ORGANISATIONAL GOVERNANCE OF CYBER SPACE IN INDIA

E. DILIPRAJ AND
RAMNATH REGHUNADHAN

Cyber space is defined by the National Cyber Security Policy of India as "a typically complex digital world arena comprising varying interactions among individuals, software and services, in an ecosystem enabled by the distribution of Information and Communication Technology (ICT) networks (NWs) as well as devices".[1] It is generally considered as a 'public good' that transcends the conventionally finite but perceived form of demarcated and delineated sovereign boundaries in the physical world. This transcending nature of cyber space and the related spatial paradigm exposes countries to a wide variety of circumstances, and can be exploited for malicious purposes by other nation-state(s) and non-state actor(s). The threat could emerge from 'rival' or 'not-so friendly' states, terrorists, criminals, anti-institutionalists, rival conglomerates or even from any random individual. In fact, as opined by Dr. APJ Abdul Kalam, the former president of India, "Cyber warfare is the biggest threat to national security which will render even the Inter-Continental Ballistic Missiles (ICBMs) insignificant as a security threat".[2] An increase over the years in the number of incidents of cyber attacks that target

Mr **E.Dilipraj** is Associate Fellow at the Centre for Air Power Studies, New Delhi.
Mr **Ramnath Reghunadhan** is a Post-Graduate Student at Mahathma Gandhi University, Kerala.

[1] "National Cyber Security Policy -NCSP 2013," available online at nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.Accessed on May 16, 2017.

[2] Air Mshl Anil Chopra, PVSM AVSM VM VSM (Retd), "Cyber: The Next Cold War", 2016, available online at http://www.defstrat.com/cyber-next-cold-war. Accessed on June 1, 2017

While cyber threats have become the new norm and cyber wars have become a reality in the current interconnected world, cyber space is still highly chaotic in terms of governance of the domain itself. Cyber related technologies are leapfrogging ahead at a rapid pace, giving no time for the establishment of a proper governance framework at all levels.

the Critical Information Infrastructure (CII) could readily have a multiplier effect on the security of the people, creating a kind of ripple down effect on the capabilities as well as the strategic interests of the state. The sources of the threats and attacks have increasingly adopted strategies that are relatively of low-risk and low-cost in nature, specifically focussing on the susceptible targets.

An imminent, precisely coordinated set of attacks could greatly overwhelm the defences of government authorities, and deplete, overutilise or render obsolete the resources in hand. It could disrupt the functioning of the critical information systems, even creating a serious threat to the national security of the country.

While cyber threats have become the new norm and cyber wars have become a reality in the current interconnected world, cyber space is still highly chaotic in terms of governance of the domain itself. Cyber related technologies are leapfrogging ahead at a rapid pace, giving no time for the establishment of a proper governance framework at all levels. Nevertheless, governments across the world, collectively as well as individually, are striving hard to create governance frameworks in order to bring order into this highly volatile domain. Even at the global level, cyber space governance involves heated debates on various platforms with the immediate agenda for creating global norms for cyber space. With the growing dependence on cyber technology for e-governance and for providing other e-services across the globe, clearly, cyber space governance would be an indispensible aspect of any country’s government in the near future. In this respect, this paper analyses the prevailing organisational governance of cyber space in India as well as the emerging challenges and loopholes, and offers suggestions in order to upgrade the governance structure in the country.

INDIAN CYBER GOVERNANCE

The history of organisational governance of cyber space in India began in the mid-1970s, with the establishment of the National Informatics Centre (NIC), with the intent to provide Information Technology (IT) solutions to the country as a whole. Within just two years, a satellite-based nationwide Very Small Aperture Terminal (VSAT) network, called NICNET (the NIC Network), was established by the NIC.[3] In 1980s, the INDONET, a public service data network, became operational.[4] This laid the foundation for the establishment of the Education and Research Network (ERNET), which was primarily intended to serve the academic and research purposes of the nation.[5] In the 1990s, India had only around five million telecom users,[6] and during the same period, the Telecom Regulatory Authority of India (TRAI) was created and was delegated with the powers to take decisions in regard to tariffs and related policy formulation(s).[7] Subsequently, it led to the formation of a new ministry, the Ministry of Information Technology (MIT), which was later merged with the Department of Telecommunications (DoT) to form the Ministry of Communication and IT (MCIT). In the beginning of the 21st century, the Telecom Dispute Settlement and Appellate Tribunal (TDSAT) was established. This ensued the inflow and imbibing of international best practices, and an effective Dispute Settlement Mechanism (DSM), which

Over the years, even with a relatively low internet penetration rate, the internet user base in the country has grown enormously, and, today, India has the second largest number of internet users in the world, mainly owing to its humongous population.

[3] Madhu, "Networks (ERNET, NICNET, OCLC, INFLIBNET, DELNET, JANET, BLAISE)", 2012, available online at http://netjrflibraryandinformationscience.blogspot.in/2012/04/unit-viii-networks-ernet-nicnet-oclc.html.Accessed on May 16, 2017.

[4] P. Raghavendra Rau and H. Raghav Rao, "INDONET: A PUBLIC SERVICE DATA NETWORK IN INDIA", 1993, available online athttps://flora.insead.edu/fichiersti_wp/Inseadwp1993/93-18.pdf. Accessed on May 17, 2017.

