Regulating the Internet: The Government of India & Standards Development at the IETF

November 29, 2018 (updated on December 17, 2018)

By **Aayush Rathi**, **Gurshabad Grover** and **Sunil Abraham**

The Centre for Internet and Society, India

The authors would like to thank **Elonnai Hickok**, **Mallory Knodel**, **Swaraj Barooah**, and **Vidushi Marda** for their thoughtful feedback. The report may not reflect their opinion(s) on the subject matter. All errors are, of course, entirely the authors'.

Executive Summary

The institution of open standards has been described as a formidable regulatory regime governing the Internet. As the Internet has moved to facilitate commerce and communication, governments and corporations find greater incentives to participate and influence the decisions of independent standards development organisations.

While most such bodies have attempted to systematise fair and transparent processes, this brief highlights how they may still be susceptible to compromise. Documented instances of large private companies like Microsoft, and governmental instrumentalities like the US National Security Agency (NSA) exerting disproportionate influence over certain technical standards further the case for increased Indian participation.

The debate around Transport Layer Security (TLS) 1.3 at the Internet Engineering Task Force (IETF) forms an important case for studying how a standards body responded to political developments, and how the Government of India participated in the ensuing discussions. Lasting four years, the debate ended in favour of greater communications security. One of the security improvements in TLS 1.3 over its predecessor is that is makes less information available to networking middleboxes. Considering that Indian intelligence agencies and government departments have expressed fears of foreign-manufactured networking equipment being used by foreign intelligence to eavesdrop on Indian networks, the development is potentially favourable for the security of Indian communication in general, and the security of military and intelligence systems in particular. India has historically procured most networking equipment from foreign manufacturers. While there have been calls for indigenised production of such equipment, achieving these objectives will necessarily be a gradual process. Participating in technical standards can, then, be an effective interim method for intelligence agencies, defence wings and law enforcement for establishing trust in critical networking infrastructure sourced from foreign enterprises.

Outlining some of the existing measures the Indian government has put in place to build capacity for and participate in standard setting, this brief highlights that while these are useful starting points, they need to be harmonised and strengthened to be more fruitful. Given the regulatory and domestic policy implications that technical standards can have, there is a need for Indian governmental agencies to focus adequate resources geared towards achieving favourable outcomes at standards development fora.

Background: Significance of Standards Development Organisations (SDOs)

The Internet's emergence and development has concomitantly been accompanied by debates around its regulatory status. After an initial enthusiasm for cyberspace independence through self-governance[1] (what has also been called "cyberanarchy"[2]), there has been a growing consensus in legal academic literature that governmental policies and regulation will be critical to determining the future of the Internet.[3] While the idea that cyberspace should be self-governing has generated a lot of scholarship[4] and guided regulation of electronic commerce[5], the realm of cyberspace is not immune to influence from state institutions and law. For instance, the possession and ownership of the Internet's physical infrastructure is governed by property rights, and Internet users are governed by the law of territorial states.[6]

However, in the absence of conventional 'command and control' forms of government regulation over cyberspace, a rich matrix of private ordering in the shape of regimes of customary norms has pervaded. These norms take varied forms, ranging from website terms of use, which have their basis in contract law, to code embedded in digital media[7], all of which dictate how online interactions are conducted. These norms, thus, have a similar effect to what is usually intended by conventional state-enacted law.[8] Within this matrix of private organisation of cyberspace norms, a critical role has been played by standards development organisations (SDOs) and their institution of open and interoperable standards.

---

[1] John Perry Barlow (1996), "A Declaration of the Independence of Cyberspace", Electronic Frontier Foundation, <**https://www.eff.org/cyberspace-independence**>

[2] Neil Weinstock Netanel (2000), "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory", 88 Calif. L. Rev. 395

[3] *For emerging consensus, see* Jack L. Goldsmith (1998), "Against Cyberanarchy", 65 U. CHI. L. Rev. 1199; Philip J. *See also* Weiser ", Internet Governance, Standard Setting, and Self-Regulation", 28N. Ky. L. Rev. 822 (2001), <**http://scholar.law.colorado.edu/articles/588**>

[4] *See* David R. Johnson & David Post (1996), "Law and Borders - The Rise of Law in Cyberspace", 48 STAN. L. Rev. 1367; Llewellyn Joseph Gibbons (1997), "No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace", 6 CORNELL J.L. & PUB. POL'Y 475l Vincent Mosco (2005), "The Digital Sublime: Myth Power and Cyberspace", The MIT Press; Jack Goldsmith (2007), "Who Controls the Internet? Illusions of a Borderless World", Strategic Direction, Vol. 23 Issue: 11

[5] The White House (1997), "Memorandum for the heads of the executive departments and agencies, Subject: Electronic Commerce", Office of the Press Secretary, <**https://fas.org/irp/offdocs/pdd-nec-ec.htm**>

