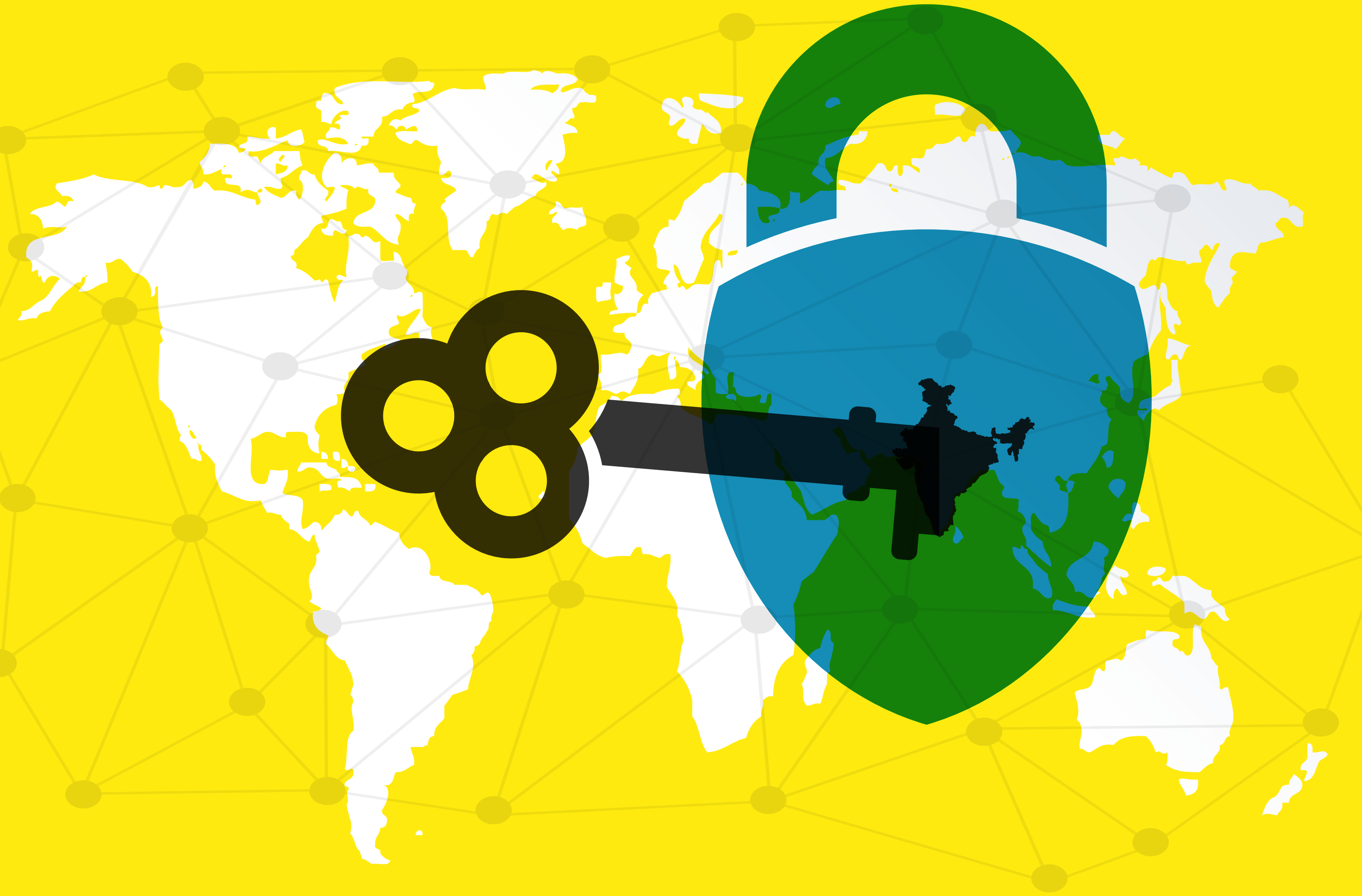
CYBERSECURITY, INTERNET GOVERNANCE & INDIA'S FOREIGN POLICY: HISTORICAL ANTECEDENTS



SAIKAT **DATTA**
INTERNET DEMOCRACY PROJECT

Cybersecurity, Internet Governance & India’s Foreign Policy:

Historical Antecendents

Saikat Datta

Internet Democracy Project
Delhi
January 2016

Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents
Author: Saikat Datta

Editor: Anja Kovacs
Design: Oorna Datta Designs
Publisher: Internet Democracy Project
Printed by: Inkprint.in

Contact:

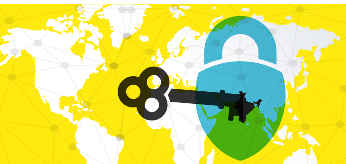
Internet Democracy Project
143-A, Second Floor
Shahpur Jat
New Delhi 110049
India

Email: info@internetdemocracy.in
Website: https://internetdemocracy.in/
Twitter: @iNetDemocracy
Facebook: https://www.facebook.com/internetdemocracy.in/

Since 2011, the Internet Democracy Project works for an Internet that supports freedom of expression, democracy and social justice, in India and beyond - through research, advocacy, and dialogue.

The views expressed in this publication are those of the author and do not necessarily represent the views of the Internet Democracy Project.

Table of Contents



List of Abbreviations

BJP	Bharatiya Janata Party
BRICS	Brazil, Russia, India, China and South Africa
CAPS	Centre for Air Power Studies
CCA	Controller of Certifying Authorities
CENTO	Central Treaty Organisation
CERT-IN	India's Computer Emergency Response Team
CII	Critical Information Infrastructure
CIRP	Committee for Internet-related Policies
CLAWS	Centre for Land and Warfare Studies
CONCERT	Countrywide Network for Computerised Enhanced Reservation Ticketing
CRIS	Centre for Railway Information Services
CTBT	Comprehensive Test Ban Treaty
GCHQ	Government Communications Headquarters
IB	Intelligence Bureau
IBSA	India, Brazil and South Africa
ICT	Information and Communications Technology
IDSA	Institute for Defence Studies and Analyses
IGF	Internet Governance Forum
IM	Indian Mujahideen
ISRO	Indian Space Research Organisation
IT	Information Technology
ITES	Information Technology Enabled Services
ITU	International Telecommunications Union
KELTECH	Kerala Hi-tech Industries Limited

LEAs	Law Enforcement Agencies
LeT	Lashkar-e-Taiba
MLAT	Mutual Legal Assistance Treaty
MTCR	Missile Technology Control Regime
NAM	Non Aligned Movement
NATO	North Atlantic Treaty Organisation
NCIIPC	National Critical Information Infrastructure Protection Centre
NDA	National Democratic Alliance
NGN	Next Generation Networks
NPT	Non Proliferation Treaty
NSA	National Security Advisor
NSG	Nuclear Suppliers Group
NTRO	National Technical Research Organisation
OIC	Organisation of Islamic Countries
RTI	Right to Information
SoPs	Standard Operating Procedures
SPP	Sector Specific Plans
TRAI	Telecom Regulatory Authority of India
UK	United Kingdom
US	United States of America
UN	United Nations
UP	Uttar Pradesh
V/T/R	Vulnerability/Threat/Risk
VoIP	Voice over Internet Protocol
WSIS	World Summit on the Information Society

About the Author

Saikat Datta is the former Editor (National Security) with the Hindustan Times, Delhi. He has been a journalist for over nineteen years, writing on the intersection between government, policy, security, intelligence and defence. His work has been awarded the International Press Institute Award, the National Right to Information (RTI) Award for Investigative Journalism and the Jagan Phadnis Memorial Award for Investigative Journalism.

He is also the author of a book on the history and the future of India's Special Forces, published by the United Services Institution. He has presented and published several academic papers for the National Security Guards, the Indian Army's think tank, the Centre for Land Warfare Studies (CLAWS) and the Indian Air Force's think tank, the Centre for Air Power Studies (CAPS).

He is currently working on several cybersecurity, risk assessment and de-risking projects for Global Corporate Security, an associate company of Reliance Industries Limited. He is also a Visiting Fellow with the Observer Research Foundation, Delhi and Lead Researcher on a cybersecurity project with the Internet Democracy Project, Delhi.

The views expressed in this paper are strictly his own and do not necessarily reflect the views of the Internet Democracy Project or of any other individual or entity that Mr. Datta is associated with.

INTRODUCTION

India's stances in global Internet governance debates have often been noted, and criticised, for their strong preference for multilateral models of engagements, as different from the multistakeholder approaches that are so well-established in the field.

This was perhaps the case most notably when it proposed, in 2011, to set up within the United Nations (UN) a Committee for Internet-related Policies (CIRP) as a new institutional mechanism to deal with big, global public policy questions in Internet governance. The CIRP would comprise 50 member-states, based on equitable geographic representation. Although it would take inputs from the Internet Governance Forum (IGF), and although the proposal mentioned multistakeholder representation for good measure, this was a classic multilateral approach.[1]

Critics welcomed, therefore, the announcement by Union Minister for Communications and Information Technology, Mr. Ravi Shankar Prasad, in June 2015, of a change in India's official policy to support for a multistakeholder approach.[2] But even then, Mr. Prasad made clear, India would continue to advocate for a dominant role of the state in security-related matters.