[5] IDSA Task Force Report March 2012, INDIA'S CYBER SECURITY CHALLENGE, Institute for Defence Studies and Analyses, New Delhi.

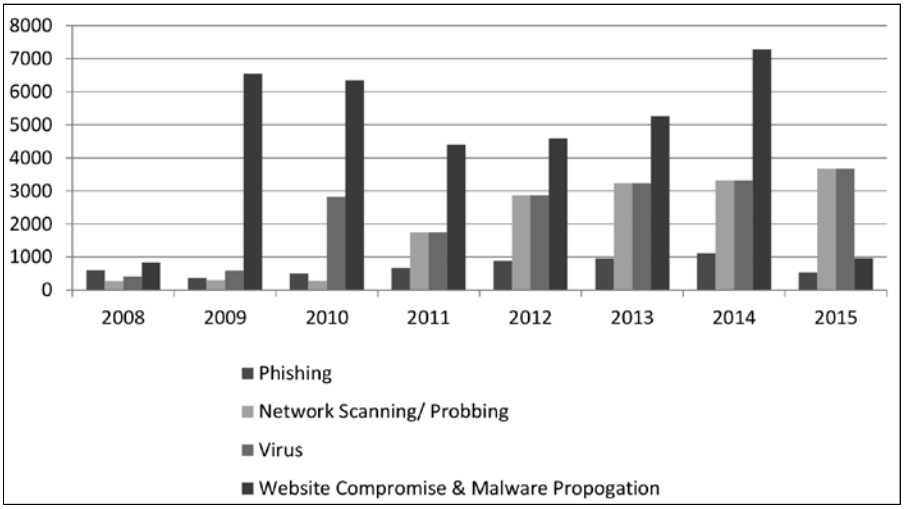
[6] Sunil Mani, "India's Telecommunications Industry," available online at http://www.nistads.res.in/indiasnt2008/t4industry/t4ind14.htm. Accessed on May 19, 2017.

[7] "History of Indian Telecommunication", 2011, available online at https://telecomtalk.info/history-of-indian-telecommunication/67789/. Accessed on May 19, 2017.

had a significant impact on the growth of the telecom sector in the country, along with an exaltation of the environment with fair competition and even the provision of safeguarding the consumers' interests. These efforts by the government, combined with the leapfrogging developments in cyber and mobile technologies, in turn, increased the number of internet users by nearly 70 times in the next 15 years.[8]

Over the years, even with a relatively low internet penetration rate, the internet user base in the country has grown enormously, and, today, India has the second largest number of internet users in the world, mainly owing to its humongous population. With this profile, there were instances where the nation was at the receiving end of cyber attacks. (Fig 1) The attacks were mostly in the form of breaches in data, phishing, trojan horse intrusions, organised cyber-related attacks, uncontrollable exploits such as computer worms or virus(es), malicious software code(s), malware attacks, websites being compromised, and so on.

Fig. 1: Cyber Security Related Incidents Dealt with by CERT-In



Source: Data compiled from CERT-In Annual Reports.

[8] M.M. Chaturvedi, M.P.Gupta and Jaijit Bhattacharya, "Cyber Security Infrastructure in India: A Study", 2008, available online at http://www.csi-sigegov.org/emerging_pdf/9_70-84.pdf, TDSAT, available online at www.tdsat.nic.in/. "Number of Internet Users - Internet Live Stats," available online at http://.internetlivestats.com/. Accessed on May 19, 2017.

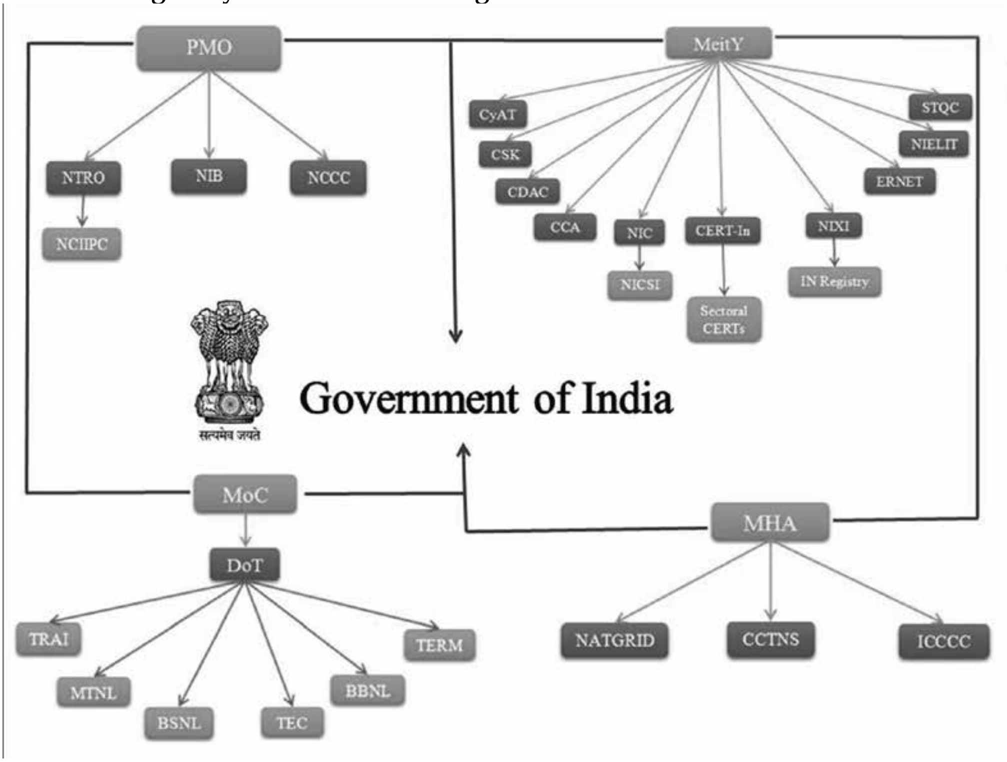
In 2015, the cyber-related attacks generally increased, and were particularly related to threats from virus(es) and / or malicious code(s). The increasing number of attacks was largely due to the huge number of first time users in India. According to a report by Symantec, India is second in the list of countries targeted by cyber criminals.[9]