[6] Margaret Jane Radin & R. Polk Wagner (1998), "The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace", 73 CHI-KENT L. Rev. 1295

[7] *See generally* Lawrence Lessig (1997), "Reading the Constitution in Cyberspace", 45 Emory L.J. 869; Lawrence Lessig (1997), "The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation", 5 CommLaw Conspectus 181

[8] *On norms as "law", see* Lawrence Lessig (1996), "Social Meaning and Social Norms", 144 U. PA. L. Rev. 2181

Independence of standards development organisations

The institution of open standards has been a formidable regulatory regime that has governed the Internet while facilitating its growth as network of networks.[9] While most SDOs developing open standards have systematised transparent processes for the development and setting of standards, the ensuing discussion highlights how they may still be susceptible to compromise.

Until 1995, before the Internet became a platform for exacting commerce as well as an additional modality for exerting extra-territorial influence, the job of private SDOs was simpler. They could focus on debating the technical strengths of proposed standards without having to weigh in the motives of the increasing diversity of stakeholders with vested interests in the future of the Internet.[10, 11] This transformation of the Internet, from a public "commons"[12] to a site of competing commercial and geopolitical interests, thus, poses challenges to both SDOs as well as governments, especially in cases where a minority of interests may have disproportionate influence over open standards.

Take, for instance, the case of the adoption of Microsoft's Office Open XML (OOXML) format as a standard by the International Organization for Standardization (ISO). Microsoft successfully got the OOXML file format fast-tracked through the ISO despite the open standard ODF (Open Document Format) already having been granted ISO accreditation earlier. This brought about widespread allegations against Microsoft of heavy-handed tactics adopted for influencing national standard setting bodies: Microsoft's attempts in several countries[13, 14] at "interfering with the governance process of sovereign countries"[15] in order to compromise the SDO, were reported. The Bureau of Indian Standards (BIS) was caught in the crossfire[16] owing to the BIS' LITD15 committee's decision to vote against OOXML at the ISO.[17] A majority of the BIS LITD15 committee's concerns concerned free access to the the proprietary binary formats, Microsoft patents on the format, and OOXML's incompatibility with the ISO-approved ODF. However, the

---

[9] Philip J. Weiser, (2001), "Internet Governance, Standard Setting and Self-Regulation", 28 N. Ky. L. Rev. 822

[10] Philip J. Weiser, (2009), "The Future of Internet Regulation", 43 U.C. Davis L. Rev. 529, <http://scholar.law.colorado.edu/articles/263>

[11] Lawrence Lessig, Open Code and Open Societies: Values of Internet Governance, 74 CHI. KENT L. REV. 1405, 1411 (1999)

[12] Supra, 9.

[13] Kai Puolamäki (2007), "Corrupt countries were more likely to support the OOXML document format", Electronic Frontier Finland, <https://effi.org/blog/kai-2007-09-05.en.html>

[14] *For instances of continued pressure from Microsoft on public servants in the domain of open standards*, see Bryan Glick (2014), "Microsoft threatened MPs over open-standards policy, claims advisor", Computer Weekly, <https://www.computerweekly.com/news/2240233813/Microsoft-threatened-MPs-over-government-open-standards-policy-claims-advisor>

[15] Deepak Pathak (2008), "Finally, My open letter on OOXML happenings in India", Deepak Pathak's Blog, <https://deepakphatak.blogspot.com/2008/05/this-is.html>

[16] Roy Schestowitz (2008) "Microsoft's Latest Smear Campaign: 'Disobedient' Chairperson in India Targeted", Techrights, <http://techrights.org/2008/04/06/microsoft-strongarming-india/>

[17] ET Bureau (2008) "OOXML put on hold amid opposition from India", The Economic Times, <https://economictimes.indiatimes.com/tech/software/ooxml-put-on-hold-amid-opposition-from-india/articleshow/3124543.cms>

Indian government's concerns were in the minority at the ISO vote, and Microsoft's attempts did culminate in the successful fast-tracking of OOXML as an ISO standard,[18] a decision which was questioned internally within the ISO as well.[19]

Certain government organisations too have been attuned to the significance of SDOs. Intelligence agencies such as the NSA have been especially interested in encryption-related developments within SDOs.[20] For instance, the NSA-authored Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG) for elliptic curve cryptography that was approved by the American National Standards Institute (ANSI), the National Institute of Standards and Technology (NIST) and the ISO was suspected to have a backdoor included as a part of the NSA's Bullrun program.[21, 22, 23, 24] The United Kingdom's Government Communications Headquarters (GCHQ) and the United States' NSA have reportedly collaborated in the past to further common interests at the IETF[25], the open standards body that has long played a crucial role in developing the Internet communication protocol suite.[26] Ian Brown (a former consultant for the United States government at IETF), while contributing to a debate at the Internet Governance Forum 2017, acknowledged the utilisation of informal mechanisms by governments to sway voting processes at the IETF.[27] One mechanism that was previously highlighted in the debate was funding favourable participation in the form of mathematicians and academicians, in order to contribute to the "humming", one of the methods by which rough consensus is determined at the IETF.[28]

