. While granting capitals flexibility, the new toolbox could provide justification for much tougher measures against foreign vendors. By end of 2019, EU countries are expected to put together a "toolbox" of measures to mitigate or counter potential threats.

Two key approaches that have been talked about in a recent Brookings study[37] towards securing our digital pathways around 5G include:

- A risk-based accountability approach (rewards-based incentives rather than penal sanctions): While recognizing the need for a risk-based approach towards cybersecurity, regulators need to evolve beyond penal sanctions to examine rewards-based incentives. This approach is as much relevant for government agencies and the public sector as for the private sector. Therefore, all parties that are designing, developing, and deploying new technologies like 5G (or AI, Robotics, etc.) should have proactive cyber protection programmes. This enables a harms-free experience of products and services from the user perspective.

- Stimulate closure of 5G supply chain gaps: Country of origin/ownership concerns must become relevant to both the corporate calculus that led to offshoring purchase decisions as well as to the market conditions that led to the destruction of a national capability in the first place. 5G supply chain market analysis must be continuous with regular engagement between regulators, industry, and the executive and legislative branches to properly incentivize globally competitive domestic sourcing alternatives.

ENCRYPTION TECHNOLOGY AND POLICY

Despite several sectoral regulations in the banking, finance, and telecommunication industries carrying stipulations, such as minimum standards of encryption to be used in securing transactions, India does not have a dedicated law on encryption. A draft National Policy on Encryption under Section 84A of the Information Technology Act 2000 was published on September 21, 2015 and invited comments from the public but was withdrawn two days later – ostensibly due to its unfeasible and unclear provisions with respect to the use of encryption technologies[38].

A new encryption policy must be framed with a primary objective of securing information security architecture of the Indian digital economy. An encryption policy for the future should set out a forward-looking agenda for the Indian digital economy, affirming the basic tenet that strongly encrypted devices and platforms are needed and recommended to secure the data of India's digital ecosystem.

ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The rising use of machine learning (ML) and artificial intelligence (AI) are considered to be dual-use technologies – while more cybersecurity companies are implementing AI-driven algorithms to prevent threats, hackers are also leveraging AI and bots to commit cyber crimes of higher levels of sophistication. AI systems are cheap, scalable, automated, anonymous, and provide a boundary in terms of distance for the attacker, diminishing the immediate morality around cyber crime.

AI-connected misuse can manifest as:

- AI-ASSISTED EVASION: Cyber criminals can overwhelm conventional law enforcement agencies with AI-assisted evasion.

- AI IN PHISHING ATTACKS: AI-created content can circumvent typical cybersecurity filters, such as email messages that are indistinguishable from those written by humans.

- AI IN SOCIAL ENGINEERING CONTEXT: Social engineering and the possibility of AI-generated "deep fakes" that can change the context in an image, an audio recording including the voice of a human being, is a peek into the damage potential of AI-aided cyber crimes.

OUR VIEW: Global policy and regulatory investments into AI provide a peek into sovereign capabilities and positions. AI-aided cyber breaches and cyber crimes are the reality that all stakeholders must face. This is an area that is grossly under-researched and under-funded – and a significant vulnerability in India's cybersecurity ecosystem.

[37] https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cyber security/
[38] https://sflc.in/faq-legal-position-encryption-india

5.5 CYBERSECURITY TALENT AND RESEARCH

Many committees and reports have highlighted the global shortage of cybersecurity professionals.

- The NSCS Joint Working Group (JWG) on engagement with the private sector on cybersecurity has recommended that the critical shortage of cybersecurity professionals needs to be "tackled in mission mode with innovative recruitment and placement procedures and specialized training of existing manpower."

- The NSCS JWG recommended that this be implemented in public-private partnership (PPP) mode, and that the ministries of communication, IT, and HRD jointly establish a cybersecurity capacity building framework and a competency framework to assess skills required, identify gaps, and devise strategies and programmes for capacity-building — including security certification schemes for IT professionals and cybersecurity related curricula for university degree programmes.

- The skills shortage would be especially pertinent to the capacity needs of solving the problem in government on the acute deficit in empanelling more auditors for all government agencies, both at the centre and state levels. A working group should be put in place to formulate a cybersecurity skills action plan that can set some key performance indicators to drive tangible outcomes addressing the gaps. A governance, risk, and compliance framework is an effective method of identifying and managing threats at an enterprise level (be it public or private).