Owing to the widespread use of, and dependence on, cyber space in the country, India is one of the most targeted countries in the world for cyber attacks. The array of threats to India's cyber security includes data theft, malwares, hacking of sensitive networks, web defacements, identity thefts, online financial frauds, e-mail spoofing, social engineering scams, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, unauthorised access to the critical infrastructures of the country, online surveillance and digital espionage. Over the years, the cyber security agencies of the country have been on a mission to reduce the malware and website compromise attacks against the country's cyber assets by strengthening the cyber defence systems like firewalls and use of malware removal tools, in the government as well as the private sector. While many acts of web defacements emanate from unfriendly countries like Pakistan, unauthorised intrusions into sensitive Indian networks are emanating from countries like China, the USA, Pakistan and a few other countries. The fact that India was identified as the fifth most snooped country by the USA through its digital surveillance programme, PRISM, as revealed in mid-2013 by Edward Snowden, has brought to light the vulnerable condition of the country's cyber security framework and its related technologies. Various fatal malwares like Stuxnet, Duqu, Flame, etc. which have the capability to damage the critical infrastructures of the country have also been identified from different Indian networks. Additionally, the country's cyber assets are also vulnerable to the most recent form of ransomeware attacks which have the ability to bring a country's cyber infrastructures to a standstill. Moreover, the potential of existing vulnerabilities in cyber space being exploited by violent non-state actors and various anti-social elements also poses a series of threats in this domain for the country.

[9] "Internet Security Threat Report (ISTR)", *Symantec*, vol 22, available online at https://www.symantec.com/security-center/threat-report. Accessed on May 16, 2017.

The prevailing threat scenario descibed above clearly showcases the inability of the state to keep up with, or adapt to, the ever shifting technological developments and the increasing number of the emerging threat vectors exploiting the existing vulnerabilities and interconnectedness, mainly due to the lack of an all-inclusive governance architecture and practice. The huge size of India's digital economy, the issue of it largely being unregulated is aggravating the challenge as far as governance of cyber space is concerned. While from a layman's perspective it might seem that the country is without any cyber governance framework, on the contrary, the country has already set up a robust cyber space governance framework that is fully functional at all levels. Fig 2 is a pictorial representation of the cyber governance organisational framework of India in its current form.

Fig 2: Cyber Governance Organisational Framework of India



Source: Data compiled by the authors.

It is clear from Fig 2 that the structure of the cyber governance organisational framework in India is spread across various departments and organisations functioning under four ministries namely the Prime Minister's Office (PMO), Ministry of Electronics and Information Technology (MeitY), Ministry of Communication (MoC) and Ministry of Home Affairs (MHA).

The PMO is the highest decision-making body and is the ultimate authority with respect to governing, coordinating and supervising cyber space in India. Under the PMO, the prominent organisations that deal with governance in cyber space are the National Technical Research Organisation (NTRO); National Information Board (NIB) and National Cyber Coordination Centre (NCCC). The NCCC is an upcoming organisation aimed to emerge as an umbrella organisation coordinating all law enforcement agencies and defence groups, especially in beefing up the cyber security of the country. Its functions include filtering, coordination and maintaining communication metadata, intelligence gathering and information sharing activities with other agencies. The Computer Emergency Response Team-India (CERT-In) acts as the main agency for establishing and running the functions of NCCC.[10] The next agency, the National Technology Research Organisation (NTRO) was set up to provide technical cyber security and intelligence, while acting as a hub for supplying technical intelligence inputs as well as for providing coordination and coherence to existing information sharing mechanisms.[11] Another important organisation under the NTRO is the National Critical Information Infrastructure Protection Centre (NCIIPC). This organisation acts as the designated agency to facilitate protection of the Critical Information Infrastructure (CII), in gathering intelligence, as well as in extrapolating emerging and imminent threats in cyber space. It is entrusted with the role to collect, analyse and disseminate intelligence, with regard to enabling any inter as well as intra-organisational linkages to identify potential, existing and emerging threats.[12]

[10] "National Cyber Coordination Centre (NCCC) of India May Become Functional", 2014, available online at http://ptlb.in/csrdci/?p=259. Accessed on May 14, 2017.