The ensuing discussion attempts to acknowledge the increasing role of SDOs and contextualise it within the observed absence of focussed participation of Indian government instrumentalities at these fora. In doing so, the specific instance of the contemporary debate around TLS 1.3 at the IETF is taken. Other SDOs such as the World Wide Web Consortium (W3C), 3rd Generation Partnership Project (3GPP), International Telecommunication Union (ITU), etc., and internet governance fora like the Internet Governance Forum (IGF) and the Internet Corporation for Assigned Names and Numbers (ICANN) are left for a later in-depth

---

[18] Katie Bird (2008), "ISO/IEC DIS 29500 receives necessary votes for approval as an International Standard", International Organisation for Standardization, <**https://www.iso.org/news/2008/04/Ref1123.html**>

[19] Stefan Krempl (2008), "New doubts about ISO's fast-track standardisation of Microsoft OOXML", Wikileaks, <**https://wikileaks.org/wiki/New_doubts_about_ISO%27s_fast-track_standardisation_of_Microsoft_OOXML**>

[20] Spiegel Staff (2014), "Inside the NSA's War on Internet Security", Spiegel, <**http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html**>

[21] Bruce Schneier (2007), "Did NSA Put a Secret Backdoor in New Encryption Standard?", Wired, <**https://www.wired.com/2007/11/securitymatters-1115/**>

[22] *See* Dan Shumow & Niels Ferguson (2007), "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng", RUMP 2007, <**http://rump2007.cr.yp.to/15-shumow.pdf**>

[23] *For an analysis of how a back-doored random bit generator came to be included in the standards, see* John Kelsey (2014), "Dual EC in X9.82 and XP 800-90", National Institute of Standards and Technology, <**https://csrc.nist.gov/csrc/media/projects/crypto-standards-development-process/documents/dualec_in_x982_and_sp800-90.pdf**>

[24] Nicole Perlroth, Jeff Larson & Scott Shane (2013), "N.S.A. Able to Foil Basic Safeguards of Privacy on Web", The New York Times, <**https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html**>

[25] GCWiki (2014), "VoIP NSA alias", GCWiki, <**http://www.spiegel.de/media/media-35537.pdf**>

[26] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts & Stephen Wolff (1997), "A brief history of the internet", Internet Society, <**https://www.internetsociety.org/internet/history-internet/brief-history-internet/**>

[27] Internet Governance Forum (2017), "IGF 2017 - State-led interference in encrypted systems", Internet Governance Forum,<**http://www.youtube.com/watch?v=3jbuO42Czog&t=72m21s**>

[28] Ibid,<**http://www.youtube.com/watch?v=3jbuO42Czog&t=65m0s**>

treatment. The specific instance of TLS 1.3 is taken keeping in mind the potential implications it may portend for the Indian government as evidenced by its own documentation — a roundtable concept note pertaining to TLS 1.3 — that will be discussed hereafter.

Case Study: TLS 1.3

Context

The revelations made by journalists on the basis of National Security Agency's documents obtained by Edward Snowden were, in the words of then Chair of the Internet Engineering Task Force (IETF), "a wake-up call" for the IETF.[29] One of the first responses from the IETF community to these revelations was a document, "Pervasive Monitoring Is an Attack",[30] acknowledging the constant widespread surveillance possible through the collection and analysis of the various artefacts produced in online communication.[31] The document articulated the IETF's newfound commitment to the preservation of privacy for internet users by mitigating pervasive monitoring. In a call for action, it stated, "[i]t is therefore timely to revisit the security and privacy properties of our standards."[32]

These initial discussions were followed by a slew of proposals in the IETF aimed at hardening the security and privacy aspects of internet standards and protocols, including but not limited to, the obsoletion of RC4 (an encryption standard that was used in TLS, but found to be vulnerable),[33] an articulation of "opportunistic security" (wherein some security is formally preferred if end-to-end security is not possible)[34], and even experiments to add security to network layer packets[35].