This was also reflected in a subsequent domestic controversy, when the government released the draft National Encryption Policy in September 2015. The draft policy included clauses seeking to direct over-the-top applications like WhatsApp to store all communication logs for over 90 days, to be made available in simple text format when sought by the government.[3] A major public outcry forced the government to withdraw the policy, but it was clear that India would continue to voice unilateral policies on Internet-related subjects when it came to security.

Why is the government predisposed towards unilateral government policy making that has far reaching implications on the daily applications of technology? In a pointed speech at the Hindustan Times Summit in New Delhi, in November 2014, India's current National Security Advisor (NSA), Mr. AK Doval, provided some important pointers to the unique confluence of themes that have shaped India's stances on technology-related issues and that contextualise its international positions in particular.

Mr. Doval, a former career intelligence officer who had served the government with great distinction earlier, had taken over as the NSA after the Bharatiya Janata Party (BJP)-led National Democratic Alliance (NDA) government came to power. The NDA won an absolute majority in the 2014 general national elections – a first since 1984 – under the leadership of the BJP's Narendra Damodardas Modi, who had taken to social media sites such as Twitter and Facebook to create a major surge of support for himself and his party. After taking oath on 26 May, 2014, Mr. Modi appointed Mr. Doval as his NSA.

- [1] India's Proposal for a United Nations Committee for Internet-Related Policies (CIRP). Statement by Mr. Dushyant Singh, Hon'ble Member of Parliament, India, on Agenda Item No. 16, Information and Communications Technology for Development. New York, Sixty Sixth Session of the UN General Assembly, 26 October, 2011. https://internetdemocracy.in/wp-content/uploads/2014/07/India-UN-CIRP-Proposal-at-UNGA-2011.pdf.
- [2] Samanta, Pranab Dhal (2015). FM Arun Jaitley-led GoM Decides to Back US Model on Internet Governance via Concessions. *Economic Times*, 23 June, http://articles.economictimes.indiatimes.com/2015-06-23/news/63746235_1_icann-gom-special-arrangement.
- [3] Datta, Saikat (2015). The Government Won't Give Up Listening in on Private Communications. *Newslaundry*, 29 September, http://www.newslaundry.com/2015/09/29/why-the-draft-national-encryption-policy-is-likely-to-return/.

Speaking at the summit,[5] Mr. Doval noted, among other things, that technology, while playing a major role in uplifting India, would at the same time serve as a major security challenge, which India would have to grapple with in the years to come. 'Another set of threats will be technology', he said, 'and those technologies will include cyber, threats over cyberspace, which is a global common. We will have high tech wars, contact-less wars'.

Mr. Doval also pointed out that 'technologies will influence threats like terrorism – they will increasingly depend upon modern means of communication, transferring money', and India's security establishment will 'have to prepare for that'.

In addition to the role played by non-state actors like terrorists, Mr. Doval identified the dominance of certain big corporations on the Internet today as a major security challenge. 'One of the problems we have is that technologically we have lost out in certain areas where the root servers are all under control of countries that are not under our control', he said. 'A lot of these control systems are with the West mainly the US [...]. They are helpful to us in some areas, but not always helpful, particularly in the corporate world. There are corporations which are very powerful, and they use it. I don't want to name them, but they are very powerful'.[6]

Mr. Doval further made the point that India needed to make up for lost ground in a technology that has emerged as one of the most critical sectors to profoundly impact India's global position as an emerging super power and a premier market. He closed his speech with a special reference to the economy: 'A country which has a vast economic potential, will have great clout. A strong economy is the surest way to secure a country', he said.

As this paper will argue, the various themes that Mr. Doval drew upon to illustrate his view of India's economic and security challenges and their intersection are an extension of India's foreign policy and its historical contextual framework.

Emerging out of its colonial past in 1947, India sought to create a space for itself in the emerging global order, while battling severe lack of resources and a shattered economy. In many ways, the emerging India took to modern tools of engineering to set right the imbalance between its past and its aspirations as an independent nation.[7] The idea of engineers, and therefore technology, helping shape a modern India began to take root, and has served as the cornerstone of India's hopes and aspirations as a leader of the modern world. This is the context, then, that has, for decades, broadly shaped India's positions on issues of technology and its foreign policy postures: keeping one eye on its colonial past and another on the aspirations to use technology to arrive as a first among equals.

And as this paper will show, this basic construct also serves as the defining context that has shaped India's positions on Internet governance and cybersecurity in the last decade or so.

[4] Datta, Saikat (2014). Ajit Doval, A Giant Among Spies, Is the New National Security Advisor. *Hindustan Times*, 30 May, http://www.hindustantimes.com/india/ajit-doval-giant-among-spies-is-the-new-national-security-adviser/story-uMyz0kgmqj3RDdwEvWLGCO.html.

[5] The full speech of the NSA, Mr. AK Doval, at the annual Hindustan Times Summit, held in November 2014, can be accessed here: https://www.youtube.com/watch?v=eccxX_H_80Q.

[6] Vincent, Pheroze L (2014). Indian Muslims Are Against ISIS. *The Hindu*, 22 November, http://www.thehindu.com/news/national/indian-muslims-are-against-isis-doval/article6625258.ece.

[7] See Khilnani, Sunil (1997). *The Idea of India*. New Delhi: Penguin, which explores how India's first Prime Minister Jawaharlal Nehru took upon building a new nation with emphasis on big infrastructure projects.

To better understand how this construct plays out in this particular field, this paper will map the economic, political and historical antecedents of India's evolving positions on Internet governance as they are shaped by its concerns on cybersecurity, by its domestic context and by its overall influence on global events as they unfold. In particular, this paper will argue that India's positions on cybersecurity and Internet governance have to be traced from four broad and interconnected perspectives that have shaped India's positions in the post-Independence period and which intersect at different points in time. These four perspectives are:

1. The evolution of a part-socialist, part-government-controlled capitalist economy to a more liberal economy post-1990, which would closely interact with domestic politics.

2. India's post-Independence / post-colonial foreign policy, in particular following the -post 1990 economic realignment.

3. A history of technology denial, especially of dual use technologies in a security framework.

4. The challenges posed by terrorism and their impact on India's foreign policy.

These four broad factors, as this paper argues, are endemic to understanding India's current positions on global issues related to cybersecurity and Internet governance.

In the remainder of this paper, I will thus investigate in detail how each of these perspectives has contributed to shaping India's positions at the global level in this area. In addition, in a final section, I will assess the role that the domestic framework plays in addressing these concerns. Through this analysis, this paper hopes to contribute to a greater understanding of both India's cybersecurity concerns and of the ways in which it approaches global Internet governance as it has emerged as one possible venue to address these pressing issues.

A good start will be to look at India's evolution of a part-socialist, part-government-controlled capitalist economy to a more liberal economy post-1990, and the interaction of this with domestic politics.

1. The Economic Moorings of India's Foreign Policy on Technology

Emerging out of its colonial past in 1947, India sought to create a space for itself in the emerging global order, while battling severe lack of resources and a shattered economy. To shape its presence in international affairs, India chose to adopt a policy of bringing together nations that had also emerged from their colonial past in the same era. This would primarily mean India seeking multilateral platforms to engage with the rest of the world, even going to the extent of creating platforms such as the Non Aligned Movement (NAM) in the hope that greater numbers would accord India a leadership position in the developing world.

But just like India's foreign policy was deeply influenced by nearly 200 years of colonial rule, it also shaped its embracing a socialist and planned economy based on five-year-plans that had been formulated by the Congress party over a decade before Independence. As India's first Prime Minister, Jawaharlal Nehru adopted a statist and centrally planned economy, the emerging India in many ways took to modern tools of engineering to set right the imbalance between its past and its aspirations as an independent nation.[8] The idea of engineers, and therefore technology, helping shape a modern India began to take root, and has served as the cornerstone of India's hopes and aspirations as a leader of the modern world.

As the first Indian Institute of Technology went up at Kharagpur[9], a small town near Kolkata, the capital of the state of West Bengal, the idea of technology was rooted as a great equaliser and an enabler. Addressing the first convocation, Nehru called the institution a 'fine monument of India, representing India's urges, India's future in the making. This picture seems to me symbolical of the changes that are coming to India'[10].

Nehru's daughter, Mrs. Indira Gandhi, as the Prime Minister of the Congress (I) government, continued with his approach, taking it further to a populist model, and coining the election slogan '*garibi hatao*' (eradicate hunger).[11] This is the period that saw several multinational companies being eased out, while banks were nationalised with '14 banks controlling 70% of the country's deposits'[12].

