SSPC RESEARCH PAPER

March 23, 2020

OVERHAULING INDIA'S CYBER SECURITY POLICY: TOWARDS BUILDING A RESILIENT AND TRUSTED CYBER ECOSYSTEM

KRITIKA ROY
RONNIE NINAN

India's move towards the digital economy has facilitated the formation of a cohesive ecosystem and accelerated the growth in sector-specific integrated services. However, at the same time, these digital developments have made the organisations vulnerable and prone to myriad cyber threats. With the surge in cyber incidents, if proactive measures are not put into place, nefarious actors may find more innovative ways to attack the cyberspace. India's existing national Cyber Security policy framework should be overhauled with an eye on the emerging technologies and emphasis on international cooperation and collaboration. This paper highlights the current status of cybersecurity in India and puts forth a few recommendations for a dynamic and resilient cyberspace.

India is at the cusp of transformation towards a digital economy, enabled by digital payment and ecosystem. In the last few years, there have been major developments in the spread of internet and banking services like the establishment of Aadhaar platform and the evolution of several digital payment modes and public service facilities like Ayushmaan Bharat. These advancements have facilitated the formation of a cohesive ecosystem and accelerated the growth in sector specific integrated services. However, at the same time, these digital developments have made the organisations vulnerable and prone to myriad cyber threats. In recent years, there also has been a surge in cyber incidents like ransomware attacks, data theft, espionage and banking frauds. Additionally, the advent of new technologies like IoT (Internet of Things), AI (Artificial Intelligence) and 5G will further increase the risks of such cases. If proactive measures are not put into place, nefarious actors may find more innovative ways to attack the cyberspace. But while it is important to be keenly aware of cyber threats, India's cyber security policy cannot be driven solely by fear and defensiveness. With this in mind, it is important that the existing national Cyber Security policy framework should be overhauled with an eye on the emerging technologies and emphasis on international cooperation and collaboration. This paper highlights the current status of cyber security in India and puts forth a few recommendations for laying an effective and resilient cyberspace.

Limitations of India's Current Policy Landscape

As the Digital India endeavour starts to take shape, India needs to have a relook at its Cyber Security Policy. In the year 2000, India promulgated the Information Technology Act as a legal policy document to deal with cyber interventions. The IT Act of 2000 laid the foundation for the Indian Computer Emergency Response Team (CERT-ln), an organization committed to cyber security standards, agreements, incident response and guidance. This Act was revised in 2008 to provide legal recognition to electronic commerce.[1] Within the IT Act, 2008, cyber security has been listed under "sections 43 (data protection), 66 (hacking), 66A (measures against sending offensive messages), 66B (punishment for illegally possessing stolen computer resources or communication devices), 67 (protection against unauthorised access to data), 69 (cyberterrorism), 70 (securing access or attempting to secure access to a protected system) and 72 (privacy and confidentiality), among others."[2] Furthermore, the country's first national level Cyber Security

1 The Information Technology Act, 2008, Ministry of Law, Justice and Company Affairs, India. Retrieved from http://cybercrime.planetindia.net/it-act-2008.htm.

2 Samaya Dharmaraj, "The current state of cyber security in India," *OpenGov,* August 1, 2018, Retrieved from https://www.opengovasia.com/the-current-state-of-cyber-security-in-india/

Policy was framed in 2013 by Ministry of Electronics and Information Technology (MeitY). This policy document is an exhaustive take on cyber security issues. The national policy had not only set high goals but also covered a wide array of initiatives ranging from an institutional framework for an emergency response to indigenous capacity building. However, many scholars argued that it merely served as a "statement of first principles" rather than being an all-encompassing framework for cyber security policy. Now, after five years of its inception, there is a dire need to articulate a specific framework towards implementing broad principles outlined in the 2013 policy document that also encompasses the fast-evolving digital environment.

India's Adherence to International Cyber Norms

Cyberspace is an anarchic medium with no formal comprehensive governance framework. Few steps have been taken by the international community to create a global governance framework for cyberspace like the establishment of the United Nations Group of Governmental Experts (UNGGE) in 2004. The major aim of the group was to advise the UN on promoting "peace and stability" in cyberspace. However, the fundamental differences, especially among the major power (the United States of America, China and Russia) have thwarted the process of regulating the cyberspace. Despite the global flux in the governance of cyberspace, India is avidly engaged in stepping up its cyber security mechanism.

India has been an active participant in the UN GGE processes where it has advocated the need to have common understanding on responsible state behavior in cyberspace and the adoption of confidence building measures by states to address issues of threats, crimes and terrorism in the cyberspace.[3] It also supports the multi-stakeholder model[4] in cyber governance and has sought support for it from Russian and Chinese, in particular through the BRICS (Brazil, Russia, India, China, and South Africa) forum. This initiative has yielded positive results as the BRICS declarations since 2015 have stressed on the need to involve relevant stakeholders in the evolution and functioning of cyber governance.