[11] Sandeep Unnithan, "Spy versus Spy", 2007, available online at http://indiatoday.intoday.in/content_mail.php?option=com_content&name=print&id=1067. Accessed on May 14, 2017.

[12] Saikat Datta, "Defending India's Critical Information Infrastructure: A report", 2016, available online at https://internetdemocracy.in/reports/india-nciipc-saikat-datta-2016/. Accessed on May 14, 2017.

The Ministry of Electronics and Information Technology (MeitY) works as an enabler in transforming the nation into a digital superpower, while empowering the citizens and creating a secure cyber space.

The Ministry of Electronics and Information Technology (MeitY) works as an enabler in transforming the nation into a digital superpower, while empowering the citizens and creating a secure cyber space. It makes policies related to Information Technology (IT), the internet (other than licensing to internet service providers), promotes infrastructure creation for e-governance and helps in bringing initiatives to bridge the digital divide and promote standardisation, and the like.[13] Many organisations operate under the MeitY. These are the Indian Computer Emergency Response Team (ICERT/CERT-In); National Informatics Centre (NIC); Standardisation Testing and Quality Certification (STQC); Controller of Certifying Authorities (CCA); Cyber Appellate Tribunal (CyAT); Education and Research Network (ERNET); Cyber Swachhta Kendra (CSK) which is also known as the Botnet Cleaning and Malware Analysis Centre; National Internet Exchange of India (NIXI); Centre for Development of Advanced Computing (CDAC); and National Institute of Electronics and Information Technology (NIELIT). The .IN Registry comes under NIXI and it supplements NIXI's activities to provide inclusiveness in the cyber domain. The National Informatics Centre Services Inc (NICSI) comes under the NIC and helps in promoting, utilising and developing the spinoff of services, technologies, infrastructure and expertise. The Unique Identification Authority of India (UIDAI), which was established in 2016 under MeitY, is responsible for enrolment, authentication, operation and management for Aadhaar, issuing Aadhaar numbers, and in playing a prominent role in ensuring the security of the identity information, data and authentication records of individuals.[14] Among all the agencies that function under the MeitY, CERT-In gains more prominence as it is the national

[13] "Ministry of Electronics and Information Technology (MeitY)", available online at http://meity.gov.in/. Accessed online on September 1, 2017.

[14] "About UIDAI", available online at https://uidai.gov.in/about-uidai/about-uidai.html. Accessed on August 29, 2017.

agency in the area of cyber security that monitors, collects, analyses, coordinates and disseminates information. It also forecasts, warns or alerts of any incidents, attacks that are imminent. It issues guidelines, advisories, vulnerability notes and White Papers relating to information security practices, procedures, and prevention, response and reporting of cyber incidents, while taking exigency measures in emergency situations. This enables an information sharing ecosystem and helps coordinate the 'cyber warriors' as well as 'cyber builders' of the nation, who are considered to be the frontline defence mechanism against most cyber threats and attacks.[15] CERT-In also functions closely along with various sectoral CERTs for the prevention and mitigation of crises in various strategic and core sectors of the state.[16]

The Ministry of Communication (MoC) plays a major role in providing services, issuing guidelines and taking necessary action with regard to infrastructure development for supporting the cyber space framework in the country.

The Ministry of Communication (MoC) plays a major role in providing services, issuing guidelines and taking necessary action with regard to infrastructure development for supporting the cyber space framework in the country. Under the MoC operates the Department of Telecommunication (DoT) under which fall various organisations, companies and autonomous bodies. These include the Telecom Regulatory Authority of India (TRAI); Mahanagar Telephone Nigam Limited (MTNL); Bharat Sanchar Nigam Limited (BSNL); Telecommunication Engineering Centre (TEC); Bharat Broadband Network Limited (BBNL); and Telecom Enforcement Resource and Monitoring (TERM). The DoT mainly intends to coordinate the Internet Service Providers (ISPs) and other related service providers, with regard to cyber security incidents, responses, and taking the requisite actions, while providing guidelines regarding roles and responsibilities, for creating a resilient but reliable network, capable of providing uninterrupted coverage

[15] "CERT India", available online at http://cert-india.com/. Accessed on May 18, 2017.