The politics of nationalism would continue to the government that succeeded Mrs. Gandhi's government. Led by a former colleague, Mr. Moraji Desai, the Janata Party government was a ramshackle coalition of parties with varying ideologies, hastily cobbled together to oppose the Congress (I). The Janata Party government was short-lived, but its tenure saw the exit of two high profile multi-national corporations: the then Industries minister and a known labour leader, George Fernandes, ensured the exit of soft drinks manufacturer Coca Cola and IBM.[13]

- [8] *Ibid*.
- [9] See a brief history of IIT, Kharagpur on the Institute's website: http://www.iitkgp.ac.in/institute/2-3.html.
- [10] *Ibid.*
- [11] Pandey, Vikas (2012). A Short History of India's Political Slogans. *BBC News*, 9 October, http://www.bbc.com/news/world-asia-india-19802394.
- [12] Srivastava, Samar (2014). Economic Milestone: Nationalisation of Banks (1969). *Forbes India*, 12 August, http://forbesindia.com/article/independence-day-special/economic-milestone-nationalisation-of-banks-%281969%29/38415/1.
- [13] Basu, Prasenjit K (2005). India and the Knowledge Economy: The 'Stealth Miracle' is Sustainable. In Prasenjit K Basu, Brahma Chellaney, Parag Khanna and Sunil Khilnani. *India as a New Global Leader.* London: The Foreign Policy Centre, p. 45. http://fpc.org.uk/fsblob/377.pdf.

The road to IBM's exit started a few years earlier with the setting up of the Dandekar Committee on automation[14]. The Committee, headed by the noted economist V M Dandekar, recommended in 1972 controls on the introduction of computers in India, due to fears that these could have a detrimental effect on employment opportunities. Faced with a large unskilled labour force desperate for employment, the Dandekar Committee set in motion the movement that would eventually end in IBM's ouster. In and around the same time, however, there were also debates that banked on the evidence collated by the Bhabha Committee in 1963[15] to reiterate the need for an indigenous computer industry.

When IBM finally left, this was an important moment: IBM's departure would create an opportunity for Indian technology companies to step in, and as noted, 'several companies emerged over the next few years to fill the hardware and software vacuum left by IBM's departure – and three of them (Tata Consultancy Services or TCS, Wipro and Hindustan Computers Ltd or HCL) were to be at the vanguard of the 1990s information technology (IT) revolution in India'.[16] The departure of these companies had a twin impact: it gave the local industry reason to start looking at IT as a new area of business and entrepreneurship, while at the same time addressing India's emerging cybersecurity concerns as domestic companies in this field emerged and evolved.

Many of these security concerns had, in fact, first emerged at the beginning of the decade, when war broke out between India and Pakistan in December 1971. Pakistan had moved into the United States of America (US) orbit by becoming a signatory to the Central Treaty Organisation (CENTO) in 1955.[17] Even though the alliance did not prove to be successful, it ensured that US sympathies would continue to side with Pakistan. In the aftermath of the 1971 war, the Nixon administration immediately placed sanctions on India, which included ensuring an embargo on the import of electronics and computers from the US.[18] This, in turn, underscored the vulnerability of India's defence sector, which needed computers and electronics for its radars and weapon systems.

By 1980, when Mrs. Gandhi returned to power, things had begun to change. Her realisation that the earlier statist models of the economy would no longer work helped create a paradigm shift. She began with a 'modest liberalisation of the economy'.[19] This ensured that at least some sections of society were beginning to get an opportunity to set up industries and push forward the rate of growth by creating an alliance of sorts between the government and private industry. As economists have noted, Mrs. Gandhi concentrated on a three-point formula: 'prioritisation of economic growth as a state goal; supporting big business to achieve this goal; and taming labour as a necessary aspect of this strategy'.

- [14] Rajaram, V (2012). *The History of Computing in India (1955-2010)*. Bangalore: IEEE Computer Society, IISC, pp. 22-24. http://www.cbi.umn.edu/hostedpublications/pdf/Rajaraman_HistComputingIndia.pdf
- [15] Basu, *op. cit*., p. 45.
- [16] *Ibid.*
- [17] CENTO, also known as the Baghdad Pact, was formed in 1955 with Iran, Turkey, Pakistan. See https://www.wikiwand.com/en/Baghdad_Pact.
- [18] Rajaram, *op. cit.*, p. 23.
- [19] Basu, *op. cit.*, p. 45.

This 'modest liberalisation' would create the fertile ground that would be exploited by her son, Mr.Rajiv Gandhi, who would also bring in what has been termed India's first telecommunication revolution, as well as extensive computerisation. As a case in point, the extensive computerisation of the railway passenger reservation service, a major exercise in itself, was in some ways, the first great step in creating online networks and ushering in the first tentative steps to grapple with cybersecurity.

The Countrywide Network for Computerised Enhanced Reservation Ticketing (CONCERT) was started in 1987 from Delhi and made available at 700 locations initially, using 3000 computer terminals. The sites were networked and allowed passengers to book their tickets at railway counters in real time, as railway officials had visibility into the availability of tickets. Interestingly, the Indian Railways was one of the first government organisations to go in for large scale computerisation, with most of the work being carried out by the Centre for Railway Information Services (CRIS) that was created in 1986.[20]

Clearly, economic concerns profoundly impacted India's slow but steady approach to first rejecting and then embracing computers – first viewing it as a threat to the economy that was predicated towards protecting jobs, but also accepting subsequently that it was an economic enabler and could provide exciting opportunities for growth. Starting in the late 1970s, a combination of largely economic, and at times seemingly contradictory, factors that grew out of the political ideologies of that time, thus had begun to come together to forge a new destiny for India's tryst with the Internet and the possibilities it offers. By the time the Rajiv Gandhi-led government came to power in 1984, these new philosophical constructs were already beginning to take shape and could be seen in what can be termed as a more 'assertive' India. Once again, it was established in the Indian economic and political consciousness that technology is an enabler and would be able to provide substantial solutions to India's long suffering economy.

• 20. For more information, see the official website: http://cris.org.in/CRIS/About_us/About_us. Also see this 2005 Computerworld Honours Case Study on Unreserved Ticketing System (UTS) and data warehousing: http://www.cwhonors.org/laureates/transportation/20055380.pdf. This response on quora.com also offers interesting insights: https://www.quora.com/What-is-the-software-and-IT-infrastructure-behind-Indian-Railways-Ticket-Reservation-System-of-IRCTC.

2. Living with Technology Denial

While India was building its indigenous IT capabilities, it was also grappling with a range of international technology denial regimes that would leave a major impact on its foreign policy posture in the future.

The fear of a US intervention during the 1971 war had led to worries about India's sovereignty being under threat by Big Power intervention.[21] This had added further impetus to India's nuclear programme that was both peaceful and military. When in 1974, India's tests of a nuclear device led to immediate sanctions, this caused major suspicions about denial of technology among Indian policymakers.

Future events proved that this was not without reason. A case in point was the major kerfuffle over the denial of cryogenic rocket engines that India had sought for its space programme in the 1980s. The entire episode of technology denial and India's reaction to it at that point explains the deep-rooted suspicions that are firmly embedded into India's foreign policy to this day. As we will see, this event from the 1980s would deeply influence India's belief in a multilateral world order decades later, when it began to wrestle with the challenges of Internet governance.

a. Hampering the Development of India's Space Program

What happened? Around 1986-87, the Indian space programme was in the midst of developing a massive rocket to launch satellites into a 24-hour orbit.[22] The Indian Space Research Organisation (ISRO) first held discussions to develop or buy cryogenic engines with Japan but 'nothing came of it'.[23] ISRO was also approached by a US company, General Dynamics Corporation, offering an American engine.[24] But the costs were prohibitive, and an offer from the European multinational corporation, Arianespace also proved to be too costly.

A third offer materialised from the Soviet Union, which offered two engines as well as a transfer of technology for a deal that would amount to USD 200 million. ISRO immediately agreed to the proposal and on January 18, 1991, inked an agreement with the Russian space agency Glavkosmos. The deal included a transfer of cryogenic technology.

However, the Soviet Union was in chaos and Mikhail Gorbachev soon announced its dissolution, forcing a major economic and political crisis. The newborn Russian federation immediately came under considerable pressure from the US, which forced the Russians to renege on the deal for the engines and the technology transfer.

- [21] See Jacob, JFR (1997). *Surrender At Dacca: Birth of a Nation.* New Delhi: Manohar. Specifically see reference to the possible intervention of the US Seventh Fleet in Bay of Bengal during the 1971 war.
- [22] Pullakat, Hari (2014). How India Developed the Indigenous Cryogenic Engine. *Economic Times*, 9 January, http://articles.economictimes.indiatimes.com/2014-01-09/news/46030395_1_cryogenic-engine-mahendragiri-isro.
- [23] Simha, Rakesh Krishnan (2013). How India's Cryogenic programme was wrecked. *Russia & India Report*, 4 December, http://in.rbth.com/blogs/2013/12/04/how_indias_cryogenic_programme_was_wrecked_31365.
- [24] *Ibid.*

Glavkosmos and ISRO immediately began to work on an alternate plan to outsource the cryogenic engines[25] to a Kerala-based unit known as 'Kerala Hi-tech Industries Limited' (KELTEC). The arrangement was designed to get around the provisions of the Missile Technology Control Regime (MTCR),[26] a broad coalition of 34 countries that imposed restrictions on the proliferation of unmanned delivery systems (missiles) capable of carrying weapons of mass destruction. However, the new arrangement once again faced tremendous pressure from the US and the then President George Bush described it as a violation of the MTCR. In May 1992 the US imposed sanctions on both the space agencies, ISRO and Glavkosmos. Despite strong objections from New Delhi, the deal had to be scrapped.