Despite the breakdown of UN GGE in 2017, India has continued to support other non-governmental efforts for developing cyber norms such as the Global Conference on Cyberspace and the Global Commission on the Stability of Cyberspace. India is also an active participant in

3 Sameer Patil, "Can India take the pole position in global cyber governance?" *Quartz India*, August 30, 2018 Retrieved from https://qz.com/india/1374396/can-india-take-the-lead-in-global-cyber-governance-against-attacks/.
4 Asoke Mukerji "International Cooperation on Cyber Space: India's role" Ministry of External Affairs, April 04, 2018, Accessible at https://www.mea.gov.in/distinguished-lectures-detail.htm?743.

discussions around the Tallinn Manual, which is a set of non-governmental guidelines for engagement during war.[5]

In a recent bid to continue its efforts in cyber norm formation, the UNGA (United Nations General Assembly) has approved two draft resolutions on the actions of states in cyberspace.[6] First, that of the Russian Federation called the "Developments in the field of information and telecommunications in the context of international security" and the second draft resolution titled "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" of the US. India voted in favour of both the resolutions.[7] These votes allow India to respond to policy windows and build on positive aspects of both approaches to formalise a move that encapsulates the needs of the region and the developing world.

India has always campaigned for "open and equal access" to the internet. In fact, the July 2018 draft National Communications Policy upholds net neutrality that highlights the country's non-discriminatory approach as opposed to the internet policies of major powers like China that tries to control the internet and the US where net neutrality has faced setbacks.

Recommendations

1. **Setting Up a Resilient Infrastructure**

The cyber landscape is continuously changing, and it is pertinent for India to effectively respond to cyber threats by outlining an institutional framework ensuring the country's digital safety. India's multi-stakeholder model involving Meity, NCIIPS (National Critical Information Infrastructure) and NCCC (National Cyber Coordination Centre) besides state level apparatus often creates confusion and coordination problem. To add on to this, there are private level CERTs that operate independently.

There needs to be a nodal cyber security officer who connects with all the CISO (Chief Information Security Officer) and CERT-In (both private and government) in order to ensure compliance, feedback and effectiveness to deal with cyber issues. Furthermore, these organizations

5 Arun Mohan Sukumar, "Upgrading India's cyber security architecture," *The Hindu,* March 09, 2016. Retrieved from https://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article8327987.ece.
6 Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," *Council on Foreign Relations*, November 15, 2018. Retrieved from https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
7 Arindrajit Basu and Elonnai Hickok, "Cyberspace and External Affairs: A Memorandum for India" *The Centre for Internet and Society*, August 2018. Accessible at https://cis-india.org/internet-governance/files/cyberspace-and-external-affairs.

could setup a "responsible vulnerability disclosure program," that could act as bug bounty and aid in fortifying the threat repository. Additionally, building a central repository of threats that can be accessible to all and by all would help undertake preventive measures. This should also include a stepwise threat re-addressal mechanism along with data-loss prevention program to avoid loss and leaks of crucial data. Moreover, effective incident management plans should be laid out and used in mock drills to ensure timely action.

It is vital to establish robust and systematic cyber risk management processes across all critical sectors that are becoming digitalised. In this context, a dedicated rapid response team should be established that can facilitate quick response and recovery plans to cyber breaches, considering most of the sectors are interdependent and these attacks may have a cascading effect. The rapid response team should be provided with specialised training and should possess quick disaster recovery capability.

There is also a need to develop expertise in the field of cyber forensics. Cyber forensics aid in examining and analysing available digital evidences as part of investigations and assessments of cyber crime. There is a stark shortage of resources as well as technical capabilities in this field in India. There is a need to set up cyber forensic training programmes and cyber crime analysis labs for effectively countering future cyber threats. It is important that there is a continuous monitoring of all ICT (Information and Communication Technology) system and networks, including analyses of logs for unusual activity that could indicate an attack. This monitoring strategy could aid in producing and enhancing supporting policies.

It is highly advisable that any new system that is being put in place must ensure "security-by-design"[8] practices to address cyber issues upstream and along the supply chain. Simultaneously, there also needs to be cooperation among different sectors, including that of government and private organisations. As cyber threats cannot be tackled in silos, multi-sector cyber security drills are required to test cooperation across multiple sectors and also address interdependencies during a major cyber attack.

There is a need for a well-coordinated effort towards cyber security that follows a reciprocal approach, that is, a combination of bottom up and a top down approach. Since the Digital India move is targeting audience sector-wise, like the banking and finance sector, healthcare sector, etc., it is also important that cyber security hubs are set up sector-wise since the attack and data thefts

[8] Security-by-design is a best practice to ensure that system is developed with security consideration upfront and throughout its lifecycle.

have also become more targeted. There is a need for a tailored industrial security program that aims at protecting the key assets in case of a cyberattack. In any industry, some of the data, systems and applications are more critical than others. For instance, in an oil/ power industry, the ICS (Industrial Control Systems), PLC (Programmable Logic Controllers) and SCADA (Supervisory Control and Data Acquisition) is important than in the healthcare system where the patient information is far more important. Few sector-specific proposals are listed below.

- **Healthcare Sector**

Healthcare in the recent past has seen technological advancement in terms of patient information storage and doctor prescriptions. As this sector moves towards digitalisation, there will be improvement in patient care and in the communication of health records. However, there is a perpetual fear of online data being stolen and ending up in the hands of cybercriminals. In 2018, MGM Hospital in Vashi, Mumbai, became a victim of a cyberattack which locked the hospital data and demanded ransom in bitcoins.[9] Similar incidents of WannaCry, Petya and NotPetya ransomware shook critical information infrastructure (CII) of many countries, especially the United Kingdom's National Health Service (NHS), where more than 70,000 devices like laptops, desktops, and medical machinery were infected asking for ransom in cryptocurrency to decrypt the encrypted data of the hospitals.[10]

It has been predicted that by 2025, most of the hospitals worldwide would move to a digital platform, thereby increasing the market size of the healthcare sector from USD 16.92 billion in 2017 to about USD 58.78 billion by 2025.[11] Such a turn of events increases the risk of cyberattacks if the network is not aptly defended from external threats.