[16] "Sectoral CERTs", available online at http://pib.nic.in/newsite/PrintRelease.aspx?relid=112078. Accessed on May 18, 2017.

with the aim to bridge the digital divide, while facilitating socio-economic development and growth, in the creation of a knowledge economy by increasing internet penetration through the provision of cost-effective but high quality broadband services to the people and the nation as a whole.[17]

The Ministry of Home Affairs (MHA) issues security guidelines, assists and sensitises other ministries, departments and critical sector organisations with regard to securing and protecting CIIs and strengthening security measures.[18] Under the MHA, the prominent organisations related to cyber governance are the National Intelligence Grid (NATGRID); Crime and Criminal Tracking Network and Systems (CCTNS); and Indian Cyber Crime Coordination Centre (ICCCC or I4C). NATGRID was conceived to create and broaden a cutting edge framework to augment India's capabilities in data linking, mining and analytics, issuing security guidelines for securing physical infrastructure, strengthening security measures and sensitising the administrative departments and organisations to vulnerabilities while assisting the corresponding ministry or department(s).[19] CCTNS focusses on modernising the law enforcement agencies, their functions, envisaging nation-wide networking, information sharing, providing citizens with interface to register complaints and avail of services, with particular focus on centralised planning and decentralised implementation.[20] Finally, I4C, set up in 2016, facilitates online reporting of cyber offences, apart from monitoring, analysing and countering 'new-age' cyber crimes by integrating around 15,000 police stations across the country, along with NATGRID. It is intended to strengthen the capabilities of existing organisations like CERT-In and Centre for Development of Advanced Computing (CDAC). It is intended to deal with issues like cyber theft, social media terrorism, related recruitment and cyber espionage.[21]

[17] Discussion draft on National Cyber Security Policy, March 2011, Department of Information Technology, Ministry of Communications and Information Technology, Government of India, available online at http://meity.gov.in. Accessed on May 17, 2017.

[18] Amitav Malik, "Role of Technology in International Affairs", Institute of Defence Studies and Analyses (New Delhi: Pentagon Press, 2016), p.157.

[19] "Ministry of Home Affairs", in http://mha.nic.in/. Accessed on May 17, 2017.

[20] "Welcome to CCTNS Citizen Portal - Tamil Nadu Police", available online at www.eservices.tnpolice.gov.in. Accessed on May 19, 2017.

[21] Anurag Dwivedi, "Indian Cyber Crime Coordination Center (I4C): A Need to Relook?", 2016, available online at http://usiblog.in/2016/08/indian-cyber-crime-coordination-center-i4c-a-need-to-relook/. Accessed on May 15, 2017.

NEED TO IDENTIFY LOOPHOLES AND BRIDGE GAPS

During the immediate aftermath of the 9/11 attacks, Jacques Derrida, the French philosopher, opined that these attacks were part of the "archaic theatre of violence" of the real visible world, in which events are still to be conducted in a "clear and great order".[22] With cyber space has ensued the emergence of vulnerabilities and an increasing number and variety of threats to the security of India and its people. According to reports by Norton in 2013, around 42 million cyber crimes happened every year in India, with more than 80 people being victimised by various forms of cyber attack every minute. This had an estimated economic burden of US $8 billion for the nation, with the impact being extrapolated to incrementally rise in the future.[23] There has also been an increased number of attacks on India, by state and / or non-state actors, with about 50 percent of bot infected systems being tracked by CERT-In between the period 2013 to 2016.[24] In a 2012 report by Kaspersky, India was ranked ninth among the list of nations targeted in cyber space,[25] which was later raised to third place in its 2017 report.[26]

While the narrative in the previous section regarding the various ministries and departments that form the organisational governance of Indian cyber space gives a sense of security, the vulnerability prevailing in the Indian cyber space cannot be neglected. Therefore, there is a need to transcend the currently existing distinctive approaches by the ministries / departments / divisions, with overlapping responsibilities and activities, often leading to ineffectiveness in tackling and mitigating threats. The diverging visions, objectives, frameworks and rules often result in relatively

[22] Yoram Schweitzer, Gabi Siboni and Eina Yogev, "Cyberspace and Terrorist Organisations", *Military and Strategic Affairs*, vol. 3, no. 3, December 2011, p. 45.

[23] Ten percent of all cyber crimes globally happen in India: Study, available online at http://www.indiainfoline.com/article/news-top-story/10-of-all-cyber-crimes-globally-happen-in-india-study-113110815347_1.html. Accessed on August 28, 2017.

[24] "CERT India", available online at http://cert-india.com/. Accessed on May 18, 2017.

[25] Y. Namestnikov and Denis Maslennikov, *Kaspersky Security Bulletin 2012*.The overall statistics for 2012, available online at https://securelist.com/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/36703/. Accessed on June 8, 2017

[26] India Third Largest Spam Spewing Nation: Kaspersky Report", 2017, available online at http://www.bgr.in/news/india-third-largest-spam-spewing-nation-kaspersky-report/. Accessed on June 5, 2017.

hindered coordination among different agencies. This can lead to the creation of gaps in effectively implementing policies, as well as in efficient functioning, which may (in the future) exacerbate any existing vulnerabilities in the cyber defence mechanisms as well as the measures in place.

In India, the NIC is mandated to manage the entire digital platform of the governmental organisation, with its own rules and regulations. But there is an extended list of organisations, bodies and projects like NCIIPC, NCCC, many of which are given prominent positions in the governance structure of cyber space. In many situations, the lack of effective coordination between these agencies in their activities causes hindrances in dealing with crises or bridging vulnerabilities on a pan-India level.[27] Even the effectiveness of NCCC in coherently engaging the intelligence agencies, industry private bodies and the different stakeholders, including the public is yet to be seen.[28] Both NTRO (NCIIPC comes under it), and NCCC are assigned the authority to protect the CIIs, but need to circumvent the problems that may arise, with regard to the challenges, divergences, efficient and effective information sharing, coordination and a coherent working structure in finding viable solutions. There are gaps in the information sharing mechanisms which can create hindrances in effectively dealing with the Critical Information Infrastructure Protection (CIIP) of the nation.