On several occasions, India's Foreign Service officers pointed out to their US counterparts that they had not raised any objections when General Dynamics approached them with a proposal to sell the engines and the technology. The US had also never raised any objections between 1988 and 1992, when the Indian and Russian space agencies were working out a deal for a transfer of technology. Moreover, India had explained that the 'high-powered hydrogen-fuelled upper stages, which took a long time to prepare, were of little military value' and could not be adapted for military applications.[27]

Finally, a revised Indo-Russian agreement was drawn up in January 1994 that agreed to transfer seven fully assembled KVD-1 engines, without the technology. Under pressure from the US a clause was inserted that India would 'agree to use the equipment purely for peaceful purposes, not to re-export it or modernise it without Russia's consent'.[28] Even then, for India, its leveraging of its bilateral relationship with Russia to by-pass a multilateral agreement without becoming a signatory or adhering to its restrictive clauses had been a success.

b. Opposition to India's Nuclear Tests

If the denial of cryogenic engines is instructive, it is not the only occasion on which India has had to face an international technology-denial regime. In May 1998, as soon as India announced a series of successful nuclear tests, sanctions were imposed by the United States.[29] The sanctions were supported by several major European countries and led to a sudden denial of several high-technology transfers that were in the pipeline.

The sanctions also resulted in an immediate stop to several security and defence-related projects that had been on the anvil. This also delayed the indigenous light combat aircraft programme and grounded the Indian Navy's Sea King helicopters.[30] This grounded India's entire anti-submarine warfare capabilities, and the sanctions would hurt Indian security needs even more the next year when the Kargil war commenced. The war in Kargil, though primarily a localised land battle between the Indian and Pakistani armies, also saw a heightened deployment of the air and naval assets. The Indian Navy was severely hampered during its combat deployment during the war as a result of the sanctions.

- [25] *Ibid.*
- [26] For more information, see the official website: http://www.mtcr.info/english/.
- [27] *Ibid.*
- [28] *Ibid.*
- [29] CNN (1998). US Imposes Sanctions on India. *CNN*, 13 May, http://edition.cnn.com/WORLD/asiapcf/9805/13/india.us/.
- [30] Ramachandran, R. (2001). Out of the Black List. *Frontline*, 13 October, http://www.frontline.in/static/html/fl1821/18210860.htm.

The sanctions were supported by the G-7 countries, which also ensured that there was no non-humanitarian lending by various monetary bodies, such as the World Bank and the International Monetary Fund.[31]

By then, however, seeking inclusion in technology denial regimes through multilateral diplomatic effort had become the hallmark of India's approach to such regimes – be it the Non Proliferation Treaty (NPT), the Comprehensive Test Ban Treaty (CTBT), or the MTCR.

Like the MTCR, the NPT and the CTBT were regimes created to impose restrictions on technology that enabled the proliferation of weapons of mass destruction or systems that could deliver them. India had never signed on to the CTBT[32] and was opposed to the NPT for decades. In fact, when Prime Minister Narasimha Rao's government began plans to carry out nuclear tests, the US immediately commenced a major exercise to persuade him not to do so,[33] which raised Indian suspicions.

On each of these international agreements New Delhi's consistent position has been to label them as 'discriminatory', and each has repeatedly been described by India as an 'unequal treaty'.[34] India viewed these regimes with suspicion, as Big Power attempts to use technology to create a world of haves and have-nots. With its history of taking leadership roles in setting up the Non Aligned Movement as a power bloc to resist Big Power hegemony, these regimes were clearly unacceptable for India in particular.[35]

And so, when in May 1998, Prime Minister Atal Behari Vajpayee's government would carry out the nuclear tests that were shelved by Prime Minister Rao under US pressure, and the tests would lead to immediate sanctions and a dip in bilateral relations with the US, India did not merely accept the status-quo. In the wake of the sanctions imposed in the late nineties, a series of secret back-channel talks[36] between the then Minister for External Affairs, Jaswant Singh, and the US Deputy Secretary for State, Strobe Talbott, took place, which India used to raise its concerns and achieve its objectives with regards to these multilateral arrangements. As it had done with Russia earlier, India leveraged its bilateral relationship with the US in an attempt to change its status-quo vis-à-vis multilateral regimes like the NPT (or the CTBT), even without becoming a signatory to any of these treaties.[37]

c. The Threat Posed by the Wassenaar Arrangement

It is in this contextual framework then that India's consistent opposition to technology regimes that came up in the mid-1990s, such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, has to be seen.

[31] Morrow, Daniel and Michael Carriere (1999). The Economic Aspects of the 1998 Sanctions on India and Pakistan. *Nonproliferation Review*, 4:1-16, p. 5.

[32] Zerbo, Lassino (2015). India and the CTBT. *The Hindu*, 14 February, http://www.thehindu.com/opinion/columns/india-and-the-ctbt/article6892680.ece.

[33] Declassified US State Department Telegram 012545 to INTSUM Collective, 'INTSUM: India: Nuclear Tests Unlikely'. Washington DC, US State Department, 24 January, 1996. https://digitalarchive.wilsoncenter.org/document/116347.

[34] Address by then External Affairs Minister Pranab Mukherjee, at a seminar on 'India and Iran: Ancient Civilisations and Modern Nations'. Tehran, 2 November, 2008, http://mea.gov.in/Speeches-Statements.htm?dtl/1768/Address+by+HEMr+Pranab+Mukherjee+Minister+of+External+Affairs+at+a+Seminar+on+India+and+Iran++Ancient+Civilizations+and+Modern+Nations+in+Tehran.

[35] These concerns also contextualise India's position on the Budapest Convention. I come back to the Budapest Convention in section 4 of this paper.

[36] Haniffa, Aziz (2004). 'Jaswant Achieved More of His Objectives Than I': Interview with Strobe Talbott. *Rediff*, 22 September, http://www.rediff.com/news/2004/sep/21inter.htm. Also see Chellaney, Brahma (2004). Jas and Strobe Show. *India Today*, 4 October, http://indiatoday.intoday.in/story/engaging-india-diplomacy-democracy-and-the-bomb-by-strobe-talbott/1/195139.html.

[37] These talks and their outcomes are discussed in greater detail in section 3(b).

The Wassenaar Arrangement was initially brought in by the North Atlantic Treaty Organisation (NATO) countries in July 1996.[38] At that time the Arrangement was signed by 41 countries, who met again in December 1996 and issued a detailed list of items that would be placed under control.[39] This list was further expanded in 2013 after the United States' Department of Commerce, Bureau of Industry and Standards, proposed a new category covering 'intrusion software',[40] following a plenary held at Vienna in December 2013 in the wake of the Snowden revelations.[41]

When the announcement of the expansion of the list was made, Indian officials stated:

> These changes could have severe impact on India's cybersecurity programme – both software and hardware – as these would come under export control regime, the entire inventory of high-end cybertechnology is with the Western countries like the US and they may deny products to Indian organisation.[42]

Officials also argued that the 41 signatories to the Wassenaar Arrangement included the countries that have produced many of the technologies that were now being included under the regime. This would create, Indian officials and policy wonks argued, a global division between the technology haves and have-nots,[43] therefore denying them the fruits of development that the West has traditionally enjoyed.

They also argued that the changes and the new inclusions would deny developing nations like India, still grappling with the cusp of major technological challenges, the ability to carry out research, impacting the emerging digital economy.[44] This would also adversely impact India's cybersecurity, since India would be deprived of the learnings of developed nations.

India's reaction to the latest proposal under the Wassenaar Arrangement was swift and forceful, consistent with its earlier position on technology denial regimes.[45] New Delhi felt that the inclusion of cyber-related items under the Wassenaar Arrangement was an attempt to continue keeping India out of the high technology stakes. It would also ensure, New Delhi feared, that India would be kept away from the high table where key decisions are taken.[46] India reacted, in 2013, by taking pre-emptive action, buying critical technologies that could possibly come under the Wassenaar Arrangement once the updated list had been accepted by the signatories.