The Union Cabinet of India, in 2017, approved the formulation of the National Health Policy,[12] under which a National Electronic Health Authority (NeHA) is to be setup. Such a policy would evolve and expand health information network across the continuum of care, in areas of e-Health, m-Health, Cloud technology and IoT, in healthcare delivery. The Ministry of Health and Welfare

9 Vrushali Purandare, "Cyber-attack on MGM Hospital," *The Asian Age*, July 19, 2018, Accessible at https://www.asianage.com/metros/mumbai/190718/cyber-attack-on-mgm-hospital.html.
10 Alex Hern, "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017, *The Guardian,* December 30, 2017. Retrieved from https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
11 Smart Hospital Market report, Allied Market Research, *Allied Market Research*, July 2018, Retrieved from https://www.alliedmarketresearch.com/smart-hospitals-market.
12 National Health Policy 2017, Ministry of Health and Family Welfare. Retrieved from https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf

introduced the draft bill for the Digital Information Security in Healthcare Act (DISHA) in March 2018.[13] One key purpose of the proposed bill is to secure data and create reliable storage of healthcare data. It will constitute a health information exchange, as deemed eligible by the Act, to hold the digital health care data of an individual (patient). The central government plans to incorporate a database to store information of patients and other health system components at the district and national-levels (National Health Information Network) which is expected to be implemented by 2020 and 2025 respectively.[14] A key suggestion to complete the project is by linking of Aadhaar to the health information network so that the patient identification would work seamlessly. It also included the private sector in developing the common network, to help in accessing information by both public and private healthcare providers.

With the implementation and allocation of funds in the Union Budget of 2019 for the Ayushman Bharat Yojana[15] that is currently underway, healthcare has been given importance as a primary focus area for the country. Meanwhile, to ensure better coverage for the healthcare initiative, the Ministry of Health issued a critical document for public consultation to completely digitalise healthcare data by 2020, with the aim to create a national digital health network called "National Digital Health Blueprint."[16] This would help deliver value-added services to the concerned user with a consent-based flow of citizen's health record.

Proposals

a. Multiple recommendations have been proposed by the Government of India, but the implementation has not been up to par. It requires better research in the implementation procedures and regulations for the same. DISHA, although a very thought-out proposal, is yet to come to fruition, and this requires a stead-fast approach for faster and widespread implementation.
b. Improved awareness, training, and resources allocation for employees, nurses and doctors to accommodate the security implications of patient information is a necessity in the healthcare sector.

---

13 Digital Information Security in Healthcare Act (Draft), Ministry of Health and Family Welfare, March 21, 2018. Accessible at https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf
14 See, Note 10.
15 Budget 2019: Government to allocate Rs 6400 crore for Ayushman Bharat Scheme, *Business Today*, July 03, 2019. Accessible at https://www.businesstoday.in/current/economy-politics/union-budget-2019-government-to-allocate-rs-6400-crore-for-ayushman-bharat-scheme/story/316068.html.
16 National Digital Health Blueprint Report for Public Comments, Ministry of Health and Family Welfare, July 15, 2019. Retrieved from https://main.mohfw.gov.in/newshighlights/national-digital-health-blueprint-report-public-comments.

c. A cyber security task force should be in place specifically for the healthcare sector under the CERT-IN, which is interoperable between the private and public healthcare providers.
d. The importance of Aadhaar information to be secure is crucial, especially as the threat of cyber attacks on the Aadhaar database remains high.[17]
e. Considering India has no dedicated privacy and data protection initiatives or laws in the Constitution of India (under Article 21) under Right to Privacy, it has been proposed that India requires a dedicated provision for the privacy of healthcare data, especially medical history, the biometric or genetic information of an individual.
f. Ayushman Bharat Yojana being a landmark project in providing better healthcare covering a chunk of the population, it is necessary to incorporate a digital data security initiative along with the scheme so as to work hand-in-hand with the developing health sector.

Energy Sector

The energy sector remains an appealing target for a well-resourced criminal organization looking to cause disruption and damage, as well as for a nation-state attempting to spread a political message or present a global posture of their goals. For instance, Ukraine's power grid led to a power outage affecting the daily lives of hundreds of thousands of citizens.[18]

The Nuclear Threat Initiative (NTI) has enlisted around 23 cyber incidents at nuclear facilities over the last three decades — owing to a multitude of threat actors and vectors such as software error, espionage, data theft, employee attempted sabotage, network intrusion and spear-phishing.[19] Stuxnet remains one of the most discussed and referenced cyber incidents, where PLCs were commandeered to sabotage the centrifuges at Iran's Natanz uranium enrichment plant.[20] As a recent example, the cyberattack in the IT network of the Kundankulam Nuclear Power Plant located in Tamil Nadu despite being air gapped showcases the vulnerability of these critical infrastructures in the country.IT networks facilitate the storage and traversing of myriad business sensitive and classified information and hence often become a soft target to gather sensitive

17 "Aadhaar Security Breaches", *FirstPost, September 15, 2018*. see https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html.
18 Kim Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," *Wired,* March 03, 2016. Accessible at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
19 Nuclear Threat Initiative, "References for Cyber Incidents at Nuclear Facilities," *Retrieved from https://www.nti.org/analysis/tools/table/133*.
20 "How Stuxnet cyber weapon targeted Iran nuclear plant", CS Monitor, November 16, 2010, Accessible at https://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

information. It could further be used in perpetrating malicious and hostile acts which could disable, destroy or compromise the computer resource critical to the security or safety of the facility.[21]

The IT Act of 2000 created the National Critical Information Infrastructure Protection Centre (NCIIPC), an organization striving to facilitate safe and secure information infrastructure for critical sectors of India, the India Country Report (2017)[22] on Smart Grids by the Department of Science and Technology highlights the growing cyber security concerns among businesses and Government regarding the Critical Infrastructure. In December 2010, the Ministry of Power constituted four CERTs dedicated to the energy sector as enumerated below.