- The JWG recommended that government and the private sector should fund R&D for development of indigenous cybersecurity products and solutions that meet international standards and address the global market. Given that global tech services sourcing is dominated by India (55 percent of all global sourcing), the potential to make India a hub or epicentre of cybersecurity software and services has been recognized at the highest levels. In 2015, following Prime Minister Modi's specific suggestion to industry body NASSCOM on this, the trade body set up a Cybersecurity Task Force (CSTF) with a vision to make India a global leader in cybersecurity by 2025, by building India's cybersecurity industry from 1 percent market share to 10 percent by 2025, having a trained base of 1 million certified, skilled cybersecurity professionals; and an ambition of creating a base of 100+ successful security product companies from India.

RECOMMENDATION: We see India's acute need to go beyond the current single IDRBT Centre of Excellence (CoE), to establish more Centres of Excellence in specific critical infrastructure sectors like transport, power, and public health care, as well as cyber forensics and cyber crime studies with Indian and global firms operating in these areas — beyond technology providers to key sector players.

5.6 CYBERSECURITY STANDARD SETTING, TESTING, AND CERTIFICATION

A critical component of developing cyber resilience involves standardisation. Standardising information security protocols enables improving efficiencies in key cyber defence processes, allows for interoperable and integrated systems, and simplifies complex cyber environments and deployment of new technological and business solutions. Common cybersecurity standards allow for a degree of certainty and business predictability in a digital economy that is meant to be borderless. For example, in the context of digital payments, standardisation allows boosting customer confidence in terms of integrity of a product or service. We believe that the government should remain cognisant of the fact that mandating a local manufacturing presence is not in itself a proxy for a safe and secure cyber environment. Any such mandates do not automatically make our ecosystem either more or less secure.

India's present standardisation, testing, and certification framework encompasses the nodal Bureau of Indian Standards (BIS), the Standardisation Testing and Quality Certification (STQC) Directorate under the MeitY, and the Telecommunications Engineering Centre (TEC) under DoT.

- BUREAU OF INDIAN STANDARD (BIS): The BIS is the national standards setting body that was brought under the ambit of a new statutory regime, the Bureau of Indian Standards Act 2016. This has been done with the intent to simplify conformity assessment schemes including self-declaration mechanisms[39]. The BIS is situated at the Ministry of Consumer Affairs in India. The overarching standard formulation is performed through a technical committee structure consisting of area-specific division councils, sectional committees, subcommittees, and panels[40]. Under the Electronics and IT Division Council[41], there are specific subcommittees tasked to develop standards for "Information Systems Security and Biometrics." The committees are multi-stakeholder in nature with representation from ministries, industry, and academia in an endeavour to mirror international SSOs[42] such as the International Standards Organization (ISO) or International Electrotechnical Commission (IEC). As the national standards organization, BIS sends members of sector specific councils to represent India's interests at various international standards developing organizations.

[39] http://pib.nic.in/newsite/PrintRelease.aspx?relid=171705.
[40] http://www.bis.org.in/home_std.asp
[41] https://bis.gov.in/?page_id=117873
[42] Standard setting organizations

- MEITY COMPULSORY REGISTRATION SCHEME (CRS): While the CRS provides a framework for compulsory certification of any product or service of public interest or national security considerations, this does not quite address cybersecurity concerns and only comprises device inspections for general safety reasons, such as mitigating risks of electric shocks, heat, or chemical hazards, etc.

- STANDARDISATION TESTING AND QUALITY CERTIFICATION (STQC): The STQC Directorate under MeitY offers quality-assurance services for information technology and electronics sectors, through a pan-India network of laboratories and centers. The qualitative testing and certification services are provided for both, the public and private sector[43]. STQC has operationalized four regional and 10 state level laboratories so far. The security benchmarks, as outlined on the STQC website, refer to the draft ISO/IEC27001 and ISO/IEC27002 standards from 2005[44] even as the international benchmarks were set in 2013. For security testing, there is only one dedicated IT Security Testing laboratory in Kolkata.

- MEITY INDIAN COMMON CRITERIA CERTIFICATION SCHEME (IC3S): The IC3S is a part of the Cybersecurity Assurance initiatives to evaluate and certify IT security products and protection profiles against the requirements of Common Criteria Standards at evaluation assurance levels (EAL 1 through 4). The main players in this programme are the Developer of IT Security Products or Protection Profiles, Sponsors, Common Criteria Test Laboratory (CCTL), the and Certification Body. The scheme provides national certification under the International Mutual Recognition Arrangement with the other member countries of Common Criteria Recognition Arrangement (CCRA), acceptable in all the member countries. India is a member of CCRA as a Certificate Authorizing Nation, which allows CCRA Certificates issued by India through STQC[45] to be accepted in other countries without re-certification. The government should ensure that there is no additional regulatory burden imposed by way of repeat testing for those offerings that are already CCRA certified. We need to develop a reciprocity principle in this context.