- [38] See this introduction to the Wassenaar Arrangement: http://www.wassenaar.org/introduction/index.html.
- [39] The first control list (as well as subsequent ones) can be found on the official website of the Wassenaar Arrangement: http://www.wassenaar.org/wp-content/uploads/2015/06/Previous/1996_OK/WA-LIST%20%2896%29%201/Control%20Lists%20-%20July%201996.pdf.
- [40] US DoC (2013) Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items. Washington DC, US Department of Commerce, Bureau of Industry and Security, 20 May, https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-11642.pdf.
- [41] Edward Snowden was employed as a contractor with the National Security Agency, a US Techint body. Snowden leaked thousands of top secret and secret NSA files that exposed several global surveillance regimes carried out by the US along with its Five Eyes partners: the United Kingdom (UK), Australia, New Zealand and Canada.
- [42] Thomas, Thomas K (2014). New Export Law Could Threaten India's Cyber Security Programme'. *Hindu Businessline*, 19 June, http://www.thehindubusinessline.com/info-tech/new-export-control-law-could-threaten-indias-cyber-security-programme/article6130704.ece. Also see Mukunth, Vasudevan (2015). Wassenaar's Woes. *Observer Research Foundation Cyber Monitor*, 3(9), http://www.orfonline.org/cms/export/orfonline/html/cyber/Cyber-Monitor09.pdf.
- [43] Sukumar, Arun Mohan (2015). Wassenaar's Web: A Threat to Technology Transfer. *The Hindu*, 5 August, http://www.thehindu.com/opinion/columns/wassenaars-web-a-threat-to-technology-transfer/article7499748.ece.
- [44] *Ibid*.
- [45] *Ibid.*
- [46] *Ibid.*

At the same time, however, New Delhi renewed its multilateral diplomatic effort with the aim of changing the multilateral paradigm and thus, making the earlier need for inclusion in this regime completely redundant. As the Wassenaar Arrangement was expanded, in 2013, to include an ever-growing list of technologies, India's then Foreign Secretary, Rajan Mathai ruled out accepting the legitimacy of these regimes as long as India was not at the decision-making table, and reiterated India's demand to be treated as an equal, which was not the case in the existing international multilateral regimes that had imposed such restrictions in the past.[47] New Delhi argued that it had an excellent track record of enforcing a 'legally based domestic export control system that would fortify the commitment to act in accordance with the guidelines' of such technology denial regimes.[48] Mr. Mathai also pointed out that India

> has a longstanding commitment to complete, universal, non- discriminatory and verifiable elimination of nuclear weapons in a time-bound manner – a vision that was set forth in the Rajiv Gandhi Action Plan. We remain committed to a voluntary and unilateral moratorium on nuclear explosive testing.[49]

Clearly, in New Delhi's view, leveraging relationships with other States to attain its objectives in multilateral forums was likely to pay the highest dividend where such discriminatory treaties were concerned. With technology-denial constructs emerging after India's attempts to harness nuclear energy for a weaponisation programme in 1974, India's opposition to any treaty or international coalitions that it deemed 'unequal' had become the norm for its foreign policy since the events of 1991, as India grappled with several economic and foreign policy crises. New Delhi consistently leveraged its equation with other governments, to engage and influence multilateral regimes. The partial success that came New Delhi's way reinforced its belief in using such an approach, especially when it came to addressing its security-related issues.

As the economic and foreign policy crises of the 90s gave further impetus to this approach, these will be examined in further detail next.

- [47] PTI (2012). India Can't Be Target of Regime Restrictions: FS Mathai. *The Hindu*, 19 April, http://www.thehindu.com/news/national/india-cant-be-target-of-regime-restrictions-mathai/article3332934.ece.
- [48] *Ibid.*
- [49] *Ibid.*

3. Charting a New Course in Foreign Policy

India's economic evolution continued to shape the country's positions on cybersecurity and Internet governance in the 1990s. As India entered the final decade of the last millennium, it came close to an economic meltdown, leading to a major reconstruction of its economic policies and the establishment of a more liberalised regime. This impacted the traditional economy, as India began the inexorable move towards a more services-oriented economy, paving the way for a greater role of computers and information technology[50] as the harbingers of great change. As the Indian economy began to grow, the Internet began to take root, slowly but steadily, thus giving birth to a new awakening to concerns about cyber security. As we will see, in addition to the uprising in Jammu and Kashmir, this also played a major role in strengthening the 'sovereignty' philosophy of India's foreign policy, while at the same time leading to India reaching out to the world, seeking new allies and shifts.

a. Economic Crisis, Political Change

In 1991, India was facing one of its worst economic crises.[51] The Gulf War in 1990 had a cascading effect on world oil prices, which in turn precipitated the crisis of the Indian economy, a year later.

As investor confidence in India eroded, this created a balance of payments deficit, sending shockwaves through the Indian economic system. [52]

As the Narasimha Rao-led Congress coalition government moved quickly to stem the rapidly spreading economic shock, it brought in an Oxford-educated economist with a World Bank background to helm the economy. Dr. Manmohan Singh would become part of the cabinet and bring about a historic liberalisation of the Indian economy that went along with the major changes that Prime Minister Narasimha Rao was planning for replacing a moribund foreign policy.

With India seeking funds and support from various Western entities to revive its economy, Prime Minister Narasimha Rao began to radically change India's earlier foreign policy biases. While India had always remained committed to Western political values,[53] it had emerged as an opponent to the Western world view on many occasions. But with India's staunch ally, the Soviet Union, dissolving, Prime Minister Rao began to look at a more pragmatic policy approach. He broke new ground by establishing diplomatic relations with Israel, ushering a new level of cooperation on security issues, while also seeking a closer equation with the United States.[54]

- 50. Computerisation in the Indian Railways', by K V Ramani, IIM, Ahmedabad Working Paper, March 1991 http://vslir.iimahd.ernet.in:8080/xmlui/bitstream/handle/123456789/6360/WP%201991_924.pdf?sequence=1&isAllowed=y
- 51. Cerra, Valerie and Chaman Saxena (2002). What Caused the 1991 Currency Crisis in India. *IMF Staff Papers*, 49(3): 395-425, https://www.imf.org/external/pubs/ft/staffp/2002/03/pdf/cerra.pdf.
- 52. *Ibid.*, p. 403.
- 53. Mohan, Raja C (2006). India's New Foreign Policy Strategy. Paper presented at a Seminar by the China Reform Forum and the Carnegie Endowment for International Peace, Beijing, 26 May. http://carnegieendowment.org/files/Mohan.pdf.
- 54. *Ibid.*

The new equation that began to emerge between India and the United States would further lead to a renewed sense of engagement that could break from the past. Two major impediments in the Indo-US relationship had begun to dissipate: the Soviet Union, a traditional ally to India, had ceased to exist, and the war in Afghanistan, supported by the US through India's traditional enemy Pakistan, was winding down after Russian troops withdrew. Clearly, there were possibilities that could be explored on both sides. A pragmatic Narasimha Rao-government was already moving ahead with many far reaching changes, and this adaptation would set the stage for a deeper engagement a decade later, that in turn, would have a major and defining impact on India's cybersecurity posturing.

The year 1990 had also witnessed a major outbreak of a popular uprising against India's rule in the Muslim-majority state of Jammu and Kashmir. The uprising was the legacy of the two-nation theory that had separated British India into two countries in 1947, based on their religious composition. Independent states like Jammu and Kashmir were given the choice to join India or Pakistan. The ruler of Jammu and Kashmir, a Dogra Rajput Hindu, threw in his lot with India, a decision that immediately led to the first Indo-Pakistan war.[55]

In many ways, the 1990 uprising in Jammu and Kashmir also played a major role in influencing India's foreign policy. The uprising led to active diplomatic and material support from Pakistan to the militancy movement, impacting India's traditional foreign policy significantly.[56]

While India was tackling the rising insurgency in Jammu and Kashmir, India and Pakistan began trading charges of human rights abuses. In many ways this single event has continued to leave a deep impact on India's foreign policy ever since. This change has been away from the 'internationalism' that was practised since independence in 1947 and instead, shifted to a new language of sovereignty.[57] India's interventions are now based on the principle that 'a call for human rights must not lead to interference in internal affairs', underscoring the theme that it will not brook any intervention in its internal affairs on any ground.

This shift, in turn, would also influence its subsequent positions on adopting a multilateral framework on various international issues such as Internet governance.[58]

b. India and the US: Stepping Up Bilateral Engagement

Despite the sanctions imposed by the US post the May 1998 nuclear tests, conducted by the short-lived Atal Behari Vajpayee-led minority government, there were back-channel bilateral talks that explored the possibility of a new relationship. President Bill Clinton tasked Strobe Talbott to engage the Indians in a series of secret parleys that would shape the next decade.[59]

The result of these secret bilateral talks was revealed in February 2000, when the US and India agreed to a slew of measures to improve their bilateral relationship.

- [55] See Dasgupta, C (2002). *War and Diplomacy in Kashmir*, 1947-1948. New Delhi: Sage, which sources de-classified documents to examine the Kashmir conflict in 1947.
- [56] See Kovacs, Anja and Saikat Datta (2015). Digital India Abroad: India's Foreign Policy and Digital Rights. In Doutje Lettinga and Lars Van Troost (Eds.), *Shifting Power and Human Rights Diplomacy: India.* Amsterdam: Amnesty International Netherlands, http://www.amnesty.nl/sites/default/files/rising_power_india_online.pdf.
- [57] *Ibid.*
- [58] *Ibid*., pp. 94-95.
- [59] See Shaikh, Nermeen (n.d.). Interview with Strobe Talbott. *Asia Society*, no date, http://asiasociety.org/interview-strobe-talbott. Also see Haniffa, *op. cit*..