- CERT - Thermal - National Thermal Power Corporation (NTPC),
- CERT - Hydro - National Hydroelectric Power Corporation (NHPC),
- CERT - Transmission POWERGRID, and
- CERT - Distribution - DP&D Division, Central Electricity Authority (CEA).[23]

Currently, the Information Sharing and Analysis Centre (ISAC - Power) which was conceived from the IT Act 2000 is the central coordinating agency to share and analyse various cyber security incidents in the power sector. But the agency has little interoperability with real-time problem solving initiatives.

Proposals

a. India requires a common Threat Intelligence Command Centre for the four CERTs in the energy sector helping private enterprises and the Government agencies to aggregate, analyse and devise plans to counter-act a cyberattack in real-time. Such Command Centre exposes the Indicators of Compromise (IoCs) in the system, post-cyber-attack for constant refinement and evolution in its operation.
b. India's energy sector was designed and built before the cyber security of these sectors were ever a concern. It has been proposed that there should be a structured plan to improve the designs of these systems with state-of-the-art technologies in a timely fashion. This helps the system to withstand cyberattacks. The advances in technology should include equipment for automation and command, such as connected appliances which derive from the IoT and detect, declare and dodge cyberattacks in real-time.

---

21 IAEA Technical Guidance/Reference Manual, "Security at Nuclear Facilities," Nuclear Security Series No. 17, *International Atomic Energy Agency*, 2011, p. 2.
22 India Country Report 2017, Department of Science and Technology, Government of India, June 2017. Accessible at http://dst.gov.in/sites/default/files/India%20Country%20Report%20on%20Smart%20Grids.pdf.
23 Grid Security Export System, Press Information Bureau, March 16, 2015. Accessible at http://pib.nic.in/newsite/PrintRelease.aspx?relid=117116.

c. There should be a central governing body of experts to train and employ skilled people in these sectors, with an increase in R&D (research and development) expenses for home-grown security technologies.

- **Banking/Finance Sector**

The financial sector faced almost thrice the cyberattacks as compared to other industries because of the easy monetary gains.[24] With reoccurring cyberattacks seen across the world from Taiwan in 2017[25] in a SWIFT attack to Malaysia's central bank being attacked in March 2018,[26] the financial sector has been affected for the longest time. The cyberattacks using SWIFT that hit India includes the Union Bank of India on July 2016[27] and the City Union Bank on January 2018.[28] In August 2018, the Indian Cosmos Bank system was hacked by cyber-criminals who siphoned off nearly 944 million rupees through multiple transactions across 28 countries.[29] The hackers stole customer information through a malware attack.

Considering the pace of digitalisation of financial transactions (non-cash payments) in the future estimated to overtake cash transactions by 2023,[30] and with increasing internet users, the security of individuals' financial data can be put to test. According to the Norton cybercrime report of 2017, about 186 million Indians have been affected by cybercrimes, estimating the total financial losses to USD 18.5 billion.[31]

The Reserve Bank of India has put in place a cybersecurity framework for all banks within the country to abide by, through resilience requirements, Cyber Security Operation Centres (C-SOC), and a Cyber Security Incident Reporting (CSIR) mechanism.[32] It includes implementation of a

---

24 "Cyber Security in Banking Sector: Our Perspective", *BDO India.* Accessible at http://www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf.aspx?ext=.

25 Iain Thomson, "Hackers nick $60m from Taiwanese bank in tailored SWIFT attack," *The Register,* October 11, 2017. Accessible at https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/.

26 "Malaysia's Central Bank Suffers Cyber Attack. Are you Vulnerable?, *CFO Innovation,* Accessible at https://www.cfoinnovation.com/risk-management/malaysia-s-central-bank-suffers-cyber-attack-are-you-vulnerable.

27 Suhasini Haidar and Manojit Saha, "Hacked: How $171mn stolen from Union Bank was recovered," *The Hindu,* Accessible at https://www.thehindu.com/news/national/hacked-how-171-mn-stolen-from-union-bank-was-recovered/article18063938.ece.

28 Saloni Shukla and Shilpy Sinha, "City Union loses $2 million in cyberattack, retrieves half," *The Economic Times,* Accessible at https://economictimes.indiatimes.com/industry/banking/finance/banking/city-union-loses-2-million-in-cyberattack-retrieves-half/articleshow/62956557.cms?from=mdr.

29 Rajendra Jadhav, "Cosmos Bank loses $13.5 million in cyber-attack," *Reuters* .Accessible at https://in.reuters.com/article/cyber-heist-india/cosmos-bank-loses-13-5-million-in-cyber-attack-idINKBN1KZ1J9.

30 RazorPay. The Era of Rising Fintech report, Accessible at https://razorpay.com/blog/era-of-rising-fintech-digital-payments-upi-report/,.