Proposal for TLS 1.3

One such proposal was updating TLS 1.2, the widely-used protocol that powers most online encryption, with security and performance upgrades.[36] Some proposed changes included disallowing outdated and vulnerable cryptography, reducing the number of round-trips required to establish TLS-encrypted communication, and entirely removing the round-trip required to resume communication encrypted with TLS.[37, 38]

---

[29] Radio Netherlands Worldwide (2014), "In response to NSA revelations, the internet's engineers set out to PRISM-proof the net", Radio Netherlands Worldwide, <https://www.rnw.org/archive/response-nsa-revelations-internets-engineers-set-out-prism-proof-net>

[30] Stephen Farrell & Hannes Tschofenig (2014), "RFC 7258: Pervasive Monitoring Is an Attack", Internet Engineering Task Force, <https://tools.ietf.org/html/rfc7258>

[31] Keiren McCarthy (2015), "Snowden to the IETF: Please make an internet for users, not the spies", The Register, <https://www.theregister.co.uk/2015/07/20/edward_snowden_to_the_ietf_please_design_an_internet_for_the_user_not_the_spy/>

[32] Supra, 30.

[33] Andrei Popov (2015), "RFC 7465: Prohibiting RC4 Cipher Suites", Internet Engineering Task Force, <https://tools.ietf.org/html/rfc7465>

[34] Viktor Dukhovni (2014), "RFC 7435: Opportunistic Security: Some Protection Most of the Time", Internet Engineering Task Force, <https://tools.ietf.org/html/rfc7435>

[35] Adrian Farrel & Stephen Farrell (2014), "Internet Draft: Opportunistic Security in MPLS Networks", Internet Engineering Task Force, <https://tools.ietf.org/html/draft-farrelll-mpls-opportunistic-encrypt-03>

[36] Tim Dierks & Eric Rescorla (2014), "Internet Draft: The Transport Layer Security (TLS) Protocol Version 1.3", Internet Engineering Task Force, <https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/00/>

[37] Eric Rescorla (2018), "TLS 1.3 Published: in Firefox Today", Mozilla Security Blog, <https://blog.mozilla.org/security/2018/08/13/tls-1-3-published-in-firefox-today/>

While most of these proposals achieved consensus early in the design process,[39, 40] there were proposed changes that were more contentious. A security proposal, for example, was to encrypt parts of the 'handshake' (the initial exchange of cryptographical data to establish an encrypted connection). In TLS 1.2, the entire handshake was in cleartext, which led to the identity of the server (with its certificate and signature) being leaked to eavesdroppers. Many network middleboxes also used this information for network management. TLS 1.3, however, encrypts most of the handshake and thus, provides greater security and privacy.

Additionally, TLS 1.2 used a static key exchange mechanism which led to non-perfect forward secrecy, i.e. if a party recorded all traffic between a client and a server using TLS 1.2, the communication could be decrypted later if the said party obtained the server's private key.[41]

To strengthen communication security provided through TLS 1.3, a proposal advocated for perfect forward security through the adoption of ephemeral Diffie-Hellman as the primary cryptographic key exchange mechanism. For its increased security, this proposal was backed by several organisations, including the Mozilla Foundation[42] and Cisco[43]. However, a consortium of financial institutions opposed this proposed change, arguing that domestic regulation required them to monitor and audit actions of employees:[44] the lack of perfect forward secrecy was used by some corporations to decrypt in-house traffic to monitor employees' communication.[45] It was also leveraged by intelligence agencies, like the NSA, to decrypt user traffic if they managed to secure the server's private key.[46, 47]

Considering the large impact of these security changes on often oppositional interests of Internet users, governments and private companies, the discussions around the design of TLS 1.3 lasted months.

Conclusion of the debate

After more than four years in development, TLS 1.3 was published as a standard on August 10, 2018.[48, 49] The consensus, since March 2018, had been in favour of a "hardened" TLS with

---

[38] Nick Sullivan (2018), "A Detailed Look at RFC 8446 (a.k.a. TLS 1.3)", Cloudflare Blog, <**https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/**>

[39] Eric Rescorla (2013), "TLS 1.3 Wish List", Internet Engineering Task Force - IETF87, <**https://www.ietf.org/proceedings/87/slides/slides-87-tls-5.pdf**>

[40] Supra, 38.

[41] Yaron Sheffer, Ralph Holz & Peter Saint-Andre (2015), "RFC 7525: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", Internet Engineering Task Force, <**https://tools.ietf.org/html/rfc7525**>

[42] Supra, 36.

[43] Patrick Crowley (2018), "TLS 1.3 and Forward Secrecy: Count Us In, and Here's Why", Cisco Blogs, <**https://blogs.cisco.com/security/tls-1-3-and-forward-secrecy-count-us-in-and-heres-why**>

[44] Andrew Kennedy (2015), "TLS: Industry Concerns about TLS 1.3", Mailing List archive of the Internet Engineering Task Force, <**https://www.ietf.org/mail-archive/web/tls/current/msg21275.html**>

[45] *Also see discussion around* Matthew Green, Ralph Droms, Russ Housley, Paul Turner & Steve Fenter (2017), "Internet Draft: Data Center use of Static Diffie-Hellman in TLS 1.3", Internet Engineering Task Force, <**https://tools.ietf.org/html/draft-green-tls-static-dh-in-tls13-01**>

[46] Kim Zetter (2014), "Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years", Wired Magazine, <**https://www.wired.com/2014/04/nsa-exploited-heartbleed-two-years/**>

[47] Supra, 38.