One of the first moves was to establish a Joint Working Group on Counter-Terrorism that would establish commonalities in goals and find new areas of cooperation. A year later, when Prime Minister Vajpayee visited the US on his first major trip abroad, this agreement would lead to the establishment of a major bilateral security dialogue.[60] During the trip both governments made a significant addition to the Joint Working Group on Counter Terrorism by creating a sub-group for cybersecurity.[61]

The new forum clearly 'grew out of' the bilateral 'counterterrorism dialogue' and was 'dedicated to protecting the critical infrastructure of the knowledge-based economy'. The forum included 'government agencies and private sector participants from India and the United States', identifying 'risks and common concerns in cybersecurity' aimed at crafting 'an action-oriented work plan on securing networked information systems'.[62]

The new forum was also tasked with creating a comprehensive dialogue and cooperation on 'cyber-security, cyber-forensics and related research and works towards enhancing co-operation among law enforcement agencies on both sides in dealing with cyber-crime'. By January 2004, India's Computer Emergency Response Team (CERT-IN) was also active,[63] modelling itself on its US counterpart. This, too, was a result of the 2001 agreement framework to 'share expertise in artefact analysis, network traffic analysis, and exchange of information'.[64]

The path-breaking bilateral dialogue of 2000-2001 would, thus, redefine India's relationship with the US and reinforce its belief in using a bilateral relationship to achieve outcomes that could change the paradigm in multilateral settings. In many ways, India's strongest relationship on cybersecurity had now emerged from a bilateral approach with the US, which would influence its positions when dealing with various multilateral forums and regimes.

c. The Impact of Terrorism

The fact that a bilateral cybersecurity dialogue between India and the US was added as a sub-set of the Joint Working Group on Terrorism is a major indicator of how New Delhi coupled technology with terrorism, thus making the latter the overarching paradigm. It also amplified New Delhi's preference for government-to-government forums to achieve its stated foreign policy objectives. While the role of terrorism in shaping India's cybersecurity and Internet governance positions is discussed in detail in section four of this paper, it is important to understand here the basics of how it became such an overarching priority.

Post-1990, after the emergence of Pakistan-sponsored terrorism in the Kashmir Valley, India was pitted against its neighbour on global forums in a bid to establish its narrative of the conflict. As the two regional neighbours sparred on various forums, each sought to build coalitions in multilateral platforms to build their case. The fall-out of this global sparring would inevitably shape the foreign policies of both nations.

- [60] India-US Joint Statement on the Occasion of the Official Working Visit of Prime Minster to Washington DC. New Delhi, Press Information Bureau, Government of India, 10 November, 2001, http://pib.nic.in/archieve/lreleng/lyr2001/rnov2001/10112001/r101120011.html.
- [61] India-US Cybersecurity Forum: Fact Sheet. New Delhi, Ministry of External Affairs and Press Information Bureau, Government Of India, 2 march, 2006, http://pib.nic.in/newsite/erelease.aspx?relid=16132.
- [62] *Ibid.*
- [63] For the official history of CERT-IN, see its website: http://www.cert-in.org.in/.
- [64] The Ministry of External Affairs' Fact Sheet on the India-US Cybersecurity Forum (see fn 58) details these agreements. Also see Cybersecurity: A Key to US-India Trade. Remarks by Kenneth I Juster, Under Secretary of Commerce, at the India-US Information Security Summit, New Delhi, 12 October, 2004, http://2001-2009.state.gov/p/sca/rls/rm/37039.htm.

This was visible when India would work hard towards de-hyphenating some of its most important bilateral relationships from Pakistan. Much of the post-Vajpayee era engagement with the US would see India's Foreign Service officers make a case that India should not be equated to Pakistan, and instead, be treated as an emerging global power since it already had a much bigger economy and was the world's largest democracy, unlike Pakistan. Seen in the light of India's discernible shift in foreign policy since 1991 which we examined earlier,[65] this created an added emphasis on 'sovereignty' as a major driver of New Delhi's international outreach. It would also further set India's foreign policy on to the path of using its bilateral or multilateral diplomatic clout to address bigger multilateral regimes.

Ironically, Pakistan's foreign policy would try and drag in India on most of its foreign policy postures on multilateral forums, such as the UN or the Organisation of Islamic Countries (OIC), with a mandatory mention of Kashmir and/or attempts to use India's gains – such as the nuclear deal with the US – to try and get similar bilateral deals.

The renewed engagements between India and the US were also partially influenced by the views that New Delhi and Washington shared on the Al Qaeda attack of 9/11. Since 1990, when New Delhi had combated terror attacks in Jammu and Kashmir, it had sought Washington's active role in reigning in what it perceived to be Pakistan's involvement in sponsoring acts of terror. This was a consistent theme that would be reflected repeatedly by subsequent Indian regimes, even though they emerged from different political dispensations.[66] But after 9/11, this relationship would undergo a significant change as terrorism became a common concern, leading to greater synergy on issues such as intelligence-sharing, and more aligned views on terrorism.

d. From Bilateral Engagements to Multilateral Gains?

A significant fall-out of the 2000 and 2001 agreements would be repeated assurances from the US government that it would support India's membership in previously restrictive technology-denial regimes like the Wassenaar Arrangement. In November 2010, the US Deputy National Security Advisor for International Economic Measures, Michael Froman, accompanying President Barrack Obama on a bilateral visit, stated that he was ready to support India's inclusion in the Wassenaar Arrangement. He clearly stated:

> the United States will support India's full membership in the four multilateral export control regimes. These are the Nuclear Suppliers Group (NSG); the MTCR; the Australia Group; and the Wassenaar Arrangement.

This position has since been repeated, with New Delhi viewing Washington DC's cooperation as a key stepping stone to joining multilateral regimes. On a bilateral visit to the US, Prime Minister Modi and President Obama once again reiterated their intention to cooperate in getting India on board multilateral regimes such as the MTCR and Wassenaar Arrangement and even on India's long-standing demand to be included as a permanent member of the UN Security Council.

- [65] See section 3(a) of this paper.
- [66] Rhode, David (2002). India Renews Call for US to Declare Pakistan a Terrorist State. *New York Times*, 17 July, http://www.nytimes.com/2002/07/17/world/india-renews-call-for-us-to-declare-pakistan-a-terrorist-state.html.
- [67] Kimball, Daryl G (2010). Obama's Message to India: Proliferation Violations Don't Have Consequences. *Arms Control Now*, 6 November, http://armscontrolnow.org/2010/11/06/obamas-message-to-india-proliferation-violations-dont-have-consequences/.
- [68] Joint Statement during the Visit of Prime Minister to USA. New Delhi, Ministry of External Affairs, 30 September 2014, http://www.mea.gov.in/bilateral-documents.htm?dtl/24051/Joint+Statement+during+the+visit+of+Prime+Minister+to+USA.

What the above highlights once again is how India has consistently aimed to leverage its bilateral relationship with the US to gain admittance into other multilateral regimes. New Delhi's calculation is hinged on building a robust bilateral relationship with the US, which, in turn, will use its clout to get it to the global high table. Washington DC's public endorsement of New Delhi's stance helps greatly in that sense. Yet, at times contradictory and confounding, India would both oppose and engage with the US at the same time. In creating this arrangement, it drew upon the pragmatic argument that if India needed to gain a foothold in the international Internet governance debates, it needed the US on its side, without diluting the traditional suspicions that India harboured.