It is believed that NCCC can help address the threat perception to take a proactive approach in dealing with the complexities, and could emerge as more accountable, if not transparent, on a need-to-know basis. This facilitates the prevention, mitigation and prosecution of anti-state or anti-social elements, and bridges the gaps in governing the cyber space while enabling a responsible as well as effective type of governance.[29] Thus, there is a possibility of creating and developing tenable solutions to the issues pertaining to the security of the nation with regard to the present and future

[27] Jonathan Diamond, "India's National Cyber Security Policy in Review", 2013, available online at http://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review. Accessed on June 5, 2017.

[28] n. 10.

[29] Geetha Nandikotkur, "India Opens Cyber Coordination Centre", 2015, available online at http://www.bankinfosecurity.in/india-opens-cyber-coordination-centre-a-8100. Accessed on May 17, 2017.

cyber space domain. Concepts like data localisation, data sovereignty, and cyber sovereignty are becoming prominent issues in the international fora. In any case, there is a prerequisite for India to become a 'cyber power' in the future. This would not be possible without the minimum physical infrastructure and technological development in technologies like the Internet of Things (IoT), cloud computing facility, network stability, CIIs, and block chain.

There is also a need to open up more data centres like the Common Service Centres (CSCs) in India, which could act as enabling factors to accelerate cloud adoption in the government services, as well as in encouraging storage of data domestically. This can help address the issues of cross-border flux of data, with regard to licensing the cloud-based services, the distributed sovereignty of data storage, and for successful implementation of international best practices. This can also increase the interoperability, address the security of CII, bring in the element of standardisation of technical parameters (of cloud computing networks), incorporate and implement a legal as well as regulatory framework for domestic and international cloud services (jurisdictions and *dejurisdictising* them), taking into consideration the interests of both the service providers and end users (cost-benefit analysis).[30] The CSCs can act as service delivery points in the rural areas of the country, acting as agents of change, promoting entrepreneurship, participatory and deliberative decision-making and capacity building, and, thereby, enabling a bottom-up approach. This can be supplemented by the establishment of a national nodal centre.[31]

Currently, in the I4C, there is a lack of inclusiveness in the deliberation, decision-making and implementing mechanisms. This affects the effectiveness of the measures being taken and their incorporation by different ministries, armed forces and other organisations. There are issues of overlapping and conflicting powers, functions, duties and responsibilities among I4C, CCTNS,

[30] Telecom Regulatory Authority of India: Consultation Paper on Net Neutrality, January 4, 2017, available online at http://trai.gov.in/sites/default/files/CP_NetNeutrality2017_01_04.pdf. Accessed on May 16, 2017.

[31] Mansi Taneja, "NIELIT to Train Thousands of Cyber Security Professionals", 2011, available online at http://www.infracircle.in/nielit-train-thousands-cyber-security-professionals/. Accessed on May 16, 2017.

In order to emerge as a cyber power, there is a need to institutionalise Research and Development (R&D) in developing (and implementing) high-end technologies like block chain, cloud computing, IoT and solutions for network security and stability.

NTRO and NCCC. All of them are given 'variant' authority to monitor, regulate and provide security in cyber space, but are instead creating fissures, jurisdictional issues or even applying isolationist tendencies over the sphere of work. It would be desirable for all these agencies to be brought into a comprehensive framework, so that they can complement and supplement each other. There exists a possibility of cooperation, coordination and convergence that can create an enabling ecosystem to prioritise, not just the security of the nation, but also the privacy and security of the country's netizens as well. These organisations could conduct a feasibility study on existing mechanisms and measures with regard to cyber resilience. In countering relevant threat perceptions, there should also be a technical capacity building mechanism at the pan-India level (on content monitoring) on the lines of the Network Traffic Analysis (NETRA) programme, which is currently under the Defence Research and Development Organisation (DRDO). But this should be balanced with the issue of the privacy of the citizens, and be in compliance with the accepted norm(s), legislative mechanism(s) and legal conditions judgement(s) in place.

Moreover, in order to emerge as a cyber power, there is a need to institutionalise Research and Development (R&D) in developing (and implementing) high-end technologies like block chain, cloud computing, IoT and solutions for network security and stability. Implementing indigenous technologies can help secure the country's system from external attacks, especially on critical infrastructure, while providing real-time access to information for the relevant stakeholders. There is also a need for expansion in activities related to development of infrastructure and indigenous technology, in the form of clusters or Software Technology Parks (STPs) and Innovation Centres in different parts of the country so as to foster innovative, creative and decentralised development of technology and security mechanisms. Currently, CDAC develops technolog(ies) related to supercomputing and cloud computing.[32] There is a need to interlink STPs, clusters and the Innovation Centres with CDAC, CSCs, NIC and ERNET, which can help accelerate the creation of infrastructure, connectivity, new technologies for data localisation, efficiency, capacity building and performance augmentation of the system in a decentralised fashion. This cluster should be interfaced and interlinked with the academia, government and industry, so as to enable an ecosystem that isn't redundant or defunct in terms of the contemporary technological developments or in dealing with threats emerging in relation to cyber space. The funding should be organised in the form of habitus of agencies or bodies that include members from the various sectors. The suggestions made so far, if implemented, could lead to the possibility of creating a second-strike capability for India, and possibly achieving cyber deterrence, at least among state actors.