[48] Eric Rescorla (2018), "RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3", Internet Engineering Task Force, <**https://datatracker.ietf.org/doc/rfc8446/**>

perfect forward secrecy.[50] Additionally, since TLS 1.3 encrypts significant portions of the handshake, it impedes the ability of middleboxes in the network from tracking communication metadata. These developments make the decryption of intercepted traffic much more difficult for eavesdroppers, including intelligence agencies. The chairs of the TLS working group described the new standard as a "major revision designed for the modern Internet" with "major improvements in the areas of security, performance, and privacy".[51]

Roundtable by the Ministry of Electronics and Information Technology

In lieu of preparing an approach paper representing India's views on the TLS 1.3 debate, the Ministry of Electronics and Information Technology (MeitY) sought to organise a roundtable on August 23, 2017 to collate various stakeholder views. The concept note for a proposed roundtable discussing the TLS 1.3 debate[52] is a useful starting point for understanding the view that Meity sought to further at the IETF. Titled "TLS 1.3 Implementation (Effects on Encryption and Decryption) - Impact on Indian Enterprises", the concept note hinted that MeitY's position on the TLS 1.3 would have been similar to that of the financial consortium at the IETF (as highlighted above).

The concept note goes on to highlight that the implementation of hardened TLS 1.3 at the IETF would result in severe impacts on how financial institutions operate in terms of surveillance and monitoring of employees, fraud monitoring as well as network diagnostics. MeitY's gravest concern highlighted in the concept note is the impediment that the implementation of TLS 1.3 would pose towards meeting regulatory and legal encryption compliances on part of financial institutions. The concept note also points out the need for the roundtable to solve for these issues "until the critical concerns surrounding enterprise security, supervision, and network troubleshooting are addressed as effectively as internet MITM and surveillance threats have been."

The MeitY, in its objectives for the roundtable, also sought to increase participation of Indian representation from diverse sectors in the TLS 1.3 working group at the IETF. However, the roundtable was subsequently cancelled and to the best of our knowledge, no other public-facing discussion on TLS 1.3 was undertaken by MeitY.

National security and policy implications

While the aforementioned concept note hinted at MeitY's position being similar to that of financial institutions at the IETF, possibly owing to the barriers hardened TLS poses for "authorised interception" of communication[53], other ministerial departments might have had

[49] Keiren McCarthy (2018), "It's official: TLS 1.3 approved as standard while spies weep", The Register, <**https://www.theregister.co.uk/2018/08/13/tls_13_approved/**>

[50] Keiren McCarthy (2018), "World celebrates, cyber-snoops cry as TLS 1.3 internet crypto approved", The Register, <**https://www.theregister.co.uk/2018/03/23/tls_1_3_approved_ietf/**>

[51] Joseph Salowey, Sean Turner, Christopher Wood (2018), "TLS 1.3", Internet Engineering Task Force Blog, <**https://www.ietf.org/blog/tls13/**>

[52] *Available on file; Sunil Abraham was one of the invitees to the roundtable.*

[53] Department of Telecommunications (), Part I, Clause 3.6, License Agreement for Provision of Internet Services, Department of Telecommunications, Government of India. See also Section 69, IT Act

different concerns and even opposing views on the security proposals for TLS 1.3 considering its domestic policy and national security implications.

For instance, governmental departments have separately expressed security concerns with Chinese telecom and networking equipment covertly providing information to Chinese intelligence agencies. In April 2010, the Ministry of Home Affairs issued regulations requiring Indian telecom companies to get security clearance for their equipment[54]; in May 2013, the National Security Council, citing Intelligence Bureau reports, claimed that Chinese equipment manufacturers Huawei and ZTE targeted network switches and routers in India as part of a Chinese Army project;[55] and in September 2018, the Department of Telecommunications excluded Chinese companies from the first 5G trials purportedly over national security concerns.[56] In the absence of uptake of indigenously manufactured telecommunication apparatus, the concerns have manifested in the government's attempts at setting up telecommunication gear test labs in India but there is no evidence of any such test labs having progressed beyond the proof-of-concept stage.[57, 58] Concerns around foreign compromise of telecommunication infrastructure is not endemic to India; similar concerns around various network equipment companies aiding intelligence agencies in other jurisdictions have been raised.[59]

As discussed above, TLS 1.2 leaked the identity of the server to all entities able to passively monitor the network, including middleboxes. Additionally, even if the networking equipment records all traffic it is transmitting, perfect forward secrecy in TLS 1.3 ensures that the communication cannot be decrypted at a later stage. Considering these two security properties, the IETF's publication of the "hardened" TLS 1.3 may be considered favourable since it assuages the aforementioned national security concerns.