Beyond its bilateral relationships, India has also been leveraging multilateral bodies that it has helped create to influence issues related to technology and security. This is reflected in India's keenness to use IBSA (a grouping of India, Brazil and South Africa – a reduced version of BRICS without China and Russia) to issue joint statements on 'enhanced cooperation' that will enable 'governments on an equal footing'.[69] Indeed, New Delhi continues to emphasise 'the need for global cooperation to ensure that [the] Internet continues to be a free and secure medium for the whole world'.[70]

This is also visible from the fact that India's 'sovereignty' emphasis in its post-1991 foreign policy closely matches that of its BRICS partners, Russia and China. So far, Internet governance has seen a 'commitment to the rule of law (domestically and internationally), even to the point of considering a conditional view of sovereignty, along with a multilateral cooperation of the states'.[71] However, Russia, China and India have, based on their historical antecedents, agreed in the past on an emphasis on 'great power privilege in the operation of the international system'.[72] Their view 'entails a strong rather than conditional interpretation of sovereignty' and is 'based on hierarchical state-society relations and limited or non-existent stakeholder consultation'.[73] As has been pointed out earlier, India has traditionally identified with less consultation and a more central role being attributed to the state, and even though it has now declared formal support for the multistakeholder approach in Internet governance, this doesn't seem to have affected this belief that it shares with its BRICS partners – at least not where cybersecurity is concerned.[74]

• 69. Statement by India, Delivered by Ambassador Dilip Sinha, Permanent Representative of India to UN in Geneva, at the UNCSTD Open Meeting on Enhanced Cooperation Pertaining to the Internet. Geneva, Permanent Mission of India to the UN, 18 May 2012, http://www.pmindiaun.org/pages.php?id=839.
• 70. *Ibid.*
• 71. DeNardis, Laura and Mark Raymond (2013). Thinking Clearly About Multistakeholder Internet Governance. Paper presented at the 8th Annual GigaNet Symposium, Bali, 21 October, pp. 14-15.
• 72. *Ibid.*
• 73. *Ibid.*
• 74. Kovacs, Anja (2015). Opportunism or Glasnost? India's Embrace of Multistakeholderism in Internet Governance. New Delhi, Internet Democracy Project, 20 September, https://internetdemocracy.in/2015/09/opportunism-or-glasnost/.
• 75. IANS (2015). India Fails to Get MTCR Membership but Wins Wide Support. *Business Standard*, 12 October, http://www.business-standard.com/article/news-ians/india-fails-to-get-mtcr-membership-but-wins-wide-support-lead-updating-115101200721_1.html.

The fact that India has tried, in various ways, to gain membership but has failed[75] has not dampened its resolve for a seat at the multilateral forums that matter to its security concerns and ambitions. Naturally, therefore, New Delhi has always responded positively to pronouncements such as those by Mr. Froman or President Obama, mentioned above, and has consistently welcomed them.[76]

In the next section, the intersection between terrorism and India's cybersecurity concerns is examined in more detailed.

• [76] Joint Statement 2012 US-India Strategic Dialogue. Washington DC, Embassy of India, no date, https://www.indianembassy.org/archives_details.php?nid=1830.

4. Terrorism, Law and Order as Drivers of the Debate on Cybersecurity

In 2012, a United Nations report on 'The Use of the Internet for Terrorist Purposes'[77] noted that:

> the benefits of Internet technology are numerous, starting with its unique suitability for sharing information and ideas, which is recognised as a fundamental human right. It must also be recognised, however, that the same technology that facilitates such communication can also be exploited for the purposes of terrorism. The use of the Internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism.

For India, the Internet has indeed been at once a major opportunity as well as a security nightmare. As explained earlier,[78] terrorism has in fact become the overarching paradigm for India's cybersecurity concerns.

a. Law and Order, Terrorism and Technology in India

India's concerns about the intersection of technology and terrorism have been accentuated with the proliferation of communication tools by terrorists using Internet-based platforms. The attack on Mumbai by Lashkar-e-Taiba (LeT) on November 26, 2008 illustrated how the terrorist-handlers based out of Karachi, Pakistan, used Voice over Internet Protocol (VoIP)[79] to direct the attack on key targets in Mumbai.

India's Law Enforcement Agencies (LEAs) have repeatedly cited the advent of the Internet and specifically social media, as one of the key challenges for dealing with law and order issues. In September 2013, when communal riots broke out in the district of Muzaffarnagar in India's most populous state of Uttar Pradesh (UP), the state police immediately blamed social media for 'inflaming hatred between the warring communities'.[80] A senior state police officer named 'Facebook, WhatsApp, Twitter' at a press conference just after the riots broke out. 'Fear and distrust between communities' he said, was being spread 'using' social media. He also pointed out that

> one specific video (being used to promote violence) which is very popular on social media, is not related to any incident in western UP and was uploaded on YouTube. [We believe] it belongs from an incident that took place outside India.

At the annual conference of all police chiefs in India, a month later, the UP state police made a detailed presentation to their counter-parts pointing out how social media was being 'abused', and repeated letters to corporations like Google and Facebook did not yield any results. In some ways, the current NSA, Mr. Ajit Doval would reflect the same views, as detailed in the introduction to this paper.

- [77] UNODC (2012). *The Use of the Internet for Terrorist Purposes*. New York: United Nations. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.
- [78] See section 3(b) and 3(c).
- [79] PTI (2009). VoIP used by 26/11 planners. 150 test calls made before attack. *India Today*, 18 August, http://indiatoday.intoday.in/story/VOIP+used+by+26-11+planners,+150+test+calls+made+before+attack/1/57314.html.
- [80] See press conference by Ashish Gupta, Inspector General of Police, Special Task Force, Uttar Pradesh Police, September 8, 2013 (at 2 minutes, 30 seconds onwards), https://www.youtube.com/watch?v=qnYfLf1HJK8.

While India has combatted terrorism through the 1980s in various forms, it faced a major challenge after the local population in the Kashmir Valley began violent protests after a large scale rigging of the local state elections was discovered just before the start of 1990. The state of Jammu and Kashmir has remained a major flash point between India and Pakistan since Independence, leading to four major wars. India has argued throughout that Pakistan has consistently used asymmetric forces against India by covertly supporting terrorist groups. The challenge posed by terrorism post-1990 meant that India also had to begin to grapple with various kinds of security challenges largely centred on secure communication technologies used by these terrorist groups.

The first major use of Internet-based communication tools by terrorists was discovered by Indian security agencies in 2006, after a little-known outfit going by the name of the Indian Mujahideen (IM)[81] carried out a series of bomb attacks across several prominent Indian cities, including Delhi and Mumbai.

The investigations into the IM terror attacks revealed that attacks had been planned over secure online communication channels.[82] This case was unique for investigators when they began to track the messages that had been sent by the IM. The tracing of the IP addresses led them to an open Wi-Fi network, which had been used by the terrorists to send their messages and ensure that they couldn't be tracked.

Subsequently, the IM improvised when they learnt that their MS Word documents could be traced. Instead, they began to send their documents as PDFs, a clear indication that the group was learning to hide its tracks between attacks.[83] Investigations would later reveal that the group was also using encrypted email accounts that would be deleted if they weren't accessed every 24 hours. This ensured that investigators had a difficult time accessing online content or metadata to anticipate attacks. The terrorists also used proxy servers extensively to 'camouflage their geographical locations'.[84]

Extracts from the interrogation report[85] of one of the prominent leaders of the IM, Mohammed Ahmed Sidibapa Mohammed Zarar, better known as Yasin Bhatkal, also shows a new breed of Indian terrorists using the Internet for planning attacks around 2007.[86]

According to Bhatkal, specific Internet-related tasks were given to other members of the sleeper cell designated 'Bhatkal Group'. One person was designated to prepare 'claim emails', taking credit for the bomb attacks that would ensue, while another would look after finding open Wi-Fi networks that would be used to transmit the emails.[87] Bhatkal also discussed how fake passports were made to help him travel anonymously; a copy of the fake document was sent on Wikisend. In addition, www.fakemailgenerator.com was used 'for creation of fake email ids'. [88] Bhatkal refers to a plethora of email identities that he used frequently for planning attacks.

- [81] Terrorist Designations of the Indian Mujahideen. Media Note. Washington DC, Office of the Spokesperson, US Department of State, 15 September, 2011, http://www.state.gov/r/pa/prs/ps/2011/09/172442.htm.
- [82] Jaleel, Muzamil (2014). NIA Probe Shows IM Men Tech-Savvy; Used Proxy Servers, Complex Code to Chat. *Indian Express*, 4 July, http://indianexpress.com/article/india/india-others/nia-probe-shows-im-men-tech-savvy-used-proxy-servers-complex-code-to-chat/.
- [83] Interview with a senior Indian intelligence official on the strict condition of anonymity.
- [84] Jaleel, *op. cit*.
- [85] An interrogation report is an investigation document based on the questioning of an accused in the presence of a police officer. The interrogation report is an inadmissible document in a court under most Indian laws. It is mostly used to extract intelligence from the accused and should be viewed as such. This is a document which is restricted and not for public consumption.
- [86] Interrogation Report of Yasin Bhatkal. New Delhi, National Investigation Agency, 2014, p. 30.
- [87] *Ibid.*, p. 78.
- [88] *Ibid.*, p. 97.

The document then goes on to explain how the group used secure and encrypted online chat applications to avoid being identified by security and intelligence agencies before and after terrorist attacks had been carried out.

The terrorist attack on Mumbai on 26 November, 2008, would again prove to be a major challenge for Indian security agencies. The attack, carried out by members of the Pakistan-based terrorist group LeT would last for three days before Indian commandos cleared the attackers from three different sites. Over three days, Indian security agencies would intercept communication between the terrorists and their handlers, believed to be based out of Karachi, Pakistan. The initial delay in being able to identify where the terrorists were calling from would lead to a major setback in the counter-terrorism operations, but the VoIP logs would be a critical part of the evidence.[89]

The recent revelations from the Snowden-documents show that the British techint agency, Government Communications Headquarters (GCHQ) was monitoring the computer of the LeT's Zarar Shah, but did not inform its Indian intelligence counterparts.[90] This raised suspicions among Indian security officials that the West was not sympathetic to India's concerns on terrorism.[91] A news report, based on the Snowden revelations, stated that 'United States spy agencies also alerted their British counterparts, according to a senior American intelligence official. It is unclear if the warnings led to the targeting of Mr. Shah's communications, but by the fall of 2008, the British had found a way to monitor Lashkar's digital networks. So had the Indians. But until the attacks, one Indian official said, there was no communication between the two countries on the matter'.[92]

b. Multilateralism the Way Forward?