On the cyber crime front, there is a low conviction rate in the country which is a major concern, amounting to just 234 convictions for 3,206 cases that were chargesheeted in 2015. There is a need to address the shortage of skilled personnel and judicial officers, as India lags far behind other nations in effectively adjudicating, and arbitrating in, such cases.

Also, on the cyber crime front, there is a low conviction rate in the country which is a major concern, amounting to just 234 convictions for 3,206 cases that were chargesheeted in 2015. The conviction rate was reduced to one-third in 2016, with many arguing about the relatively ignorant attitude of some of the officials or judicial officers in matters of adjudicating powers or veracity of digital evidence (in the aftermath of covering up of tracks by perpetrators).[33] There is a need to address the shortage of skilled personnel and judicial officers, as India lags far behind other nations in effectively

[32] "Centre for Development of Advanced Computing (C-DAC)", available online at https://cdac.in/. Accessed on May 18, 2017.

[33] A. Saikia, "Why Most Cybercrimes in India Don't End in Conviction", available online at http://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html. Accessed on June 8, 2017.

adjudicating, and arbitrating in, such cases. In the virtual world, it is being said that attacks can take place at the speed of light[34] and, thus, the existing legislations, namely, Telecom Regulatory Authority of India (TRAI) Act (1997), Information Technology (IT) Act (2000), Information Technology Amendments Acts (2008) and / or the National Cyber Security Policy (NCSP) (2013) have to be supplemented, if not complemented, by effective mechanisms to deal with matters in real-time.

There is a need to impart digital/cyber literacy and related high quality skills to the country's population. This issue gets exacerbated, especially due to the higher number of people lacking digital literacy, and, thereby, increasing the vulnerability, particularly in times of crises. The need to impart that kind of knowledge requires more trained professionals, teachers, infrastructure and, thus, more funding. There is also a need to tap the human resources in the country, especially when India has one of the largest cross-sections of youth in the world in terms of the demographic dividend.

The government has initiated the ISEA (Information Security Education and Awareness) project for developing human resources in the fields of data protection, and information security awareness generation, apart from offering cources like B.Tech, M.Tech and Ph.D in computer science in various universities and colleges across the country. A number of courses related to cyber security have also been initiated by the National Skill Development Agency (NSDA). Further, the government has set up the R.C. Bose Centre for Cryptology and Information Security with the aim to enable research, training, development and teaching in the field of cryptology and cyber security.[35] The universities and institutions should give more importance to skill-sets rather than just producing degrees or credentials. This can be given emphasis during the recruitment process, and can even help to reduce the brain-drain to a great extent. BSNL is said to have initiated the development of cities, interlinking it to cyber physical systems, and use of cloud computing for localisation and storage of data in cooperation with MTNL and BBNL for facilitating the requisite infrastructure facilities, especially the CII and its

[34] S. Kumar, ed., *India's National Security: Annual Review 2013* (New Delhi: Routledge, 2014), p.60.

[35] "Cyber Security Violations", Press Information Bureau, 2014, available online at http://pib.nic.in/newsite/PrintRelease.aspx?relid=112078. Accessed on May 16, 2017.

protection. It also intends to start a technical university, which, along with the Standardisation, Testing and Quality Certification (STQC) Directorate of the Meity, can develop and train proficient, skilled and adept personnel while improving the human resource capital and skilled professionals in the country.[36]

According to a few sources, in 2013, India's cyber security manpower numbered only around 556, which is miniscule in comparison to 1.25 lakh in China, 91,080 in the US and 7,300 Russia.[37] Due to the increasing number of internet users in the country, probably larger than the total population of a few countries in Europe, the existing cyber infrastructure as well as the related institutions in India are facing increasing 'stress' in implementing state-of-the-art measures, mechanisms and programmes. This can possibly delay the elevation of India as a 'digital power'. The National Cyber Security Policy 2013 (NCSP 2013) of the Government of India estimates that an additional 5 lakh skilled professionals are needed to protect India's cyber frontiers.[38] According to the report by the Central Statistical Office (CSO), the shortfall of cyber personnel could result in an increasing number of conflicts, litigations and issues with regard to cyber space. There are innovative ways to find skilled hackers and cyber security experts, such as conducting information security competitions like Capture the Flag (CTF), hacking exercises, cross-domain efforts for collaboration among companies to get experts on deputation, and so on. Such efforts have been tried and tested successfully in countries like the USA, Israel, China and Japan, which claim to have in place resilient cyber defence systems; it will require political will and support from the highest level possible for such an effort to succeed in India.[39] The issue can, to a great extent, be dealt with effectively by restructuring the recruitment process(es)

[36] "BSNL to set up Technical University for Engineering and Management Courses", 2014, available online at http://indiatoday.intoday.in/education/story/bsnl-to-set-up-technical-university/1/355586.html. Accessed on June 8, 2017.