On the other hand, perfect forward secrecy implies that TLS 1.3 makes "it much harder for eavesdroppers [including intelligence agencies] to decrypt intercepted traffic"[60], which may have implications for domestic surveillance carried out by Indian law enforcement. Section

---

[54] The Associated Press (2010), "India bans Chinese telecom equipment", Canadian Broadcasting Corporation, <**https://www.cbc.ca/news/business/india-bans-chinese-telecom-equipment-1.874847**>

[55] Joji Thomas Philip (2013), "NSC points to Huawei, ZTE's links with Chinese military", The Economic Times, <**https://economictimes.indiatimes.com/news/politics-and-nation/nsc-points-to-huawei-ztes-links-with-chinese-military/articleshow/20056800.cms**>

[56] Muntazir Abbas (2018), "India dials Cisco, Samsung, Nokia, Ericsson, says no to Chinese Huawei, ZTE", The Economic Times, <**https://telecom.economictimes.indiatimes.com/news/india-rings-cisco-samsung-nokia-ericsson-for-5g-trials-bars-chinese-huawei-zte/65800938**>

[57] Press Trust of India (2016), "DoT to float tender for telecom gear test lab in Delhi", The Economic Times, <**https://economictimes.indiatimes.com/industry/telecom/dot-to-float-tender-for-telecom-gear-test-lab-in-delhi/articleshow/51060363.cms**>

[58] Johnson TA (2013), "No one thought telecom equipment testing lab will take time after proof of concept", The Indian Express, <**https://indianexpress.com/article/cities/city-others/no-one-thought-telecom-equipment-testing-lab-will-take-time-after-proof-of-concept/**>

[59] *See* Jason Vest and Wayne Madsen (1999), "How the U.S. undid UNSCOM through its empire of electronic ears", The Village Voice, <**https://fas.org/irp/news/1999/02/vest_madsen.htm**>; David Kravets (2013), "NSA Leak Vindicates AT&T Whistleblower", Wired Magazine, <**https://www.wired.com/2013/06/nsa-whistleblower-klein/**>; BBC Technology (2018), "Huawei and ZTE handed 5G network ban in Australia", British Broadcasting Company, <**https://www.bbc.com/news/technology-45281495**>

[60] Supra, 49.

69 of the Information Technology Act, 2000, read with Rule 17 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, for instance, empowers Government agencies to mandate the disclosure of decryption keys being utilised by service providers. Further, the obsoletion of certain encryption algorithms and key exchange mechanisms in TLS 1.3 also portends to have implications for the preparation of a national-level encryption policy, if the Government envisions a policy similar to the previously retracted draft.[61]

There are implications of the development in domestic regulation of industries as well. For example, the aforementioned concept note identified that the obsoletion of static RSA key exchange mechanisms may pose challenges for Internet Service Providers to comply with the License Agreement that they enter into with the Department of Telecommunications; the license only permits use of 40-bit RSA encryption or equivalent while also prohibiting bulk encryption[62]. Yet another example can be found in the financial sector: banks may find it hard to implement the mandatory logging of activity required by the cybersecurity regulations issued by the Reserve Bank of India, a concern similar to what the consortium of financial institutions highlighted at the IETF.[63] Financial institutions regulated by the RBI may similarly find it impossible to meet the requirements mandating the local (in India) storage of "end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction" as provided under the RBI's notification mandating storage of payment system data in India.[64]

Clearly, the debates around TLS 1.3 involved serious interests of citizens' privacy, Indian businesses, and intelligence and defence agencies, which the government had taken cognizance of. The impact of international standard setting on domestic strategy formulation along with a concomitant need for harmonisation of domestic policies with internationally instituted standards is amply evident.

Notwithstanding the outcome at the IETF, we observed low participation from the concerned government departments at the relevant IETF meetings[65] wherein several key issues relating to TLS 1.3 were discussed and voted upon. This is surprising given the MeitY's broader capacity-building efforts such as the offer of scholarships and fellowships in lieu of encouraging Indian participation in working groups at the IETF.[66]

---

[61] *The previous draft national encryption policy, most prominently for the purposes of this brief, permitted the usage of only those encryption algorithms and key sizes that would be notified by the Government.*

[62] Department of Telecommunications, Part I, Clause 2.2 (vii), License Agreement for Provision of Internet Services, Department of Telecommunications, Government of India. *The Unified License Agreement, however, does not prescribe an RSA encryption pre-size while retaining the prohibition on bulk encryption. The term 'bulk encryption' has not been defined.*