31 Norton Cybersecurity Insights report 2017, Accessible at https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

32 Reserve Bank of India. Cyber Security Framework in Banks, Accessible at https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF.

safer platform for constant surveillance with advanced real-time capabilities to detect threats across interconnected systems. A Cyber Crisis Management Plan avoiding confusion in the event of any cyberattack is also proposed in the circular, including detection, response, containment and recovery.

India has seen many reforms in the banking sector to help the customers enjoy greater benefits such as financial inclusion, Pradhan Mantri Jan Dhan Yojana, Interbank ATM Transactions through National Finance Switch (NFS), Immediate Mobile Payment Service (IMPS), etc. But it comes at a price when financial data shared within the system is not secure and safe.

Proposals

a) Indian banks can equip Artificial intelligence and machine learning as it helps reduce noise by distinguishing between real alerts and false positives. As the support by machine learning improves mechanisms over time they can be deployed to integrate diverse security controls and platforms. Integrated systems can conduct continuous sweeps across the Indian bank's IT data, applications, and network and infrastructure, interrogating databases in search of anomalies.
b) India's banking sector under the authority of the central bank requires area-wise network segmentation, better firewalls, and visibility solutions to detect and respond to attacks in real-time.
c) Use of effective techniques to enhance threat detection and threat response in the Indian banking infrastructure, through deception technology by generating traps or decoys that mimic the real technology could be put in place. [33]
d) Introduction of blockchain, with permissioned access, could keep the financial data shared within the system encrypted, to avoid any theft or loss of data, coupled with the ability to be regulated as a consortium blockchain.

- **E-Governance**

E-governance is how governments, through technology, improve relationships with their citizens. E-governance connects the citizens directly or indirectly to the government processes. Public-private partnership is a key component in e-governance, wherein this engagement addresses awareness, training, technological improvements, vulnerability remediation, and recovery operations. Along with reduced paperwork, improved databases, and better inter-connectivity, e-

[33] "What is Deception Technology?" *ForcePoint*, Accessible at https://www.forcepoint.com/cyber-edu/deception-technology.

governance also boasts of increased efficiency in public administration and deeper societal penetration.

Although there are multiple challenges for adoption of e-governance in India due to language constraints, low IT literacy, accessibility of IT services at grass-root level, lack of awareness among people, and economic challenges to adopting major projects, but the potential is endless. A central component of successful e-governance implementation is about identity management and the security of data from cyber threats. Through Aadhaar system, India has moved ahead in the race for e-governance, with a central registry of citizens identity. But the protection of this data is important for e-governance to succeed.

Multiple initiatives taken up by the Government of India includes the Digital India initiative which spawned the Digital Locker (DigiLocker), [34] wherein government and other agencies can send digital documents of citizens, and store citizen documents and certificates, enabling accessibility of documents anytime and anywhere, with verification at source systems in place. Jan Dhan Yojana, a mammoth initiative providing economic inclusivity to unbanked citizens, is part of India's e-governance development initiatives. Another such initiative is the e-Sign initiative, [35] where a digital signature cannot be impersonated and is safer and less misused for government documents and certificates. Nevertheless, the data breaches continue to be of prime concern.

Proposals

a. India should encourage the adoption of Public Key Infrastructure (PKI) like the Digital Locker platform, for trusted communications and transactions within the government, to facilitate collaboration and cooperation among stakeholder entities including the private sector in the area of cyber security in general and protection of CII in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures and adoption of best practices.
b. India requires a forward-looking and flexible policy framework when implementing e-governance to ensure the best outcomes from a public policy outlook. Although India is not yet ready for mobile governance, the scope of it along with e-authentication capabilities could boost the e-governance mechanism in India. And the data protection framework for the same should apply to both the private and public sectors, working hand-in-hand.

[34] Nikhil Agarwal, "What is DigiLocker and how to use it to carry all documents on your mobile phone," *LiveMint,* Accessible at https://www.livemint.com/Technology/vt7Sx2J2DTaoyVpMqsRxiM/What-is-DigiLocker-and-how-to-use-it-to-carry-all-documents.html.
[35] Further details about E-sign (NSDL e-Gov) may be accessed at https://www.egov-nsdl.co.in/e-sign.html.

c. For the protection of data while in process, handling, storage, and transit and the protection of sensitive personal information to create a necessary environment of trust, India requires round-the-clock sectoral CERT's for coordination and communication for effective incidence response and crisis management.
d. India requires a mandated periodic audit and evaluation of the adequacy and effectiveness of CII, and for it to succeed it should have a well aware and equipped work force that is well sensitized in the importance of data security in e-governance.
e. Confidential files should be crypto-isolated in a secure application space. Devices that are accessing the confidential data should be tested for integrity.
f. Wider adoption of initiatives like e-Sign into government activities can lessen the hassle and misuse of the existing system.

- **Transportation Sector**

The transportation system is becoming more connected by utilizing the possibilities from the IoT, self-driving cars, unmanned aerial vehicles (UAVs), better-integrated railway systems to the implementation of blockchain into the shipping industry to reduce hassles and thereby increasing efficiency. However, the transportation sector is also affected by the menaces of cyber-threats. As more devices and control systems are connected online, more vulnerabilities will appear, increasing the potential for disruption to physical assets.