[37] S. Joshi, "An IT Superpower, India has Just 556 Cyber Security Experts", 2013, available online at http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece. Accessed on June 8, 2017.

[38] "National Cyber Security Policy (NCSP 2013)", available online at http://meity.gov.in/content/national-cyber-security-policy-2013-1. Accessed on June 5, 2017.

[39] E. Dilipraj, *Cyber Enigma: Unravelling The Terrors in the Cyber World* (New Delhi: KW Publishers, 2017), pp. 212-225.

as well as streamlining the existing training programmes in an effective manner. An assemblage of a skilled but coordinated 'cyber army' for the nation can effectively match the force projected by the likes of China, the US and even other major non-state actors such as Google and Facebook.

The current reliance on public sector R&D has not, in the larger context, entailed the creation of an innovative environment in India that can efficiently upgrade, depending upon the increasing complexity of challenges. While India has accepted the populist approach of multi-stakeholderism when it comes to global internet governance, by including the private stakeholders, non-governmental actors and civil society, the country needs to invest in infrastructure development, instituting effective regulatory mechanisms and security measures, particularly in dealing with the protection of CIIs in its domestic environment.

The country needs to invest in infrastructure development, instituting effective regulatory mechanisms and security measures, particularly in dealing with the protection of CIIs in its domestic environment.

Currently, the focus on R&D could be need-oriented, and Public-Private Partnerships (PPP) in each sector need to be identified. India has already set up Information Sharing and Analysis Centres (ISACs) for information sharing and exchange on cyber incidents in the financial sector, and for entailing advice in taking appropriate steps and measures in mitigating crises. But the necessary steps should also be undertaken to set up similar ISACs in the petroleum and power sectors in a mission mode.[40]

Lastly, there is a need to take a proactive approach in terms of legislations (both domestic and international), and for implementing effective mechanisms on the ground. There is also a need for modernising the forces (in the cyber realm) with regards to their technical and legal capabilities, particularly in the form of a cyber police force, that can manage, coordinate and implement effectively the different norms and provisions that exist, as well as provide, enable, supplement, optimise and incorporate the use of international best practices with regard to India. There is also a need to undertake urgent steps

[40] n. 35.

to categorically implement the cyber security strategies in the short term (1-3 years), medium term (3-5 years) and long term (5-15 years) periods.

The threats in cyber space will evolve in new forms with the emergence of the Internet of Things (IoT), cyber physical systems, cloud computing and other future technologies.

CONCLUSION

The domain of cyber space is sometimes perceived to be an unregulated and chaotic spatial paradigm which is devoid of any politico-physical boundaries or demarcations. This could possibly create a kind of overlapping, confusion and / or issues within or between the organisations and ministry(ies). But a form of distinct centralised institutional governance on a distinct plane cannot exist, particularly because of the inherent nature of cyber space that transcends all boundaries or delineations existing in the physical world. The threats in cyber space will evolve in new forms with the emergence of the Internet of Things (IoT), cyber physical systems, cloud computing and other future technologies. In developing countries like India, with a large number of users, any form of the conventional approach undertaken by the ministry(ies) or government organisation(s) to work within a particular sphere does not provide optimum results, particularly in the cyber domain where everybody and everything is interconnected, interrelated and interdependent. Rather, an efficient and effective inter-organisational or inter-ministerial coordination, approach or body is necessary. The ability and utility of the architectural framework of a nation depends on its organisations, their coherent nature and coordinated actions as well as activities. India should focus on the development of "core internet infrastructure",[41] identify the existing and emerging complexities in cyber space and create new norms that can be set as international benchmarks. This is a prerequisite for creating as well as strengthening the effective governance of cyber space as well as developing the country into a 'knowledge powerhouse', which

[41] Indrani Bagchi, "India for Inclusive Internet Governance", 2014, available online at http://economictimes.indiatimes.com/tech/internet/India-for-inclusive-internet-governance/articleshow/34189920.cms. Accessed on June 3, 2017.

would, in turn, help, create a dynamic, security-oriented but open cyber space, with a distinct focus on an ecosystem that enables innovation and investment.

The inherent nature of cyber space creates a kind of virtual world that is interconnected and interlinked, and, thus, is hard to be equated with the 'Westphalian' concept of sovereignty. But the disruptions created in cyber space can create a kind of ripple effect that would greatly influence almost every actor, state and non-state alike. Currently, with the increasing incidences of cyber threats and attacks on almost every digitally interconnected nation, there is a need to bring in effective solutions, of which an important component resides upon the effective institutionalisation of organisational governance as well as coordination and regulation of cyber space within the nation. In order to have a safe and secure cyber space, India must enhance its organisational governance structure that enables expeditious information sharing, coupled with the establishment of a coordinated response system capable of alleviating as well as mitigating any kind of possible impairment by the malignant activities of different actors in cyber space. This includes protection as well as preservation of CIIs, which will not only reduce the vulnerabilities of the system but, most importantly, help maintain integrity. This is a requirement for a safe and secure cyber space and is possible only through a combination of institutional structures, people, processes, technology and cooperation.