GLOBAL PARTNERS DIGITAL

February 2016

Mapping the Cyber Policy Landscape: India

WRITTEN BY **SHUCHITA THAPAR**

Global Partners Digital
Second Home
68 - 80 Hanbury Street
London
E1 5JL
+44 (0)203 818 3258
info@gp-digital.org
gp-digital.org

Global Partners & Associates Ltd
Registered in England and Wales

Designed by SoapBox
Typeset by Jonathan Jacobs
Cover image adapted from David Nagy under Creative Commons Licence 2.0.
https://www.flickr.com/photos/ndave/

Company Nº 520 1603
VAT Nº 840 1912 54

GLOBAL PARTNERS DIGITAL

Mapping the Cyber Policy Landscape: India

WRITTEN BY SHUCHITA THAPAR

gp-digital.org

CONTENTS

INTRODUCTION

India's focus on cybersecurity is relatively nascent, but rapidly growing. In the past few months alone, the field has been in the news following significant cyber attacks on Indian IT companies[1] , and large-scale data breaches leading to the compromise of debit cards from 19 Indian banks[2]. It was recently reported that there were nearly 40,000 cybersecurity incidents in India between January and October 2016[3]. The Central Government in November 2016 also announced demonetization measures[4], withdrawing larger-denomination (i.e., INR 500 and INR 1000) currency notes from usage. This has led to a spike in the usage of electronic money, which means there will be increased necessity for strong cybersecurity systems and norms in the short-term future[5].

There have also been reports that the Central Government is looking to set up an INR1,000-cr cybersecurity R&D fund[6] , as well as to expedite the creation of a National Cyber Coordination Centre[7] , and to revamp cybersecurity norms applicable to banks[8] . The Minister for Electronics and Information Technology recently announced measures strengthening the Indian Computer Emergency Response Team ("CERT-IN"), along with the creation of specific state emergency response teams and sectoral teams[9] . All this goes to show the recent focus on cybersecurity as an area where resources and research are targeted.

However, there is limited legislation and policy covering the field. Few civil society organisations work on issues of cybersecurity. While there are several government ministries and agencies working on cybersecurity and allied issues, they remain largely uncoordinated and generally unchallenged. In 2012, a Joint Working Group on cybersecurity[10] made several suggestions as how the private sector could be engaged with in relation to cybersecurity, including involvement in capacity building, creating institutional frameworks and preparing security standards. However, this report did not specifically refer to civil society or NGOs, and mainly focused on industry players. This has generally been a feature of cybersecurity policy, as will be further detailed in this report.

This report attempts to review;

- The ministries and government bodies working most directly on cybersecurity issues;
- The legislative and policy framework governing cybersecurity;
- Non-governmental organisations working on cybersecurity issues;
- The input that civil society has into the functioning of the said ministries, policies and organisations; and
- Possible areas for engagement with cybersecurity policy for civil society.

1. http://www.newindianexpress.com/thesundaystandard/2016/oct/16/pak-launches-sneaky-cyber-attack-1528282.html
2. http://www.livemint.com/Industry/ji7zhXV7E8atsU8GHsskDN/RBI-likely-to-tighten-cyber-security-norms.html
3. http://economictimes.indiatimes.com/news/defence/watchdog-detects-39730-cyber-attack-cases-this-year-ravi-shankar-prasad/articleshow/55458837.cms
4. http://www.firstpost.com/business/blow-to-black-money-pm-modi-bans-rs-500-and-rs1000-currency-notes-from-midnight-3095368.htm
5. http://www.cio.in/news/modi%E2%80%99s-currency-ban-cybersecurity-implications-abound>
6. http://www.thehindubusinessline.com/money-and-banking/govt-to-set-up-1000cr-cyber-security-rd-fund/article9258781.ece
7. http://www.vccircle.com/infracircle/ministry-float-request-proposal-national-cyber-coordination-centre/
8. See footnote 2
9. http://www.thehindu.com/business/Centre-unveils-steps-to-boost-cybersecurity/article16442937.ece
10. http://pib.nic.in/newsite/printrelease.aspx?relid=88442>

This report has been prepared as part of an ongoing GPD capacity building process for civil society activists in the global South, as a tool to support interaction with national and regional cybersecurity policy questions. The aim is the promotion of more consultative processes in policy and legislative drafting. The next phase of this project will involve capacity development training in conjunction with partner institutions for local civil society activists, as well as the identification of best practices for long-term and sustainable engagement. This report reflects policy developments announced up till late November 2016.

A. Methodology

This report is based primarily on doctrinal research, following review of available material in the public sphere. This research is informed also by general experience in the field of cybersecurity and engagement with the discourse surrounding the field. It is also important to clarify what 'civil society' refers to in this report. Civil society is a diverse assembly of groups, networks and movements, containing a variety of viewpoints and positions on issues of cybersecurity. Given the complexities involved in defining civil society, this report does not attempt to define it, but generally uses the term to refer to actors or organisations involved in cybersecurity research and policy which are not formally allied to either the government of India or to the technology industry, and which may generally tend to raise rights-based concerns in the law/policy sphere.

01

GOVERNMENT INSTITUTIONS

This chapter focuses on reviewing the most significant ministries, and the organisations operating under them in the field of cybersecurity, as well as the legal and policy framework that primarily governs cybersecurity in India.