[63] Reserve Bank of India (2016), "Cyber Security Framework in Banks", Reserve Bank of India, <**https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF**>

[64] Reserve Bank of India (2018), "Storage of Payment System Data", Reserve Bank of India, <**https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF**>

[65] *Analysis available on file: one MeitY employee attended IETF 99, none attended IETF 100, one attended IETF 101. Notably, IETF 101 also had a participant from the Ministry of Home Affairs.*

[66] Ministry of Electronics & Information Technology (2018), "Internet Proliferation and Governance", Ministry of Electronics & Information Technology, <**http://meity.gov.in/content/internet-proliferation-governance**>

An overview of measures adopted by Indian government bodies

The MeitY has an Internet Governance division whose role has been described as representing India's "[p]ublic [p]olicy concerns on global platform[s]", including "[e]ncouraging greater participation in [the] Internet Engineering Task Force (IETF) Working groups"[67] among other internet governance fora. We laud the Government's efforts in setting up such a division, and two further accompanying offices: the MeitY chair on Internet Policy[68] and the web portal on India Internet Governance.[69]

Notably, the MeitY seeks to evolve a multi-stakeholder approach towards participation in matters of Internet Governance. However, it does not go into detail of how the approach may differ for various internet governance fora. Regarding developments at the IETF, we found two relevant events organised in the past: the roundtable we discuss earlier, and a a technical talk, 'Internet standards and securing IoT devices', organised in August 2017,[70]

The Internet Governance division of the MeitY also sponsors the activities of the India Internet Research & Engineering Forum (IIREF), which are carried out by the Center for Development of Advanced Computing (C-DAC).[71] IIREF has organised events related to developments at the IETF[72], published IETF meeting reports[73], and also aims to financially supports IETF participants with a fellowship[74]. The latter effort, however, seems to have been discontinued.[75]

The Indian Government also engages with other internet governance fora and standards bodies. The Government has been active in sending comments to the ICANN,[76] which regularly has open consultations. The Bureau of Indian Standards (BIS) was set up through Parliamentary legislation for the "harmonious development of standardisation activity in

---

[67] Ibid.

[68] MeitY Chair on Internet Policy (2018), "MeitY Chair on Internet Policy", MeitY Chair on Internet Policy,, <http://internetpolicy.in/home/>

[69] India Internet Governance (2018), "India Internet Governance", India Internet Governance, <http://indiaig.in/>

[70] India Internet Governance (2017), "Internet standards and securing IoT devices", India Internet Governance, <http://indiaig.in/internet-standards-and-securing-iot-devices/>

[71] Indian Internet Research and Engineering Forum (2018), "About Us", Indian Internet Research and Engineering Forum, <https://iiref.in/about>

[72] Indian Internet Research and Engineering Forum (2018), "List of Expert Meetings/Brainstorming Sessions", Indian Internet Research and Engineering Forum, <https://iiref.in/meeting>

[73] Indian Internet Research and Engineering Forum (2018), "IIREF Reports", Indian Internet Research and Engineering Forum, <https://iiref.in/ietfreports>

[74] Indian Internet Research and Engineering Forum (2018), "Fellowship", Indian Internet Research and Engineering Forum, <https://iiref.in/fellowship>

[75] *At the time of writing this brief, the Fellowship webpage was not available through the IIREF website. Previously, one of the authors of this report (Gurshabad Grover) was awarded the fellowship for participation at IETF102, albeit at a delayed stage making his participation impossible. The fellowship, although meant to be, was not extended to the next IETF event.*

[76] India Internet Governance (2018), "Government of India Submissions", India Internet Governance, <http://indiaig.in/government-of-india-submissions-2/>

India",[77] and participates as the national standards body in relevant work at the ISO and the International Electrotechnical Commission (IEC).

Recommendations

The primary recommendation here is to focus resources towards high-quality Indian participation at every SDO.

A long-term outlook would entail consistent public funding that promotes research and development programs in various public and private stakeholders in this space. The funding should also be constantly evaluated based on metrics typically associated with scientific rigour, such as acceptance of research in peer-reviewed journals.[78] The scholarships and fellowships set up by the MeitY is a step in the right direction which needs more publicity to be effective.