- TELECOMMUNICATIONS ENGINEERING CENTRE (TEC): TEC is the principal standards development and certification forum for telecommunications equipment that is used in network infrastructure. Under the Indian Telegraph Amendment Rules of 2017, it is mandated that all telecom equipment is to undergo testing and certification. The Department of Telecom has been developing essential requirements for the same. As per the framework set out, the testing will be carried out by accredited labs, and TEC's role is to certify due compliance. In addition, the TEC also interacts with multilateral agencies such as the ITU and European Telecommunications Standards Institute (ETSI) to articulate India's perspective on standardization. TEC has a specific cybersecurity division, entrusted with the responsibility of securing overall networks by defining the ICT network security framework, participating in standards organizations such as ITU, and coordinating activities with major domestic cybersecurity agencies[46]. The TEC had floated a tender process (with a latest draft published in December 2017) to create Telecom Security Testing Lab with the purpose of ensuring resilience and security of all types of telecom/IP equipment. The proposed lab is meant to test for device and network resiliency against vulnerabilities related to cyber threats (e.g. the distributed denial of service attacks, botnets, phishing and identity theft[47]). In this regard, Indian Telephone Industries (ITI) Limited has set up two labs in Bangalore to enable telecom companies and vendors get network equipment certified[48]. The labs were setup under the aegis of the National Digital Communications Policy.

On India's participation in the global standards arena, India is a "participatory country" at the ISO, but the degree or quality of participation in IT security aspects has been inadequate. India's participation in terms of contingents at these fora is considerably smaller than global counterparts. India has not played an active role in IEEE or IETF as well thus far, though specific agencies have been engaging with their global counterparts. There are several opportunities for international collaboration on standards setting.

- India lacks adequate device-level security standards (as per the CRS scheme at MeitY), and it would be in the national interest to expedite developing and establishing cybersecurity standards as per ITU or the Common Criteria ISO standards. Efforts, such as the 5G "test bed"[49] being set up at IIT Madras, is a good opportunity for embedding security benchmarks.

- In the realm of digital payments, global standardisation conversations are driven by industry-led entities, such as EMV Co, PCI-SSC (Payment Card Industry Security Standards Council) and the FIDO Alliance. India, RBI, IDRBT, and affiliated agencies should seek to play a more active role with these entities.

> INDIA MUST PLAY AN ACTIVE ROLE IN GLOBAL STANDARDS CONVERSATIONS, SUCH AS AT IEEE AND IETF, IMPROVING OUR QUALITY OF PARTICIPATION IN GLOBAL IT SECURITY FORA.

[43] http://www.stqc.gov.in/content/about-stqc
[44] http://stqc.gov.in/content/information-security-testing-and-assessment
[45] http://www.commoncriteria-india.gov.in/overview.php
[46] http://www.tec.gov.in/cyber security-cs/
[47] http://www.tec.gov.in/pdf/Tenders/Technical%20requirements%20of%20Security%20lab.pdf
[48] https://telecom.economictimes.indiatimes.com/news/iti-sets-up-telecom-gear-testing-centre-in-bengaluru/67940041
[49] https://telecom.economictimes.indiatimes.com/news/indias-5g-testbed-to-be-fully-operational-by-2021-project-coordinator/66137722

6. RECOMMENDATIONS FOR INDIAN CYBERSECURITY POLICY – 2020-25

Keeping with the framework of the United Nations Guide to Developing a National Cybersecurity Strategy, we have the following recommendations to the Office of the NCSC towards making India a global cybersecurity hub featured in the top 10 mature economies in terms of cyber readiness on the UN Global Cybersecurity Index within the next three years.

Our view is that India should take an ecosystem approach – critically evaluating how gaps can be closed with a sense of urgency. The following recommendations are framed in that vein:

6.1 CYBERSECURITY GOVERNANCE

RECOMMENDATION 1:

"WHOLE-OF-GOVERNMENT APPROACH"

WITH DISTINCT SUPERVISORY AND IMPLEMENTATION ROLES

India should take a "whole-of-government" approach to cybersecurity, akin to that taken by Australia which has outlined its cyber strategy in its recent 2019-20 budget with investment layouts on establishing a Cybersecurity Centre and a Security Response Fund[50], building centres with cyber sprint teams for agencies across the board, and developing a shared objective and an integrated government response to cybersecurity issues. The purpose of this approach is to create a culture that facilitates a shared vision across different ministries (Home, Electronics and IT, Health, etc.). Inter and intra-agency coordination strengthens the consistency of decision making instead of an aggregate of different authority points. It establishes a unified effort between agencies to maximize all available resources at its disposal – be it human capital, funding, and infrastructure in a collaborative manner.