A. RELEVANT MINISTRIES

State governments

a. Telangana State Government

The only state government with a specific policy relating to cybersecurity is the Telangana state government. The Telangana cybersecurity policy[1] was released recently, on 15 September 2016[2]. While the policy itself emphasizes co-operation and knowledge sharing with the private sector, the draft policy was not published for public comments. News reports suggest that expert opinions were solicited in the framing of the policy[3], but the process of drafting remains opaque. Some excerpts from the policy referencing engagement with the private sector include:

"... Encourage State-State and inter-institutional partnerships to promote data sharing and collaborative research efforts"

"The State shall collaborate with NALSAR, legal experts in the area of cyber security, The Hague Security Delta, Cyber Cell, TIPCU etc. to study the existing legal frameworks, identify problems and formulate advocacy laws to tackle real-time issues faced by these entities. This collaborative effort will be given the needed impetus to counter the ever evolving nature of cyber threats."

"The government shall set up T-CERT, a nodal agency for the state to coordinate with institutions, organizations and companies... A dedicated officer at the nodal agency shall coordinate with stakeholders and drive the State's efforts."

"The Government shall collaborate with the private sector to provide customized training programs for Police and Government Departments, PSUs, Banks, and other key Industries which are associated with critical infrastructure."

"In addition, the Government will enter into strategic partnerships with the private sector to set up infrastructure such as cyber security training and development labs, which in turn will facilitate the development of new products."

As referenced above, the policy makes it clear that the government is seeking to engage with both private organisations and other governmental institutions.

1. http://www.telangana.gov.in/PDFDocuments/Telangana-Cyber-Security-Policy.PDF"
2. http://www.thehindubusinessline.com/news/national/telangana-releases-four-new-it-policies/article9110907.ece
3. http://www.deccanchronicle.com/nation/current-affairs/290316/telangana-building-cyber-security- framework-official.html

However, no explicit engagement with civil society (as opposed to academic institutions and industry) appears to be sought throughout the policy, and there has been little engagement[4] with the policy by civil society organisations subsequent to its introduction into the public domain. Human rights questions have not been addressed in this policy.

The Telangana government has, however, sought public comments[5] for other ICT-related policies such as the Open Data Policy[6] which was released concurrent to the cybersecurity policy. The Telangana government has also participated in the creation of organisations such as the Society for Cyberabad Security Council ("SCSC")[7]. The SCSC is a joint initiative between the Cyberabad Police Commissionerate and IT industry to promote increased cybersecurity in the Telangana IT industry. The Telangana government has also entered into numerous memoranda of understanding with various private institutions to set up research centres, laboratories and incubators[8].

b. Ministry of Electronics and Information Technology ("MEITY")

This ministry is at the core of cybersecurity operations of the government. It takes an active approach to the development of information technology ("IT"), which it does by seeking to promote innovation in building IT products and otherwise in the information communication technology sector.

The stated mission of MEITY[9] is as below:

"To promote e-Governance for empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT & ITeS industries, enhancing India's role in Internet Governance, adopting a multipronged approach that includes development of human resources, promoting R&D and innovation, enhancing efficiency through digital services and ensuring a secure cyber space."

MEITY has been at the forefront of the development of cybersecurity policies, including the National Cybersecurity Policy of 2013 and the draft Encryption Policy of 2015. These are discussed in more detail in a later segment of the report.

MEITY also works towards building skill-enhancement resources and knowledge centers for cybersecurity activities. These are particularly supported by the National Institute of Electronics and Information Technology ("NIELIT"), an autonomous body under the administrative control of MEITY, set up to assist with education and human resource development. MEITY has also directly engaged with civil society and academic organisations working in the field of IT through grants and joint engagements, although not specifically in relation to cybersecurity.

CERT-IN[10], the nodal agency dealing with cybersecurity in India, is also under the control of MEITY. CERT-In has been designated under Section 70B of Information Technology (Amendment) Act 2008 to serve as the national agency performing the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents;
- Forecast and alerts of cyber security incidents;
- Emergency measures for handling cyber security incidents;
- Coordination of cyber incident response activities; and
- Issuing of guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

While CERT-IN acknowledges academic institutions and the general citizenry of India as stakeholders in its development[11], its public engagements have remained mainly with similar organisations in other countries[12] .

4. https://ccgnludelhi.wordpress.com/2016/09/28/reviewing-telanganas-cybersecurity-framework-part-i-of-ii/
5. http://cis-india.org/openness/comments-on-the-telangana-state-open-data-policy-2016; https://ciipc.wordpress.com/2016/09/28/comments-on-telangana-open-data-policy-2016/
6. https://data.gov.in/sites/default/files/Telangana-Open-Data-Policy-2016.pdf
7. http://cyberabadsecuritycouncil.org
8. http://www.newsnation.in/article/145929-cisco-and-telangana-government-ink-mou.html?COMD
9. http://meity.gov.in/content/vision-mission
10. http://www.cert-in.org.in
11. http://appsit.odisha.gov.in/uploadDocuments/FormNotification/G_S_R%2020%20(E)2.pdf
12. http://www.thehindu.com/business/Industry/certin-signs-cyber-security-pacts-with-3-nations/article8159117.ece; and http://www.vccircle.com/infracircle/indian-computer-emergency-response-team-focusing-partnership-nations/

As referenced above, the Minister for Electronics and Information Technology has recently announced that the central CERT-IN mechanism is to be strengthened, with 26 new posts being sanctioned.[13] Various states, including Maharashtra, Tamil Nadu, Telangana, Kerala and Jharkhand are also seeking to set up state CERTs[14]. Further, in addition to the existing banking sector CERT, it appears likely that additional sectoral CERTs will be created in the power sector[15].