The aviation industry, shipping industry, and railway system are vulnerable to such cyber-attacks. In May 2019, Kolkata airport suffered a cyber-attack that led to the shutdown of LAN (local area network), thereby delaying more than 30 flights and stranding around 4000 passengers. The attack also blanked out airline check-in terminals, flight information display, and airport CCTV surveillance.[36] The shipping industry is far more essential to be secure from cyber-attacks considering the number of goods that are transported daily. The railway industry, which heavily relies on IT and automation, control train movements, control signaling infrastructure, support train operations and timetabling planning, too is highly vulnerable to cyber-attacks.

To ensure cyber security in the Indian railway system, many initiatives have been implemented to digitalise and maintain the railways, such as the RailCloud Server,[37] which is a virtual server

[36] Tamaghna Banerjee, "Kolkata: 4000 flyers stranded as cyber-attack led to delay of 30 flights," *Times of India,* Accessible at https://timesofindia.indiatimes.com/city/kolkata/4000-flyers-stranded-as-cyber-attack-led-to-delay-of-30-flights/articleshow/69332483.cms.
[37] "Suresh Prabhu launches RailCloud for server optimization", *Times of India*, July 12, 2017. Accessible at https://economictimes.indiatimes.com/industry/transportation/railways/suresh-prabhu-launches-railcloud-for-server-optimisation/articleshow/59567324.cms.

accommodating bigger data with an in-built security system and Rail Saarthi App.[38] Although the railway is yet to initiate a railway-centric sectoral CERT, it is working in coordination with the CERT-In.

Threats to the shipping industry involve navigation, cargo control, disruption of trade activity, and even loss of lives. Therefore, cyber security is necessary for this industry. The WannaCry ransomware is an example of cyberattack that affected the global supply chain, corrupting navigation data, and causing delays of cargo transport. [39] In the logistics industry, cyber safety is more crucial to resilience and safety than to the protection of customer data.

The risk of cyberattacks is rising in the aviation industry. As the industry gets closer to becoming fully e-enabled and automation increases, pilot practices and training will need to adapt in the event of a system failure or cyber-security breach.

Proposals

a. Sectoral initiatives such as the establishments of CERT for Railways, Aviation, and Cargo Shipping is required to avoid future setbacks.
b. Introduction of a closed blockchain system into the port management system of the Indian port system, in coordination with the Sagarmala initiative, can drastically increase secure transfer of data.
c. A distributed architecture system in the Indian transportation sector could allow the cyber-threat to be contained in a particular area, rather than a single system that could be potential targets for cyber-attacks.
d. The advances in AI and machine learning should be tested and utilised to detect anomalies and cyber attacks in any of the three transportation sector.
e. Protection of public data is also paramount, hence there is a need for periodic audit and evaluation of the adequacy and effectiveness of digital infrastructure in railways, shipping and aviation industry.

[38] "Railway launches mobile app that does more than just booking", *Economic Times*, July 14, 2017. Accessible at https://economictimes.indiatimes.com/industry/transportation/railways/railways-launches-mobile-app-that-does-more-than-just-booking/articleshow/59597348.cms.
[39] Adrian Gonzalez, "The WannaCry Cyberattack: Another Warning for Supply Chain Executives," *Talking Logistics,* Accessible at https://talkinglogistics.com/2017/05/15/the-wannacry-cyberattack-another-warning-for-supply-chain-executives/.

2. Addressing the Threat of Emerging Technologies

As emerging technologies transform the operation of organizations and communities around the world, their sustainability is threatened by a myriad of cyber risks. There has been substantial growth in IT spending in India and scaling up in the use of technologies such as the IoT, Cloud Computing, AI and BlockChain.[40] It is expected that these will rise further, transforming India into one of the largest internet based markets across the world. With 5G and IoT set to reshape the entire ICT infrastructure, this, in turn, would pave the way for more dynamic cyber threat scenario.

AI and machine learning are data driven technologies that self-learn to perform an intended task. This technology could be employed as a potential guard against security threat that can keep a check on any probable cyber attack. In 2014, DARPA (The Defense Advanced Research Projects Agency) announced a Cyber Grand Challenge Mayhem as a two-year project with the goal of testing whether it was possible to develop AI systems that could find, verify and patch software vulnerabilities. As a result, Mayhem -an AI system was created that not only patched its own vulnerabilities but was also capable of exploiting the vulnerabilities of the opponents.[41] Thus, AI systems could assist in building smarter antivirus software as well as firewalls. For instance, old antivirus programmes scan networks to catch known viruses and malware. These programs need humans to update it regularly and are unable to keep up with malicious actors who deploy intelligent bots and tools to compromise networks easily. By leveraging machine learning, some antivirus programmes have been able to remove humans from the equation like the Avast Cybercapture.[42]

As the country moves towards 5G network and livelihoods depend on the network, cyber security should be given utmost importance.[43] The faster speed of the network is also likely to present opportunities for hackers to target more devices and launch bigger cyber attacks. Moreover, the associated increase in the volume, velocity and veracity of data also makes it easier for hackers to orchestrate more wide-scale cyber attacks without getting noticed. Many experts articulate that one of the biggest weak links in the future of cybersecurity is the communication between different

---

40 "Cyber Security in India: Opportunities for Dutch Companies," December 2028. Accessible at https://www.thehaguesecuritydelta.com/media/com_hsd/report/218/document/Cyber-Security-in-India.pdf.

41 David Brumley, "Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them," *IEEE Spectrum,* January 29, 2019, Accessible at https://spectrum.ieee.org/computing/software/mayhem-the-machine-that-finds-software-vulnerabilities-then-patches-them.

42 Aaron Tay, "How emerging technology is advancing cybersecurity methods," *TechinAsia,* May 13, 2019, Accessible at https://www.techinasia.com/emerging-technology-advancing-cybersecurity-methods.