The new strategy should start with a "whole-of-government" approach with a long-term objective of moving towards a "whole-of-nation" approach. The end-state for such an approach should (a) promote partnerships (with private sector and non-traditional stakeholders) that lead to enhanced situational awareness and coordinated efforts to address critical threats at both, local and central levels, and (b) lead towards improved engagement with global partners to rapidly identify, characterize, and report risk incidents that pose a threat to India. We believe that NCSC is best equipped to execute this approach by streamlining the existing lines of communications instead of creating new lines that create overlap or ambiguities. The streamlining could incorporate a more cohesive project management outlook as seen with the United Kingdom's National Cybersecurity Centre. A suggested organizational chart to streamline and earmark responsibilities is provided hereinbelow:

- Currently, the NCSC plays both supervisory and implementation roles. This works well during peace time but can be challenging for the ever-ready state of preparedness that is required for cybersecurity. In line with this, the National Cybersecurity Policy should take a principles-based approach so that different government agencies responsible for its implementation have a consistent view of strategic intent and can refer to the policy in cases of differences of opinion on how the policy is implemented. The cybersecurity principles enshrined in the policy document can be supplemented

with specific rules to address some of the identified gaps. This is how robust policy and legislative documents have been framed. In India, the Telegraph Act is quoted as a good example of a legislative framework that follows this philosophy.

- There is an urgent need for clearly defined roles and responsibilities, processes, decision rights, and the tasks required to ensure effective implementation of the strategy. This includes identifying the stakeholders who will oversee the implementation of the National Cybersecurity Policy and establishing performance targets for various ministerial or governmental departments, institutions, or individuals responsible for specific aspects of the strategy and subsequent action plan. Currently, the Office of the NCSC and the CERT-IN are stretched and forced to react putting out fires due to weak capacity at the implantation or enforcement levels. Specifically, there is a need to:
  - Ensure stronger intra-government coordination to ensure adequate linkages between NCIIPC, CERT-IN, and the different government agencies that are directly or indirectly responsible for supporting implementation. This should be supplemented by the creation of intra-government task forces to address a particular issue (e.g. implications of cybersecurity on IoT).
  - Establish fusion centres embedded at a NCCC level that can share threat information between different levels of government.

> A "WHOLE-OF-GOVERNMENT" APPROACH DRIVEN BY NCSC IN PROJECT MANAGEMENT MODE ALLOWS FOR BETTER ALIGNMENT ACROSS MINISTRIES AND AGENCIES, AND WITH THE NATIONAL CYBERSECURITY STRATEGY.

Stakeholder(s): National Security Council (PMO), Ministry of Electronics and IT, National Technical Research Organization (NTRO)

Timeline: Short to Medium-term (12 to 18 months)

RECOMMENDATION: Undertake a "whole-of-government" approach led by NCSC in project management mode, as seen with the United Kingdom's National Cybersecurity Centre. This would lead to better alignment with strategic intent and ensure that cybersecurity principles enshrined in the National Cybersecurity Strategy 2020 are followed and efforts across various ministries (Home, Electronics and IT, etc.) resolve any inter and intra-agency coordination gaps.

RECOMMENDATION 2:

NATIONAL CYBERSECURITY BUDGET AND PUBLIC-PRIVATE TASKFORCE

Given the significance of the issue, there is an urgent need to create additional budgetary allocation for the national cybersecurity programme. State governments of Andhra Pradesh, Telangana, and Haryana have earmarked separate budgets for cybersecurity (e.g. 10 percent of state government IT spends) on setting up operation centres and other tasks. This is akin to Singapore that announced[51] that it was looking to spend 8 percent to 10 percent of its IT budget on cybersecurity in line with similar practices in Korea (10 percent spend) and Israel (8 percent spend across the government).

- India should look to formalize a funding mechanism that looks specifically at addressing cybersecurity challenges with institutional capacity, additional resource allocation for dedicated cybersecurity teams in key government departments/agencies as well as creating separate budgets for cybersecurity research and training. There are no public and private assets when it comes to cybersecurity. All assets are equally at risk, and this makes a PPP model the ideal structure for creating greater funds to address the issue. India could learn from the global experiences on cybersecurity budgeting and pursue public-private partnerships to create a deeper set of national cybersecurity resources for both the government and the private sector, to meet the cybersecurity challenge. This has been particularly successful in Europe and Singapore (see table on International Best Practices in Section 4.1).
- A public-private cybersecurity task force, constituted with members from Indian and global companies and government agencies, can bring together available cybersecurity expertise that exists with the private sector and effectively apply it in the public sector. The task force would look separately at critical infrastructure sectors, create threat information sharing platforms, invest in cybersecurity research and talent development, and invest in public education.