Reports were released in October 2016 that MEITY was expected to shortly issue a request for proposals to set up a National Cybercrime Coordination Centre ("NCCC") to safeguard India's cyberspace against potential threats.[16] When reports were initially released in 2013 of the setting up of the NCCC, the National Information Board ("NIB") had reportedly mandated the Operational Group on Cyber Security to dialogue with stakeholders and share information to prepare a roadmap for operationalising the cyber monitoring agency.[17] However, whether these consultations were carried out remains unclear. The Minister for Electronics and IT has now confirmed that Phase I of the NCCC has been tendered and is expected to be operational by March 2017. A budget of INR 985 crore has been allocated for this project over a period of five years.[18]

c. Ministry of External Affairs ("MEA")

The MEA[19] is responsible for coordinating with other governments on matters of foreign policy. Representatives from the MEA are also responsible for negotiating the signing of treaties and conventions on internet-related issues. In recent years, several bilateral and multilateral engagements have discussed the issue of cybersecurity. Some notable recent understandings have been reached (through CERT-IN) with Singapore [20], the UK[21] , Korea, Canada, Australia, Malaysia, Singapore, Japan and Uzbekistan. The MEA has also signed a memorandum of understanding setting out cybersecurity as an area of cooperation with the Shanghai Cooperation Organization. However, civil society engagement with these processes has remained limited, and the agreements entered into are generally not available in the public domain.

d. Ministry of Home Affairs ("MHA")

The MHA[22] is in charge of internal security in the country. The Ministry oversees a number of intelligence gathering and coordinating units in charge of internal security. Because of its role in intelligence-gathering, this ministry has traditionally remained relatively opaque in terms of its functioning, with its agencies typically operating outside of statutory frameworks.

In an answer given in the Lok Sabha earlier this year[23], the Minister for Home Affairs noted that the MHA would be responsible for framing policies related to classification, handling and security of information relating to the Government in consultation with other stakeholders, and the monitoring of its implementation. In relation to this, the National Information Security Policy Guidelines ("NISPG") were issued by the MHA in the month of July 2014 to various Ministries and Departments for implementation. However, these guidelines do not appear to have been released into the public domain.

News reports also suggest that permission for the formulation of an independent cybersecurity architecture under the Intelligence Bureau has been given in order to combat the rise of online radicalisation[24]. It remains unclear whether such an architecture has actually been formulated.

The MHA has previously solicited presentations from organisations and parties working in the cybercrime and security domain[25]. These presentations were

13. See footnote 9
14. See footnote 9
15. See footnote 9
16. See footnote 9
17. http://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article8327987.ece
18. http://www.news18.com/news/tech/government-is-preparing-for-cyber-war-ravi-shankar-prasad-1311376.html
19. https://www.mea.gov.in/
20. http://www.mea.gov.in/bilateral-documents.htm?dtl/26061/List+of+AgreementsMoUs+signed+during+the+visit+of+Prime+Minister+to+Singapore
21. http://pib.nic.in/newsite/PrintRelease.aspx?relid=149372
22. http://mha.nic.in/
23. http://mha1.nic.in/par2013/par2016-pdfs/ls-010316/830.pdf
24. http://indianexpress.com/article/india/india-others/mha-nod-for-cyber-security-wing-under-ib
25. http://mha.nic.in/sites/upload_files/mha/files/CyberCrimePresentation_060416.pdf

requested to showcase the abilities of the organisations in respect of cybercrime, with an especial focus on issues relating to crimes against women and children. This indicates that engagement with private society organisations is sought in certain situations.

e. Ministry of Defence ("MOD")[26]

The MOD is the ministry that has traditionally been responsible for national security, with its role consisting primarily of the collection of signals intelligence and external intelligence. Its role in the defence of cyberspace is evolving, with it playing a major role in research on cybersecurity. Both the Institute for Defence Studies and Analysis ("IDSA"), as well as the Defence Research and Development Organisation ("DRDO") are engaged in research in the field of national security in cyberspace.

IDSA[27]

IDSA is an autonomous body funded by the MOD which conducts research on the 'problems of national security and the impact of defence measures on the economic, security and social life of the country'. It brings out a monthly publication called 'Strategic Analysis' which contains research articles on international political, strategic and security issues. IDSA has previously recommended public-private partnerships for information security in identified sectors dependent on the use of IT.[28] The IDSA in its research has also sought assistance from experts from the private sector in arriving at recommendations. [29]

DRDO[30]

DRDO is a network of more than 50 laboratories engaged in developing defence technologies covering various disciplines, including aeronautics, armaments, electronics, combat vehicles, engineering systems, instrumentation, missiles, advanced computing and simulation, special materials, naval systems, life sciences, training, information systems and agriculture. The DRDO is seeking to set up several 'Technology Development Research Centers' for research in the field of cybersecurity across India, in partnership with major educational institutions.[31]

f. Prime Minister's Office ("PMO")

The office of the Prime Minister includes various agencies and advisors important to the Prime Minister. Given the increasing focus on cybersecurity in national and international contexts, the office of the National Cybersecurity Coordinator was created by the current government in 2015.[32] Dr Gulshan Rai, who was previously heading CERT-IN, was elevated to this post. Dr Rai has previously stressed the need for stakeholder collaboration for risk mitigation. [33]

National Cyber Security Research Fund[34]

It was recently announced that in the wake of increasing threats in cyberspace, an INR 1,000 crore fund will be set up to look into research and development for cybersecurity products and systems. This fund has already been approved by the Cabinet Committee on Security and is to be administered by a high-powered committee chaired by the National Security Advisor ("NSA"), Mr Ajit Doval, who reports to the PMO. This fund will reportedly be open to academia and industry, depending on the research expertise required for specific projects.