43 Karishma Mehrotra, "V Kamakoti: With 5G, more people will be dependent on network, so security will be very important," *The Indian Express,* August 05, 2019. Accessible at https://indianexpress.com/article/technology/tech-news-technology/v-kamakoti-5g-technology-network-security-wifi-internet-5878156/.

devices connected to the internet also known as IoT. In 2016, a cyber attack using hundreds of thousands of cameras, routers and digital video brought down websites of big companies, including Spotify, Twitter and the New York Times.[44]

With the number of devices multiplying so are the security challenges in the cyberspace. This shows the dual nature of current ICT technologies -- if they can be used for defences than they can also act as an effective offensive weapon. These advances are also making the techniques used by hackers more innovative and smarter. There are automated phishing kits, to exploit emerging technologies like machine learning and ready to use malware (or ransomware) that can be bought off the dark web. Autonomous malware, once within the system, can mimic a normal user behavior and may spread within the network without any assistance from humans.

In days to come, more futuristic technologies would become a part of the ICT matrix and the policy document should be agile to accommodate the impact of disruptive technologies and future challenges of the digital landscape. These advances in new age technologies would facilitate the easy defeat of traditional cyber solutions, so reliance on static cyber defence may no longer be viable. There is a need for a cybersecurity framework that employs active defence mechanism like creating a "zero-trust model" as opposed to the "Trust, but verify" model, that means treating all systems or networks with suspicion of being attacked. This will enable a proactive response to any vulnerability detected.

Handshaking of public and private entities is another area that needs to be addressed thoroughly in cybersecurity policy making. This partnership is especially well-suited for areas that require diverse types of expertise and knowledge to address cyber security issues. This partnership is also an answer to government's limited resources for capability building. Most of the private players in India have imbibed the security culture and the best practices due to the demands and interests of global clients. They have eminently delivered services to their satisfaction. The IT sector is the most mature in its preparedness, and the country can benefit immensely if its services are leveraged for meeting the needs of cyber security. Thus, the country needs to prioritize collaboration to figure out how to utilize the potential of all emerging technologies to lock down current and future IoT devices against threats.

[44] Nick Huber, "A hacker's paradise? 5G and cyber security," *The Financial Times,* October 14, 2019, Accessible at https://www.ft.com/content/74edc076-ca6f-11e9-af46-b09e8bfe60c0.

3. Building Trust and Promoting Collective Responsibility

In the digital era, it is important to have the ability and the capability to respond and manage cyber security incident from the grass root level. The key to tackle cyber threats and regulate cyber affairs is by building confidence among citizens. This process requires a collective effort. But without investing in the creation of sufficient cyber resources, any kind of cyber security effort would be a hoax.

The cybersecurity talent pool should be a combination of intelligence units, academia and industry. Governments should invest in human capital and collaborate with institutes of higher learning to expand the cybersecurity workforce. The government and the local establishments should support and facilitate basic research, technology demonstration, proof of concept and test-bed projects, especially in thrust areas of cyber security. There needs to be a set of baseline regulation for user policies covering acceptable and secure use of the organisation's systems.

Moreover, there needs to be a cognizance of few prevalent factors in the country like dynamically changing cyber threat landscape, the technical complexity of cyberspace and availability of skilled resources and appropriately addressing these gaps. To establish a cyber secure society, there needs to be security awareness programmes at all levels. For instance, setting up a staff training programme and introducing curricula academia and organizing conferences on the subject. This also includes educating people to tackle threats of disinformation and misinformation campaigns. These programmes could be tailor made to suit the interests of different segments of society, small scale traders and businesses. Under the ambit of corporate social responsibility and outreach programme, cyber hygiene and basics of cyberspace could be taken to grass root level. It is vital to recognize that businesses and individuals can reduce cyber incidents by taking basic measures. There needs to be a dedicated team that keeps the general public aware of the new cybersecurity measures that are in line with current technological changes. Though the government does maintain websites and twitter accounts like cyber Swachhta Kendra and Cyber dost, however, the reachability and promotions of the same have been low.

Government schemes such as 'Make in India,' 'Start-Up India' and 'Digital India' supplements the growth of cyber security market in India and are the links towards Public-Private Partnership (PPP) model.[45] India has seen an exponential increase in the tech-savvy population. These schemes enable the setting up of resilient cyber infrastructure. For instance, a startup called Smokescreen

[45] Tamaghna Banerjee, "Kolkata: 4000 flyers stranded as cyber-attack led to delay of 30 flights," *Times of India,* Accessible at https://timesofindia.indiatimes.com/city/kolkata/4000-flyers-stranded-as-cyber-attack-led-to-delay-of-30-flights/articleshow/69332483.cms.

uses deception technology to track and defeat hackers. Such startup companies with advanced capabilities would not only inject know how but also dynamism into the local cybersecurity community.[46] The Government can aid indigenous cybersecurity companies which can develop globally competitive and innovative capabilities in strategic areas of interest and sustain the long-term growth of a competent, professional workforce.

4. Need to have Effective International and Regional Cooperation in Cyberspace

Cyber Security as an issue is not confined by borders and hence requires a global solution and consideration. The current state of affairs shows that the jurisdictional gaps are often exploited by the perpetrators to their advantage. With the growing global interdependencies, a cyberattack on any country may have a spillover effect on other states as well. Therefore, there is a need to build a strong chain of active international collaborations both bilaterally and multilaterally in cybersecurity for an effective global cyber security network. Only through effective international "consensus and cooperation" cyberspace can become a more safe and secure place.