[51] https://www.csa.gov.sg/news/speeches/min-opening-speech-at-govware2015

– New cybersecurity Centres of Excellence are an imperative, and India should prioritize their creation with external funding, where required from the private sector. Three to five dedicated research competence centers, or Centers of Excellence established or incubated within leading academic institutions, are important for India to move up the cybersecurity maturity curve.

– India should prioritize on extending institutional cybersecurity support to the MSMEs and startups as well as its citizens. In the financial sector, the US sectoral framework helps SMEs adopt appropriate cybersecurity safeguards. Israel has excelled in building a state-of-the-art cybersecurity ecosystem. The OECD espouses the benefits of introducing security labels to products and services to better inform the market and promoting cybersecurity insurance markets. In the UK, the government has adopted market-driven solutions, such as cyber risk insurance for SMEs, to promote good cybersecurity practices. The UK has implemented a citizen-facing capacity building programme (Cyber Aware) and a cyber essentials platform to shield SMEs from low-level exploits.

– The skills shortage would be especially pertinent to solving the problem in government on the acute deficit in empanelling more auditors for all government agencies, both at the Centre and State levels. A Working Group should be put in place to formulate a cybersecurity skills action plan that can set key performance indicators to drive tangible outcomes addressing the gaps. A governance, risk, and compliance framework is an effective method of identifying and managing threats at an enterprise level (be it public or private).

- India's new Policy should only be applicable for a specific time period – 2020 to 2025. This is similar to the U.K. Government's Cybersecurity Strategy (2016-21). The National Cybersecurity 2020 policy should be subjected to a midterm review after the first 24 months, say in 2022, to ensure that security efforts keep abreast with rapid technological advancements. Additionally, government and private sector agencies should build accountability through annual assessments, identifying vulnerabilities, developing standard operating procedures, mapping cyber breach incidents, and conducting regular cyber breach simulation trainings to ensure preparedness. Development of national cyber forensic capabilities needs to be improved, and the private sector can play an important role in bringing in global best practices and expertise in this area.

> A PUBLIC-PRIVATE CYBERSECURITY TASK FORCE COULD TAKE FORWARD THE 2013 JWG MANDATE TO SPECIFIC OUTCOMES, SUCH AS ESTABLISHING CENTERS OF EXCELLENCE, A SKILLS ACTION PLAN, AND SUPPORT PLATFORMS FOR SMES AND STARTUPS.

Stakeholder(s): National Security Council (PMO), Ministry of Electronics and IT, Industry chambers (AMCHAM, NASSCOM, etc.)

Timeline: Medium-term (18 months)

RECOMMENDATION: A public-private cybersecurity task force, constituted with members from Indian and global companies and government agencies, should take forward the earlier JWG mandate into specific tangible outcomes: the establishment of Centers of Excellence (CoE), a cybersecurity skills action plan on capacity building and training programmes, and support to small to medium enterprises (SMEs) and startups (similar to the UK's Cyber Aware programme).

RECOMMENDATION 3:

CYBERSECURITY CAPACITY AND READINESS AT STATE LEVEL

It is critical to build local capacities in the form of state-level CERTs and CISOs. These agencies at the state cannot be purely be vested with executive powers but must be empowered with enforcement mechanisms for it to remain effective. Any state-level framework guaranteeing responsive cyber federalism approaches should ensure that it is in alignment with the national-level strategy and does not purport to create any overlaps or misalignment with the 2020 Vision outlined at the central level. Following are two specific recommendations for developing stronger cybersecurity capacity at a state and a municipal level:

1. State 'Cyber Readiness' Index: The measurability of the states' cybersecurity readiness can be gauged y through an initiative and methodology co-developed by Cyber Agency with Niti Aayog similar to the lines of the National E-Governance Readiness Index or States' Ease of Doing Business Index. We appreciate the government and National Council of Applied Economic Research (NCAER)'s work carried out in 2008 to provide an assessment of Indian States/UTs in the sphere of

e-Governance. A similar empirical approach that was put in place for examining ICT adoption can be used to benchmark security practices across various agencies, at centre and state levels.

2. Cybersecurity Framework for Smart Cities: Smart cities are built around connected systems and sharing large amounts of data across various infrastructures. The Danish Center for Cybersecurity has been mapping how cybercrime aimed at disrupting IT networks and IT infrastructure could threaten energy supply, in the context of smart city projects in Denmark[52] In developing appropriate standards for building cyber secure cities, NIST launched the Global City Teams Challenge (GCTC) programme alongside an international technical working group IOT-Enabled Smart City Framework. The framework provides a simple-to-use analytical tool for early investigation of smart city applications. NIST has also developed a framework for Cyber Physical Systems. An integrated governance mechanism for protection of smart city infrastructure through the special purpose vehicle (SPV) established by Ministry of Housing and Urban Affairs (MoHUA) for protection of smart city infrastructure to manage cyber risks. The lifecycle of building the infrastructure from conception stage to "end of life" should embed both, security and privacy by design.