The other committee members responsible for administering the fund will include the deputy NSA, representative of the principal scientific adviser, the CEO of Niti Aayog, the Chairman of the National Technical Research Organisation, the Director General of DRDO, the National Cyber Security Coordinator, and the secretaries of departments of

26. http://www.mod.nic.in
27. http://www.idsa.in
28. http://www.idsa.in/system/files/book/book_indiacybersecurity.pdf
29. Ibid.
30. http://www.drdo.gov.in/drdo/English/index.jsp?pg=homebody.jsp
31. http://economictimes.indiatimes.com/news/defence/drdo-gtu-to-set-up-cyber-security-centre/articleshow/47141932.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
32. http://economictimes.indiatimes.com/news/politics-and-nation/gulshan-rai-becomes-first-chief-of-cyber-security-post-created-to-tackle-growing-e-threats/articleshow/46449780.cms
33. http://www.cii.in/PressreleasesDetail.aspx?enc=ECFHZjGsSx/3QOLn7WspZqcCC8uIN1YGBdy7Hfp1h8kHuZOHbxYN7DwiLw0m9gHVsvNZxW8S7T4DjI2DxL8gKQ==>n
34. http://indianexpress.com/article/india/india-news-india/cyber-security-nsa-administered-rs-1000-cr-fund-kept-open-to-private-players-3740699

Home, IT, telecom, science and technology, atomic energy and expenditure.

National Critical Information Infrastructure Protection Centre ("NCIIPC")

Section 70A of IT Amendment Act 2008 mandated the creation of a national nodal agency in respect of critical information infrastructure ("CII") protection.[35] This agency, being the NCIIPC, was finally created through gazette notification dated January 16, 2014[36] and placed under the control of the National Technical Research Organisation ("NTRO") under the PMO. The stated mission of the NCIIPC is "to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders".[37] However, where the draft framework for the protection of CII[38] acknowledges the role of stakeholders, they are listed as follows:

- The CII owner
- Service providers to the CII
- NCIIPC
- CERT-IN
- Law enforcement agencies

This makes it clear that the understanding of stakeholders in terms of CII may not include civil society or even academic or industry bodies.

B. LEGISLATIVE FRAMEWORK

a. The Information Technology Act, 2000 ("IT Act") (as amended up to date) and rules thereunder

The IT Act is the primary legislation dealing with technology and cybersecurity in India. The Central Government is empowered to make rules relating to a number of issues under the Act, as specified under Section 87, and state governments are empowered to make rules on issues specified under Section 90. There are limited substantive provisions under the IT Act relating to cybersecurity, but some important institutions dealing with cybersecurity have been set up under the Act (as discussed above).

A draft amendment act to the IT Act was circulated in 2008, which was criticised on several grounds, including the violation of civil liberties[39]. The committee which prepared the draft amendment act included Shri Kiran Karnik, President NASSCOM; Legal Experts Shri Vakul Sharma and Shri A.K. Singh, Advocates; IT Industry representatives Shri Ajay Chaudhry, Chairman, HCL Infosystems Ltd., Shri R. Ramaraj, MD and CEO, Sify Ltd. and Shri Ajit Balakrishnan, CEO, Rediff India Ltd.; Dr. A.K. Chakravarti, Adviser, DIT and Shri Antony De Sa, Joint Secretary, Ministry of Commerce and Industry. Shri M.M. Nambiar, Additional Secretary, Department of Information Technology was Member Secretary of this Committee[40]. It can be seen from this that although input from technical, governmental, and industry experts was solicited, civil society was not involved in the preparation of the draft amendment act. [41]

Despite extensive public feedback, civil society commentary on the draft amendment act was not taken significantly into account, and the IT Amendment Act of 2008 was passed. This included cybersecurity related provisions such as Section 70A, which permitted the Central Government to designate any agency as the nodal agency for CII protection, and which led to the creation of CERT-IN.

It has recently been reported that the IT Act will once again be re-evaluated

35. https://ccgnludelhi.wordpress.com/2016/11/11/protecting-critical-information-infrastructures-in-india
36. https://nciipc.gov.in/bitstream/document/46/1/Gazette%20Notification.pdf
37. https://nciipc.gov.in/?p=vision
38. https://nciipc.gov.in/bitstream/document/141/1/Draft%20NCIIPC%20Framework%20for%20Protection%20of%20CII.pdf
39. http://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008
40. deity.gov.in/hindi/sites/upload_files/dithindi/files/documents/PressRelease.doc
41. http://cis-india.org/internet-governance/blog/cyber-regulations-advisory-committee-no-civil-society

for significant amendments.[42] It is to be hoped that these amendments will be undertaken only once a full-fledged consultation process takes place.