Currently, active participation from the Indian government is only being seen at the ITU-T and ICANN. Keeping in mind the influence of SDOs in cyberspace, we recommend that the Indian Government send a 5-member contingent to various technical SDOs, including the IETF, W3C, 3GPP (4G and 5G). Notably, we observed a lack of representation from national security agencies, law enforcement, and national defence wings in the TLS 1.3 debate, and in Internet Governance fora in general. As we highlight earlier, developments like TLS 1.3 have important implications for communication security and can assuage concerns of foreign surveillance on Indian networks. India has historically procured (and continues to procure) most networking equipment from foreign manufacturers; a common response to the threats posed by such infrastructure has been a call for the adoption of indigenously produced equipment.[79] It is the absence of alternatives that have, in part, necessitated procurement from foreign manufacturers. Consequently, a shift to indigenously produced equipment will require concerted support and direction from the government to first enable an ecosystem for such production. The shift to indigenous equipment, then, promises to be a long-drawn effort. Concomitantly participating in technical standards setting can be a more effective method of establishing trust in networking infrastructure.

Moreover, the government can actively open up these activities to organisations working in the area to represent a diversity of views from across stakeholder groups. The roundtable discussing TLS 1.3 that the MeitY sought to conduct could have been an important starting

---

[77] Bureau of Indian Standards (2018), "Standards Overview", Bureau of Indian Standards,, <http://bis.gov.in/?page_id=132>

[78] Sunil Abraham (2015), "Hits and Misses With the Draft Encryption Policy", The Wire, <https://thewire.in/tech/hits-and-misses-with-the-draft-encryption-policy>

[79] *For recent examples, see* D. S. Hooda (2018), " At digital war: India might lose the cyberspace face-offs unless IT infrastructure of the military is indigenised soon.", Indian Express, <https://indianexpress.com/article/opinion/columns/cyber-warfare-indian-military-defence-cyber-attack-at-digital-war-5416998/>; Smita Purushottam (2018), "Chinese threat to cybersecurity: Why India needs a comprehensive & concrete action plan for national security and economic health", Financial Express, <https://www.financialexpress.com/opinion/chinese-threat-to-cybersecurity-why-india-needs-a-comprehensive-concrete-action-plan-for-national-security-and-economic-health/1363012/>; Girish Shahane (2018), "For India's national security, technological self-sufficiency remains a crucial, yet neglected goal", Scroll, <https://scroll.in/article/903707/for-indias-national-security-technological-self-sufficiency-remains-a-crucial-yet-neglected-goal>

point for assimilating these diverse views for representation at the IETF; it sought to solicit views from at least four groups of stakeholders: the technical community, academia, civil society, banking and financial community, and law enforcement agencies. The MeitY could have additionally invited representatives from telecom companies, network operators, Indian defence wings, and the national intelligence agencies.

Even though the stated approach of the MeitY is to develop a multi-stakeholder approach, there is a pronounced need to develop different strategies for internet governance fora and standards body depending on their participation model. For example, even though the Government of India can regularly engage with ICANN processes due to its open consultations, high engagement with ongoing work at the IETF can only be sustained with individuals dedicated to following the work of specific working groups over prolonged periods of time. This strategy has been adopted by the NSA, for example, which has had an employee even taking up administrative and leadership positions in influential working groups at the IETF.[80]

Additionally, existing standards and internet governance work (highlighted in the previous section) across bodies like the MeitY, the National Internet Exchange of India (NIXI), and the BIS can be harmonised and coordinated for more effective contributions to developments in the various fora. For instance, we found no evidence that BIS is collaborating with the MeitY on engagement with open standards in the IETF. The Government can also explore collaborations with non-governmental organisations that aim to increase Indian participation at the IETF, such as Internet Society,[81] India Internet Engineering Society (IIESoc),[82] and the Centre for Internet and Society.

As we have highlighted through the debates surrounding TLS 1.3, the institution of SDOs and technical standards has implications for domestic policy, regulation of businesses, and security of critical military and intelligence infrastructure. This sphere of influence extends to the development issues, wherein recent discourse has highlighted advantages that the global North has historically enjoyed in setting technical standards.[83] Participation in SDOs, thus, can give India an edge in influencing global technical norms, and presents an untapped geopolitical opportunity for India.

---

[80] Dan Goodin (2013), "Critics: NSA agent co-chairing key crypto standards body should be removed", Ars Technica, <**https://arstechnica.com/information-technology/2013/12/critics-nsa-agent-co-chairing-key-crypto-standards-body-should-be-removed/**>

[81] Internet Society Kolkata Chapter (2017), "Indian IETF Capacity Building Phase II – Interim Report", Beyond the Net (Internet Society), <**https://www.internetsociety.org/resources/doc/2017/indian-ietf-capacity-building-phase-ii-interim-report/**>

[82] India Internet Engineering Society (2018), "About IIESoc", India Internet Engineering Society, <**https://www.iiesoc.in/about**>

[83] *See* Luna DR Mayan JC, García MJ, Almerares AA, Househ M. (2014), "Challenges and potential solutions for big data implementations in developing countries", Yearb Med Inform. 9(1):36–41; Martin Hilbert (2013), "Big Data for Development:From Information-to Knowledge Societies", <**https://ssrn.com/abstract=2205145**>