> STATE-LEVEL SECURITY FRAMEWORKS SHOULD BE ALIGNED WITH THE NATIONAL CYBERSECURITY STRATEGY. A CYBERSECURITY READINESS INDEX COULD HELP ASSESS STATE CAPACITIES.

Stakeholder(s): Ministry of Electronics and IT, National Cybersecurity Coordinator (NCSC), IT/Electronics departments across states, Niti Aayog (support on design of the Index)

Timeline: Long-term (18 to 36 months)

RECOMMENDATION: Any state-level security framework for ensuring responsive cyber federalism should be in alignment with the National Cybersecurity Strategy, with no overlaps or misalignment with the Central vision. For building stronger capacities at the local level, India should develop a Cybersecurity Readiness Index (suggestion: in partnership with MeiTY and Niti Aayog) along the lines of the government's similar effort to measure e-Governance readiness in 2008.

RECOMMENDATION 4:

ROLE IN GLOBAL CYBERSECURITY STANDARDS SETTING

6.2 INTERNATIONAL COOPERATION ON CYBERSECURITY

India should play an active role in global dialogues on international standards setting. While India is a "participatory country" at the ISO, the quality of participation in the IT security aspects has been inadequate. India's participation in terms of contingents at these fora is considerably smaller than global counterparts. India should endeavour to play a more active role in standard setting organizations like ISO/IEC, ITU, 3GPP, IEEE, IETF, etc. The National Cybersecurity Policy 2020 should attempt to bridge this gap and mention this as a priority in clear terms.

This prioritisation can be further qualified by stating that India would:

- Harmonize domestic (national or state-level) cybersecurity approaches and regulations with global commitments, that may be UN-led, bilateral (US-India), or via treaties, such as the Budapest Convention.
- Expedite the development and establishment of cybersecurity standards as per ITU or the Common Criteria ISO standards. In this regard, efforts, such as the 5G "test bed"[53] being set up at IIT Madras, are ripe territories for embedding security benchmarks.
- India's bilateral or plurilateral trade and investment agreements should look at incorporating cybersecurity as a prominent part of a chapter or section on data, including cross-border data flows, which is often the subject of much debate and negotiation (e.g. at G20 in Tokyo, June 2019, where Japan's pitch for free data flows "with trust" faced resistance from others, including India). India has some expertise in cross-border data issues at the Ministry of Commerce (e.g. at its WTO ambassador's office in Geneva, and this expertise could be enhanced with cybersecurity inputs and collaboration with the NCSC). These sections should look at working language that takes the bilateral frameworks, such as US-India and EU-India, beyond into implementation and specifics. The chapter could include, for instance, support for establishment of international cybersecurity norms and confidence building measures, commitment to cybersecurity capacity building, and participation in the development of international cybersecurity standards.

[52] https://www.politico.eu/article/cyber-threats-could-turn-smart-cities-into-dumb-ones-copenhagen/?utm_source=POLITICO.EU&utm_campaign=1da2626df8-EMAIL_CAMPAIGN_2019_09_09_05_11&utm_medium=email&utm_term=0_10959edeb5-1da2626df8-190406433

[53] https://telecom.economictimes.indiatimes.com/news/indias-5g-testbed-to-be-fully-operational-by-2021-project-coordinator/66137722

Stakeholder(s): Ministry of Electronics and IT, Ministry of External Affairs (MEA)

Timeline: Long-term (18 to 24 months)

6.3 CYBERSCURITY RISK MANAGEMENT

RECOMMENDATION 5:

CYBERSECURITY FOR CRITICAL INFRASTRUCTURE AND KEY SECTORS

For protection of critical information infrastructure, protection framework design should focus on early-warning systems, detection, response, and crisis management. It is important to facilitate public-private sector collaboration in this area, since both the public and private sectors own and manage assets in a CII realm. There is a need for institutions, such as the NCIIPC, to coordinate closely with CERTs to streamline cybersecurity efforts.

- The NCIIPC should look at the US NIST Framework and the EU's Network Information Systems Directive (NIS Directive) for strategic direction on threats regarding critical infrastructure. In this regard, a Task Force comprising industry and academia could be established to look at framing a CII strategy to ensure clear delineation of non-critical systems from critical ones and ensuring there are no overreaching implications and unnecessary compliance burdens imposed. The Task Force can look at creating objective criteria in determining those that are providing critical services and functions, and whose compromise, damage, or destruction through a significant cybersecurity incident.

- Creation of Information Sharing and Analysis Centers (ISACs) for the designated critical sectors will enable a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents, and threats, as well as sharing experience, knowledge, and analysis. European legislations, like the NIS Directive and the Cybersecurity Act, nourish the creation of 11 sectoral ISACs and PPPs within the EU, and 25 ISACs in the US.