Rules framed under the IT Act

In addition to the genesis of the IT Act itself, the process of creation of rules under the Act has been highly contentious and has attracted significant critique for being opaque and insufficiently consultative. The possibility of non-governmental engagement with the drafting process under the IT Act comes from Section 88 of the IT Act, which mandates the constitution of an advisory committee called the Cyber Regulations Advisory Committee. ("CRAC"). The section provides that the CRAC is to consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit. The CRAC is also to advise the Central Government or the Controller either generally as regards any rules or for any other purpose connected with the IT Act.

The CRAC was constituted in 2001, but after two meetings, remained dormant for over a decade. Further, the 22-member CRAC included no representatives from civil society. Following public demand, the CRAC was reconstituted in 2012, but despite claims to the contrary, it continued to include no civil society representation. The Lok Sabha's committee on subordinate legislation said this about the CRAC in 2013: "It is not clear... whether, in the reconstituted CRAC, there are members representing the interests of principally affected or having special knowledge of the subject matter as expressly stipulated in Section 88(2) of the IT Act."[43]

CRAC had a meeting in September 2014 wherein it described itself as constituted by "members from all sections of the Society, including Government, Industry, Civil Society and Academy". However, there appear to be no such members, unless civil society can be considered to be represented by the Computer Society of India, which is a technical body. The impact of this failure to consult civil society or academia can be seen in the fact that there is very limited consideration of human rights questions in the work of the committee, including in terms of the impact of blocking content and other questions.[44]

C. POLICY FRAMEWORK

a. 12th Five Year Plan - Report of sub-group on Cybersecurity

The 12th FYP Report on Cybersecurity[45] is amongst the most civil-society friendly policy guidelines on the subject of cybersecurity, mentioning improving interaction and engagement with stakeholders including academia and non-governmental organisations as a target aim. The Report also discusses the establishment of a think tank for cybersecurity policy inputs, discussion and deliberations. Although this document is not binding, it indicates an encouraging willingness to engage with civil society and other stakeholders on the subject of cybersecurity.

b. The National Cyber Security Policy 2013

The National Cyber Security Policy was first released in discussion draft form in early 2011[46], with public comments solicited until 15 May 2011. However, no civil society inputs into this policy appear to be available in the public domain – this may be because few policy and research organisations were active in the space of cybersecurity in 2011. While several government/industry/academic/civil society bodies such as IDSA[47] , the Centre for Communication Governance[48], the Centre for Internet and Society[49] and DSCI[50] post-facto have reviewed the policy, and have generally commended it, it remains vague in terms of details on how its stated goal of public-private participation is to be achieved, and it includes no specific references to the protection of civil liberties or engagement with civil society. It has

42. http://economictimes.indiatimes.com/small-biz/legal/if-all-goes-well-indian-it-act-may-enter-21st-century/articleshow/54707994.cms
43. http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf
44. http://scroll.in/article/703746/blocking-online-porn-who-should-make-constitutional-decisions-about-freedom-of-speech
45. http://meity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf
46. http://meity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf
47. http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813
48. https://thefsiindia.wordpress.com/2013/07/13/indias-national-cyber-security-policy-preliminary-comments
49. http://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review
50. https://www.dsci.in/node/1051

been pointed out that the scope of the policy is generally ambiguous, and contains the possibility of overreach in terms of the maintenance of privacy rights and other human rights[51]. It has also been noted that despite the policy being over three years old, operationalization has been relatively slow. [52]

c. The Draft Encryption Policy 2015 (Withdrawn)

Section 84A of the IT Act allows the government to prescribe encryption standards as follows:

"84A. The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption."

A draft national encryption policy[53] was released in September 2015 for public comments, and was withdrawn two days later following public outrage regarding its draconian provisions[54] . These included governmental access to all encrypted information, including personal emails, messages or even data stored on a private business server, and a requirement for users to store all encrypted communication for at least 90 days. Any encryption keys were also to be handed over to the government.

The government, in withdrawing the impugned draft, acknowledged the role of public sentiment[55] and has sought to rework the draft. It is likely that a redrafted encryption policy will be released to the public shortly, which will probably have a multistakeholder focus.[56] The DSCI has formed an advisory group on encryption policy to discuss encryption issues and is engaging with the government to formulate the policy. However, the DSCI group is comprised entirely of industry members.[57]

d. The Reserve Bank of India ("RBI") notification relating to the Cyber Security Framework in Banks and the Securities and Exchange Board of India ("SEBI") policy on Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories

Both the RBI[58] and the SEBI[59] have recently released policies relating to cybersecurity requirements for the bodies governed by them (i.e. banks, and stock exchanges, clearing corporations and depositories respectively). However, neither of these policies were released for public consultation, and make no reference to stakeholder participation. Given the specialized nature of the tasks carried out by both the RBI and SEBI, and the fact they primarily govern companies rather than individuals, this may be appropriate. Both the RBI[60] and the SEBI[61] have declared their intention to revise the above-mentioned policies, but in public statements, it appears likely that the consultation process will involve only industry representatives.