International cooperation is the backbone of cyber capacity building and sharing of best practices in the cyberspace. A number of maturity models have been developed to "assess and benchmark" cybersecurity capacity at the international level, and the Global Forum for Cyber Expertise (GFCE) was created as a first attempt to exchange and pool international expertise on CCB.[47] However, capacity building efforts are often seen as a foreign policy tool, that is, a mere means to advocate a particular model of internet governance, create market access for domestic companies, or promote specific technical standards.

It is important to understand that cyber security is important not only for security in itself, but also due to its larger impact on social and economic development worldwide. The cyber capacity building efforts need to be formulated as a chain process whereby small initiatives pave the way for larger projects.

India should also partner with international organisations like INTERPOL, Asia Pacific Emergency Response Team (APCERT), ASEAN CERT and others to tackle cybercrime and

---

[46] Libza Mannan, "Security startup Smokescreen uses deception technology to track and defeat hackers," *YourStory,* January 10, 2018, Accessible at https://yourstory.com/2018/01/security-startup-smokescreen-uses-deception-technology-track-defeat-hackers.

[47] Mirko Hohmann, Alexander Pirang and Thorsten Benner, "Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach," *Global Public Policy Institute,* March 06, 2017. Accessible at https://www.gppi.net/2017/03/06/advancing-cybersecurity-capacity-building-implementing-a-principle-based-approach.

enhance cyber incident reporting and response linkages. India has signed Memorandum of Understandings (MoUs) with various countries and also holds cyber-dialogue and cyber exercises with various nations. However, the country should also lead the cybersecurity dialogue in regional forums like SAARC and BIMSTEC, considering that most of the participants are developing countries and have weak ICT infrastructure that are prone to cyber attack. Many of the developing countries experience a dearth of trained manpower in the field of cybersecurity. India can effectively step up its game in the field and can aim to become a regional leader in developing norms in the cyberspace.

Conclusion

India has been embracing the changing digital landscape for a long term sustainable economic growth and public benefits. For instance, establishing a centralised database to ensure a one-stop solution for citizens to easily access government schemes, smart city initiatives or incorporating 5G network for speed and accessibility. With the digitalizstion project in full swing, cyber security cannot be left for afterthoughts. A whole lot of problems require an all-encompassing smart security solution. One of the best means as mentioned above is building a zero-trust model. Thus, being prepared to proactively safeguard organisations and institutes from possible cyber attacks.

It is applaudable that the country is moving in line with the current technological developments, however, the policies, legislations and regulations to address the issues due to these advances have been moving at a snail's pace. It has been announced that in 2020 India would come out with cyber strategy policy.[48] The only concern is if the country is equipped enough to walk the talk. Previously, past governments too came forth with authorities to regulate compliance and enforce penalties for non-compliance under the Information Technology Act 2000. But it was not as effective as expected. The Information Technology (Amendment) Act 2008 has been inactive for years, and very limited significant jurisprudential development has occurred on the subjects of cyber security, privacy and data protection over the past few years.

The government needs to be proactively engaged in order to create robust and clear laws in this matter. There is a need to train tens of thousands of security analysts, architects, threat analysts and security operations staff to address the resource gap in the field of cyberspace.

[48] "India to Unveil Cybersecurity strategy Policy in Jan," Press trust of India, *Business Standard,* August 28, 2019, Accessible at https://www.business-standard.com/article/pti-stories/india-to-unveil-cybersecurity-strategy-policy-in-jan-119082801528_1.html.

The threat of cyberspace is only going to rise in the coming years. If going digital is necessary to be at par with the changing world, then building a resilient and trusted cyber ecosystem is also a staunch necessity. This can only be achieved by effectively utilising state-of-the-art technologies and resources. The government needs to adopt a risk-based approach to security based upon assets rather than controls. Dedicated budget allocation should be there for research and development.

To further strengthen cybersecurity, global partners can come together, co-create and adopt world-changing solutions to high-impact cybersecurity challenges, including technology development, related industries, and building knowledge institutions. Underpinning this perspective is also a conscious attempt to 'glocalize' – localize the global and globalize the local -- to generate economic development opportunities whilst simultaneously tackling cybersecurity issues.

Only a holistic approach towards cybersecurity would facilitate the creation of a vibrant cyber security environment. The country should not have to wait for a cyber catastrophe to try to make this space safer and more predictable.

KRITIKA ROY is a Research Analyst at the Cyber Security Centre of Excellence, Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

RONNIE NINAN is a post-graduate scholar at the Symbiosis School of International Studies, Pune, India.

Disclaimer: *The views expressed in this paper are authors' own.*

The **Society for the Study of Peace and Conflict (SSPC)** is an independent, non-profit, non-partisan research organization based in New Delhi, dedicated to conduct rigorous and comprehensive research, and work towards disseminating information through commentaries and analyses on a broad spectrum of issues relating to peace, conflict and human development. SSPC has been registered under the Societies Registration Act (XXI) of 1860. The SSPC came into being as a platform to exchange ideas, to undertake quality research, and to ensure a fruitful dialogue.

Published by: Society for the Study of Peace and Conflict. Post Box: 10560, JNU Old Campus, New Delhi-110067. Website: **www.sspconline.org**

We welcome your feedback. Email your comments at sspconline@gmail.com

Designed and typeset by Excel Solutions, New Delhi.