- We recommend that, to begin with, sectoral ISACs for the six designated critical sectors (transport, power and energy, telecom, government, banking and financial services, and strategic/public enterprises) could be formed under the command of the NCIIPC, which also could take up the responsibility of a Governing Council that allows information exchange between the ISACs.

- India should look at the creation of national-level CERTs for all other designated critical sectors (currently only power sector CERTs are in existence). These sectoral CERTs should play a key role, next to key players and stakeholders, such as national regulatory authorities, industry associations (e.g. telecom, banking, and energy), and justice and law enforcement agencies. We could take a proactive view and look at other CII sectors and best practices from the US as well as Europe. Healthcare is an important sector to consider, and the National eHealth Authority is an important regulator that will have a keen interest in the security of digital health records of citizens.

> NEW ISACS (INFORMATION SHARING AND ANALYSIS CENTRES) TO BE SET UP FOR CRITICAL SECTORS, TO ENABLE INFORMATION EXCHANGE ON CYBER THREATS AND OTHER ALLIED ISSUES ACROSS PRIVATE AND PUBLIC SECTORS.

Stakeholder(s): Ministry of Electronics and IT, National Cybersecurity Coordinator (NCSC), related sectoral regulators and ministries.

Timeline: Short to medium-term (12 to 18 months)

United States	Europe	India
• 25 sector-based ISACs make up the National Council of ISACs (NCI) in the US. Initial formation was in the aftermath of attacks on World Trade Center (1993) and Oklahoma City (1995).	• Created later than US's and factored in lessons and learning from the American model. More industry-driven with government providing functional (secretariat-led) support.	• An independent non-profit that exists as a PPP model with close interfaces to NCIIPC. • Largely an events-centric and awareness-focused entity. • Does not seem to be an active organization
• Sectors include automotives, aviation, communications, election infrastructure, electricity, emergency response, financial services, healthcare, IT, maritime, et al.	• Sectors include energy, water supply, health, financial market infrastructures, banking, railways, aviation, maritime, road transport, food distribution, et al.	• Mostly, has conducted workshops around the power sector and a programme with Tata Communications. • No sectoral allocation of ISACs is seen yet.

RECOMMENDATION: New ISACs (Information Sharing and Analysis Centers) are required for designated critical sectors (transport, power and energy, telecom, government, banking and financial services, and strategic/public enterprises). This will enable a central resource for gathering information on cyber threats and allow two-way sharing of information between the private and the public sector. Six sectoral ISACs for the critical sectors could be formed under the command of the NCIIPC, which could also set up a Governing Council to allow and oversee information exchange.

RECOMMENDATION 6:

CYBERSECURITY RISK-BASED APPROACH AT GOVERNMENT ENTERPRISE AND AGENCY LEVEL

The OECD advocates cybersecurity frameworks to adopt risk-based frameworks. The European Network and Information Security Authorities (ENISA) states that regulations should not articulate how businesses comply with security requirements. Instead, good IT governance can be informed by internationally endorsed standards, such as the ISO27001 and 22301, which offer internationally consistent principles on organizational security. Some of the salient frameworks that are suitable for adoption and incorporation are as follows:

- CIS CRITICAL SECURITY CONTROLS: Publication of best practice guidelines for computer security. The project was initiated early in 2008 as a response to extreme data losses experienced by organizations in the US defense industrial base. The guidelines consist of 20 key actions, called Critical Security Controls (CSC), that organizations should take to block or mitigate known attacks. The controls are designed so that primarily automated means can be used to implement, enforce, and monitor them. The security controls give no-nonsense, actionable recommendations for cybersecurity, written in language that is easily understood by IT personnel.

- NIST CYBERSECURITY FRAMEWORK: Provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyberattacks. The framework has been translated into many languages and is used by the governments of Japan and Israel, among others. It "provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." Version 1.0 was published by the US National Institute of Standards and Technology in 2014, originally aimed at operators of critical infrastructure. It is used by a wide range of businesses and organizations and helps shift organizations to be proactive about risk management. In 2017, a draft version of the framework, version 1.1, was circulated for public comment. Version 1.1 was announced and made publicly available on April 16, 2018. Version 1.1 is still compatible with version 1.0. The changes include guidance on how to perform self-assessments, additional detail on supply chain risk management, and guidance on how to interact with supply chain stakeholders.

> GOOD IT GOVERNANCE IN PUBLIC AND PRIVATE ORGANISATIONS MUST BE CONSISTENT WITH INTERNATIONALLY-ENDORSED STANDARDS, SUCH AS ISO:27001, THE NIST FRAMEWORK, AND EUROPE'S ETSI OUTCOME FRAMEWORKS.