51. See footnote 48
52. http://www.governancenow.com/gov-next/egov/cyber-security-ministry-of-electronics-it-cyber-space-deity-digital-india-egovernance
53. http://www.thehindu.com/news/national/govt-to-withdraw-draft-encryption-policy/article7677348.ece
54. http://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore/
55. http://meity.gov.in/sites/upload_files/dit/files/Encryption%20Policy_govt.pdf
56. http://economictimes.indiatimes.com/news/defence/terrorist-groups-use-internet-as-their-main-tool/articleshow/54601987.cms
57. https://www.dsci.in/taxonomypage/602
58. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF
59. http://www.sebi.gov.in/cms/sebi_data/attachdocs/1436179654531.pdf
60. http://www.livemint.com/Industry/ji7zhXV7E8atsU8GHsskDN/RBI-likely-to-tighten-cyber-security-norms.html
61. http://www.business-standard.com/article/markets/sebi-steps-up-effort-to-tackle-cyber-

02

NON-GOVERNMENTAL STAKEHOLDERS

The Indian policy space has historically been driven by bureaucrats, similar to the UK system.[1] Until recently, there was little room for non-governmental stakeholders to engage on security issues.[2] However, this is changing with an increasing number of non-governmental bodies playing a role in shaping India's security policy.[3] As discussed below, many security think tanks also engage on cybersecurity issues.

This section will review the various significant non-governmental stakeholders currently working with issues relating to cybersecurity policy. It will also set out their engagement with issues relating to cybersecurity. They are broadly classified under four heads viz., industry or industry supported bodies, civil society organizations, think tanks and academia.

A. INDUSTRY ORGANISATIONS

a. Data Security Council of India ("DSCI")

DSCI is a company which works on data protection in India,[4] set up by the National Association of Software and Services Companies ("NASSCOM"). Their primary focus is on issues of privacy and cybersecurity.[5] On both issues, DSCI develops best practices and frameworks, publishes studies, surveys and papers.[6] The DSCI has been conducting an annual Information Security summit in conjunction with NASSCOM for more than a decade, the next iteration of which is in December at New Delhi.[7] DSCI has also recently opened its first international chapter in Singapore, with the aim of encouraging information exchange, knowledge development, and the creation of best practices in cybersecurity.[8]

b. NASSCOM - Cyber Security Task Force

NASSCOM recently established a separate dedicated cybersecurity task force[9] in collaboration with DSCI.[10] It is aimed at building technical expertise in cybersecurity issues and will look to set up hubs to train cybersecurity professionals. The task force consists of four working groups, one of which focuses on policy development.[11]

c. Federation of Indian Chambers of Commerce and Industry ("FICCI")

FICCI is an industry body representing the interests of Indian businesses across sectors.[12] Their Information Technology sector works on some cyber security issues. A recent FICCI survey highlighted information security risks faced by Indian

1. http://www.hindustantimes.com/india/india-s-most-influential-think-tanks/story-emb0db2lmqltL8pKeYuZiL.html
2. Ibid.
3. Ibid.
4. https://www.dsci.in/about-us
5. Ibid.
6. Ibid.
7. http://www.dsci.in/AISS2016/
8. https://www.dsci.in/content/data-security-council-india-dsci-launches-its-first-global-chapter-singapore
9. http://www.nasscom.in/nasscom-setsup-cyber-security-task-force-build-india-cyber-security-hub
10. https://www.dsci.in/taxonomypage/1182
11. Ibid.
12. http://ficci.in/ficci-in-news-page.asp?nid=11403

16

companies.[13]

d. Associated Chambers of Commerce & Industry of India ("ASSOCHAM")

ASSOCHAM is an industry group that focuses on, among other things, the Information Technology (IT) sector. It organizes an annual summit on Cyber & Network Security.[14]

B. CIVIL SOCIETY ORGANISATIONS

a. Centre for Internet and Society ("CIS")

The Centre for Internet and Society is a non-profit organization which undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives.[15] Their areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cybersecurity.[16] CIS has produced analysis on cybersecurity issues and organized events centered around cybersecurity in the past.[17] CIS also currently appears to be seeking to add to its cybersecurity team.[18]

b. Software Freedom Law Centre- India ("SFLC")

SFLC is a donor supported legal services organization that seeks to protect freedom in the digital world.[19] SFLC is organised as a society registered under the Societies Registration Act, 1860.[20] SFLC's current projects include online freedom, privacy, internet governance, patents and development of the right to information.[21]

c. Internet Democracy Project ("IDP")

The Internet Democracy Project is an initiative of Point of View.[22] IDP's work focuses on understanding the linkages between the internet and the nature of democracy.[23] IDP works on issues relating to internet governance, cybersecurity and freedom of expression and recently published a map of the various government agencies that regulate cybersecurity in India.[24]

C. THINK TANKS

a. Observer Research Foundation ("ORF")

ORF is a public policy think tank started in Delhi in 1990.[25] ORF's research is spread across six different themes, with a dedicated cybersecurity and internet governance initiative.[26] Their flagship internet conference CyFy is held in October every year.[27] They have produced reports on a number of internet related issues, ranging from the digital economy to internet governance and cybersecurity.[28]

b. Vivekananda International Foundation ("VIF")

VIF is a think tank that works on a number of different issues across six centres.[29] Their centre on National Security and Strategic Studies also works on cybersecurity issues.[30]

c. Ananta Aspen Centre ("AAC")

AAC works on public policy and international relations issues.[31] They have organized

1. 13

13. http://ficci.in/ficci-in-news-page.asp?nid=11403
14. http://www.assocham.org/eventdetail.php?id=1278
15. http://cis-india.org/
16. Ibid
17. http://cis-india.org/internet-governance/blog/cis-cybersecurity-series-part-1-christopher-soghoian
18. http://cis-india.org/jobs/policy-officer-cyber-security
19. http://sflc.in/about-us/
20. Ibid
21. http://sflc.in/our-projects/
22. https://internetdemocracy.in/about/
23. Ibid
24. https://internetdemocracy.in/2016/03/an-interactive-map-of-cybersecurity-institutions-in-the-government-of-india/
25. http://www.orfonline.org/about-us/
26. http://www.orfonline.org/programme/cyber-media/cyber-security-internet-governance/
27. http://www.orfonline.org/cyfy/
28. http://appsit.odisha.gov.in/uploadDocuments/FormNotification/G_S_R%2020%20(E)2.pdf
29. http://www.vifindia.org/AboutUs1
30. http://www.vifindia.org/articles/cybersecurity
31. http://anantaaspencentre.in/about_us.aspx

Track II dialogues including the recent India-US Strategic Dialogue.[32]

d. The India Foundation

The India Foundation works on a range of domestic policy issues.[33] Their Centre for Security and Strategic Studies works on national security issues, including cybersecurity.[34] They have also held events on national security issues.[35]

e. Synergia Foundation

Synergia Foundation is a policy think tank and a consultancy organization.[36] They have worked on cybersecurity, among other issues. They organized a conference on cybersecurity, entitled Cyber 360 in 2015, which brought together experts from around the world.[37]

D. ACADEMIA

Non-Technical Academia

a. Centre for Communication Governance, National Law University Delhi ("CCG NLU-D")

CCG NLU-D is a research centre within the National Law University at Delhi.[38] The aim of the Centre is to ensure that the Indian legal education establishment engages more meaningfully with communication law and policy.[39] It does this through three verticals, being civil liberties, global internet governance, and the recently launched vertical on cybersecurity.

b. The Institute of Global Internet Governance and Advocacy ("GIGA")

GIGA has been established as a centre for research, advocacy and training on global internet governance at the NALSAR University of Law, Hyderabad.[40] The Centre aims to develop as an academic think tank to research issues relating to internet governance and its interface with national legislations.[41]

Technical Academia

c. Cybersecurity Education and Research Centre, ("CERC") Indraprastha Institute of Information Technology

CERC aims to build capacity and increase awareness of cybersecurity issues. [42] It also aims to create cybersecurity professionals.[43] Their focus is on issues such as privacy, secure coding, critical infrastructure among others.[44]

d. Centre of Excellence in Cyber Systems and Information Assurance ("CSIA"), Indian Institute of Technology, Delhi

Like the CERC, the CSIA's focus is on raising awareness and providing training on Information Assurance.[45] They also develop short term courses for industry, government and academia on cybersecurity and information assurance.[46]

In addition to the above, there are several organisations that work primarily or at an ancillary level with technology law and policy, as well as cybersecurity. While some of the major players are listed above, there are several new entities entering the field every day, such as Microsoft's recently launched Cyber Security Engagement Centre at Delhi[47] . There are also several academic and industry bodies that work in the field or allied technical areas, such as the Institute for Information Security at Mumbai[48], and the Cellular Operators Association of India ("COAI")[49].

32. http://anantaaspencentre.in/track_II_dialogue.aspx
33. http://www.indiafoundation.in/who-we-are
34. http://www.indiafoundation.in/our-centres
35. http://www.indiafoundation.in/event-reports
36. http://www.synergiafoundation.in/home
37. http://synergiaconclave.synergiafoundation.in/
38. http://ccgdelhi.org/
39. Ibid
40. http://thegiga.in/Home.aspx
41. Ibid
42. http://cerc.iiitd.ac.in/
43. Ibid
44. Ibid
45. http://csia.iitd.ac.in/
46. http://csia.iitd.ac.in/index.php/research/about
47. https://news.microsoft.com/en-in/microsoft-increases-cybersecurity-investments-in-india/#sm.0005zvkvo1avled2zmm2g115uiwbe
48. http://www.iisecurity.in
49. http://www.coai.com/

03

MAPPING UPCOMING OPPORTUNITIES

This section will review various action areas that are gaining traction and appear to be amenable to civil society input. This section will cover two major focus points for civil society organisations seeking to work with cybersecurity, i.e. the potential sites for engagement as well as methods of engagement.

While the section on potential sites for engagement primarily focuses on specific processes and policies which are likely to commence shortly, it must be noted that non-governmental actors also have important roles to play in proactively building conversations around cybersecurity including through the development and dissemination of healthy practices and identifying areas that require policy intervention.

A. SITES FOR ENGAGEMENT

There are several processes relating to cybersecurity or technology generally which are likely to begin shortly and which may be useful for civil society to engage with. However, there is limited clarity around specific dates and inputs which are likely to be solicited for these processes, as well as the actors from whom assistance may be sought.

a. Amendments to the IT Act

As discussed above, the IT Act is likely to be amended again. While it is not legally necessary that the draft be released to the public for commentary, given past precedent, it is likely. This may be a good opportunity to make substantive suggestions around the main legislation governing cybersecurity in India.

b. Draft Encryption Policy

MEITY has recently written to several industry associations including COAI, Association of Unified Telecom Service Providers of India ("AUSPI"), and Internet Service Providers Association of India ("ISPAI") seeking their opinions and inputs that on a "robust and secure" encryption policy. However, according to various news reports, these associations have asked the government to release a white paper on the topic, which will likely be released for public consultation. [1]

c. State Cybersecurity and IT Policies

Various state governments (including Karnataka, Haryana, Telangana and Andhra

1. http://economictimes.indiatimes.com/news/economy/policy/it-ministry-revises-work-on-encryption-policy-seeks-industry-views/articleshow/53475867.cm