- ETSI CYBERSECURITY TECHNICAL COMMITTEE (TC CYBER): The European Telecommunications Standards Institute (ETSI) established a new cybersecurity committee (TC CYBER) in 2014 to meet the growing demand for guidance to protect the Internet, the communications, the business it carries. TC CYBER is working closely with relevant stakeholders to develop appropriate standards to increase privacy and security for organizations and citizens across Europe. The committee is looking in particular at the security of infrastructures, devices, services, and protocols, as well as security tools and techniques to ensure security. It offers security advice and guidance to users, manufacturers, and network and infrastructure operators. Its standards are freely available online. A principal work item effort is the production of a cybersecurity ecosystem of standardization and other activities.

- FACTOR ANALYSIS OF INFORMATION RISK (FAIR): Emerged as the standard Value at Risk (VaR) framework for cybersecurity and operational risk. The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing information risk. It provides information risk, cybersecurity, and business executives with the standards and best practices to help organizations measure, manage, and report on information risk from the business perspective. The FAIR Institute and its community focus on innovation, education, and sharing of best practices to advance FAIR and the information risk management profession.

RECOMMENDATION: Securities regulator SEBI has prescribed a cyber resilience framework for stock exchanges. This has five core principles, identical to those in NIST's framework: Identify, Protect, Detect, Respond, and Recover. Similarly, good IT governance at the agency level, whether public or private, must ensure consistency with internationally endorsed standards such as ISO:27001, the NIST framework, and outcome frameworks at ETSI within Europe, for integration within the government and strategic public enterprises.

6.4 CYBERSECURITY LEGISLATION AND REGULATIONS

RECOMMENDATION 7:

CYBER CRIME REGULATIONS AND LAW ENFORCEMENT

The National Cybersecurity Policy 2020 should push for the development of a domestic legal framework that clearly defines cyber breaches, risk incidences, and liability principles and develops clear norms beyond just purely cyber crime aspects that are already a part of the existing IT Act framework. Most often, this capability takes the form of cyber crime legislation, which can be achieved by enacting specific new laws or amending existing ones (e.g., the penal code, laws regulating banking, telecommunications, and other sectors).

Cyber crime law enforcement capabilities should be enhanced by the adoption of global frameworks. Two specific frameworks that Indian authorities should consider are:

- BUDAPEST CONVENTION ON CYBER CRIME (CETS No.185): It is the world's first and largest multilateral cyber crime treaty, with 60 ratifications. Designed by the Council of Europe in 2001, it strives to harmonize national cybersecurity laws and form a basis for international cooperation. India is one of the few major non-signatories to the convention, even though it is considered a major instrument for cross-border cyber crime investigations and for securing e-evidence. The convention has established a dedicated "Cloud Evidence Group," which explores solutions for governments/authorities to access evidence stored on cloud servers in foreign jurisdictions. India's concerns on sufficiency in data privacy frameworks could be resolved by a mature data privacy framework that is in the form of the Personal Data Protection Bill presently.
- INTERNATIONAL DATA SHARING ARRANGEMENTS: International conversations are now focusing on data sharing arrangements for law enforcement access. One such framework is articulated under the US' recently enacted Clarifying Lawful Overseas Use of Data (CLOUD) Act, designed to enable easier law enforcement access to data stored across borders through direct data sharing arrangements. The amendments under the CLOUD Act specifically enable foreign states to make binding requests for direct law enforcement access to data held by companies located in the US, upon execution of bilateral executive agreements. The UK–US Data Sharing Agreement forms a template for future executive agreements authorized under the Act. The EU and the US are currently negotiating an agreement. India should be amenable to negotiating the adaptation of similar agreements at bilateral and plurilateral levels.

We should also examine the Council of Europe's Convention 108[54] that serves as the first legally binding international instrument (of 1981) in the data protection field. Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data. "Convention 108+" was amended in 2018 to create a more comprehensive legal regime around data protection, with 55 signatory countries.

Stakeholder(s): Ministry of Home Affairs (MHA), Ministry of Electronics and IT, Ministry of External Affairs (MEA)

Timeline: Medium-term (18 to 24 months)

[54] https://www.coe.int/en/web/data-protection/convention108-and-protocol

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals

Amrit Singh Deo
Senior Managing Director
+91 916 742 8242
amrit.singhdeo@fticonsulting.com

Prasanto K. Roy
Senior Director
+91 981 003 0240
prasanto.roy@fticonsulting.com

Subhodeep Jash
Senior Consultant
+91 701 161 7029
Subhodeep.jash@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT

AMCHAM INDIA

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

www.fticonsulting.com