Pradesh) have recently significantly enhanced their budgets in relation to cybersecurity. Telangana has already released its cybersecurity policy, but is awaiting the release of other policies in relation to the Internet of Things and Smart Cities, which also have strong relevance to questions of cybersecurity. As and when drafts of these policies are released, it may be useful to examine them to understand the processes discussed.

d. NCCC

As discussed above, the tendering process for the NCCC has begun and the first phase of the project is likely to begin by March 2017. The NCCC will remain under the control of MEITY, which has traditionally been one of the more amenable ministries to public input. It may thus be useful to work on areas which the NCCC is likely to cover.

e. Draft NCIIPC Framework

The draft NCIIPC framework has been available in the public domain for consultations for a significant period of time, and has not yet been finally notified.[2] This framework would form the policy basis for the protection of Critical Information Infrastructure in the country, and any inputs to this may be useful.

f. National Cyber Security Research Fund

As discussed above, the National Cyber Security Research Fund has explicitly been kept open to private participation. When more details become available, this may form an important site for academia to both seek funding as well as engage with government organisations on research questions.

g. International processes

India is an active participant in several international processes relating to cybersecurity. Although inter-state MOUs are generally under strict governmental control, engagement with research groups like the UN Group of Governmental Experts ("UN GGE") is not necessarily so, and it may be possible to engage with representatives appearing on behalf of India at such forums.

2. https://nciipc.gov.in/bitstream/document/141/1/Draft%20NCIIPC%20Framework%20for%20Protection%20of%20CII.pdf

04

MEANS OF ENGAGEMENT

In addition to formal processes of engagement with public policy, there are several ways to create spaces for intervention in the law and regulation sphere of cybersecurity. Some of these are as listed below.

a. Public consultation

This is the most direct and targeted form of intervention, but remains dependent on whether laws, policies and delegated legislation are opened to public comments prior to finalization. India does not have an overarching law on the subject, and the IT Act is also silent on the topic. It thus remains discretionary whether stakeholder consultation is carried out prior to the formulation of rules and regulations.

b. Academic advisory

Post-facto review of legislations and policy, as well as independent academic writing (which may be targeted at policymakers or otherwise) can play an important role in formulating public thought and consensus on topics in respect of complex issues.

c. Advisory committees

As discussed above, relatively few formal advisory bodies look to engage with civil society, but tend to gravitate towards industry organisations instead. However, offering to provide expertise on issues flagged in various governmental policies, along with tracking calls for information, may provide a method for direct discussion on important topics.

d. Public events

Civil society organisations may look to create dialogue around important cybersecurity issues by conducting conferences, symposiums, roundtable discussions and independent panels.

e. Judicial challenge

In cases of legislation that is violative of human rights, it may be imperative to challenge the same via the judicial system. Courts are generally given the power of review over legislation and delegated legislation, and especially in cases of violation of fundamental rights, civil society organisations may seek to file litigations in the public interest. With respect to technology law, the most significant example of a

successful judicial intervention is probably the case of Shreya Singhal v. UOI[1], which led (among other things) to Section 66A of the IT Act being struck down.

f. Media engagement

Similar to academic advisory but with greater reach, civil society organisations can influence policy by creating innovative strategies to formulate public opinion on topics, including through social media campaigns, writing for large newspaper/ magazine publications, appearing on televised discussions etc. An important example of the success of this was the discussion around net neutrality.[2]

g. Technological innovation

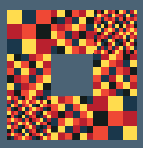
In order to keep pace with changing technology, laws dealing with cybersecurity must be flexible and able to encompass innovation. In several cases however, it may be even more important to develop technological solutions to cybersecurity issues, which is an area civil society organisations with the requisite technical experience may be able to deal with.

1. http://indianexpress.com/article/opinion/columns/speaking-for-freedom/
2. http://www.thehindu.com/opinion/op-ed/on-multistakeholder-governance-of-the-internet/article7440857.ece

CONCLUSIONS

The cybersecurity field in India is gaining traction, with increasing governmental attention and budgetary allocations and participation in both international and domestic forums. As can be seen above, from a policy standpoint, there is theoretical support for non-governmental engagement on cybersecurity issues. However, this engagement appears to be mainly targeted towards industry bodies rather than civil society. Equally, the types of organisations which solicit inputs are limited to those which discuss "civilian" cybercrime, rather than cyberattacks, cyberterrorism and cyberwarfare. This is possibly a legacy from the very recent shift from a multilateral mode of internet governance to a more inclusive, multistakeholder model, coupled with significant national security concerns.

In mapping the cybersecurity field in India with the aim of identifying policy processes that are amenable to engagement, it becomes clear that there is limited information regarding various processes, and how likely they are to seek inputs. Given this, a valuable starting point might be creating spaces where interaction can take place, identifying issues where there might be points of accord with government agencies or where civil society can contribute research and other expertise, or building capacity to enable civil society to engage most effectively with various processes. It is hoped that with increasing civil society engagement in the field, attitudes towards civil society participation in cybersecurity processes will become more accepting.



GLOBAL PARTNERS DIGITAL

Human rights in a connected world

GLOBAL PARTNERS DIGITAL
Second Home
68 - 80 Hanbury Street
London E1 5JL
+44 (0)20 3 818 3258
gp-digital.org