India has tried to address the challenges that its security agencies are faced with in the areas of law and order and terrorism in a variety of ways. In 2011, a petition was filed by Yahoo! India Pvt Ltd. against the Union of India in the Delhi High Court.[93] The petition records repeated demands for access to IP addresses and email content by the government, citing demands from the Intelligence Bureau (IB),[94] India's premier internal intelligence organisation. The petition records how the IB sought this data under section 28 of the Information Technology Act 2000, through the offices of the Controller of Certifying Authority (CCA) under the Department of Information Technology, Government of India.

More important for this paper, however, is that instances such as those detailed above have also sharpened India's approach favouring a multilateral approach to cybersecurity at the global level. In fact, for New Delhi, building a broad global coalition on security issues, both from an approach and treaty perspective, has been the corner stone of its foreign policy, especially when it impinges on its global security concerns, for almost two decades now. Thus, in September 1997, India became one of the early signatories to the International Convention for

- [89] Express News Service (2015). Enforcement Directorate Probe Finds Link between Hurriyat Leader, 26/11 Funds. *Indian Express*, 20 July, http://indianexpress.com/article/india/india-others/common-link-between-2611-financiers-jk-man-charged-by-enforcement-directorate/#sthash.JJGdmNrH.dpuf.
- [90] Glanz, James, Sebastian Rotella and David E Sanger (2014). In 2008 Mumbai Attacks, Piles of Spy Data, But an Uncompleted Puzzle. *New York Times*, 21 December, http://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html?_r=0.
- [91] Interviews with several serving intelligence and counter terrorism officials who spoke on the condition of strict anonymity confirmed this.
- [92] Glanz et al., *op. cit*.
- [93] CM Petition No. 17844 of 2011, filed by Yahoo! India Pvt. Ltd. in the High Court of Delhi, New Delhi.
- [94] The Intelligence Bureau is India's federal internal intelligence agency under the Union Ministry of Home Affairs. It is patterned on the UK's Security Service (MI5) and its Director is considered the country's top police officer, with a five-star ranking.

Suppression of Terrorist Bombings.[95] A year earlier, India had tabled a draft Comprehensive Convention on Terrorism, which it revised and resubmitted during the 55th UN General Assembly in 2000[96] and it has continued to press for it over the years.[97]

It is against this background then, that Minister Prasad's insistence, highlighted in the introduction to this paper, that security-related issues would continue to see a dominant role by the State as far as India is concerned, has to be understood. Mr. Prasad made this amply clear in the same message in which he announced India's change in policy to embrace multistakeholder approaches to Internet governance.[98] Security concerns have resulted in India grappling to have a greater say in the Internet governance space in the belief that it will have a more forceful voice using the multilateral approach.

In many cases, those concerns are centred around issues of online jurisdiction. For instance, if an online crime were to occur beyond India's territorial boundaries, but the evidence was present in servers in India, would the laws of other nations be applicable here? This is also complicated by the fact that Indian security officials frequently complain that getting data under the Mutual Legal Assistance Treaty (MLAT) has been a huge challenge. These issues are a recurring theme and a major reason for India's opposition to the Council of Europe's Convention on Cybercrime, better known as the Budapest Convention.

The Budapest Convention came into being on November 23, 2001 as a first multilateral effort by member signatories to address jurisdictional issues. Intended to create a 'common criminal policy aimed at the protection of society against cybercrime',[99] the convention also set the gold standard for cybersecurity – confidentiality, integrity and availability (CIA) of computer systems.

For India, the agreement, though beneficial at many levels, was, however, unacceptable. Taking a cue from Russia that the Convention was fatally flawed and could jeopardise issues of sovereignty,[100] India along with China and Brazil argued that a treaty negotiated by Europeans for themselves was clearly unacceptable to their aspirations and sovereignty.[101] While India generally opposes treaties that it has not been party to during the negotiation on the clauses, it was particularly opposed to the implications of clause 32 (b) of the Convention, which it deemed to be discriminatory. The clause refers to 'trans-border access to stored computer data with consent or where publicly available' and specifically states that a Party may, without the authorisation of another Party, 'access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system'.

- [95] United Nations International Convention for Suppression of Terrorist Bombings, New York, 15 December, 1997: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-9&chapter=18&lang=en.
- [96] Aust, Anthony (2001). Counter-Terrorism: A New Approach. The International Convention for the Suppression of the Financing of Terrorism. In JA Frowein and R Wolfrum (Eds.), *Max Planck Yearbook of United Nations Law*, 5: 285-306, http://www.mpil.de/files/pdf1/mpunyb_aust_5.pdf.
- [97] PTI (2015). India Calls for Early Adoption of Convention on Terrorism in the UN. Times of India, 15 October, http://timesofindia.indiatimes.com/india/India-calls-for-adoption-of-convention-on-terrorism-in-UN/articleshow/49379312.cms. Also see Anand, Arpita (2015). India in Global Governance: Engaging the Counter Terrorism Regime. Paper presented at the IDSA Fellows Seminar, New Delhi, 22 May, http://www.idsa.in/event/IndiainGlobalGovernance_aanant.
- [98] Samanta, *op. cit.*
- [99] See the Preamble to the Council of Europe's Convention on Cybercrime, Budapest, 23 November, 2001, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.
- [100] Security, International Cooperation and Cybersecurity: A Treaty Dialogue. Remarks by Boris Vasilev, Expert, Office of the Special Coordinator of the Ministry of Foreign Affairs, Russian Federation at CyFy, New Delhi, 2013, http://cyfy.org/speaker/boris-vasiliev/.
- [101] Grigsby, Alex (2014). Coming Soon: Another Country to Ratify Budapest Convention. New York, Council on Foreign Relations, 11 December, http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/. Also see Singh, Pratap Vikram (2013). India Won't Sign Budapest Pact on Cyber Security. *Governance Now*, 15 October, http://www.governancenow.com/news/regular-story/india-wont-sign-budapest-pact-cyber-security .

While echoing the worry that most servers are situated in the US as a reason for India's decision to not sign the convention,[102] India instead has consistently sought US involvement in pushing for establishing a root server in India[103] in the belief that it will give it much greater say and control over the Internet.[104] India has also tried to find redressal for its concerns by submitting a proposal in 2014 in the United Nations' International Telecommunications Union (ITU) to develop a 'public telecom network architecture that keeps traffic originating and terminating in the country/region and meant for the country/region, as well as address resolution relating to such traffic' local.[105] In this same draft resolution, India also requested the ITU Secretary-General to 'work with all other stakeholders, including international organisations, to make changes so that it is possible to discern the country location of a particular IP address'.[106] The proposal, despite being presented twice with modifications, did not find much support.

As mentioned in the introduction, in 2011, India had already proposed the establishment of a UN Committee on Internet-related Policies (CIRP). This proposal, too, did not receive much support.

While India had, thus, been pushing for a more multilateral approach to governing the Internet through new treaties and frameworks internationally, on the domestic front, it, however, continued to lack abysmally where cybersecurity was concerned. This, in turn, would also shape India's foreign policy posturing, as it sought to balance its internal inadequacies with a rapidly changing international environment deeply impacted by emerging Internet-based technologies.

- [102] Singh, *Ibid.*
- [103] Samanta, Pranab Dhal (2015). Internet Governance: US Considering India's Pitch to Locate 'Root server'. *Economic Times*, 3 September, http://articles.economictimes.indiatimes.com/2015-09-03/news/66178452_1_internet-governance-root-thirdlargest-internet-user-base.
- [104] Koshy, Jacob (2015). To Assert Global Clout, India wants Own Internet Root Server Like US. *Huffington Post India*, 3 October, http://www.huffingtonpost.in/2015/09/03/root-servers_n_8080896.html.
- [105] Kovacs, Anja (2015). *Reinterpreting Document 98: India's Proposals at the ITU Plenipot 2014 and the Evolution of Internet Governance*. New Delhi: Internet Democracy Project. https://internetdemocracy.in/reports/re-interpreting-document-98-indias-proposals-at-the-itu-plenipot-2014-and-the-evolution-of-internet-governance/.
- [106] *Ibid.*

5. Cybersecurity: National Policy, Statutes and Critical Information Infrastructure

In his seminal 2010 paper on 'Cyber Power',[107] Joseph Nye, a scholar with the Belfer Center for Science and International Affairs at the Harvard Kennedy School, pointed to the use of cyberspace to attain national objectives. Cyber power, he noted, can be used to 'produce preferred outcomes within cyberspace' and it can be used 'to produce preferred outcomes in other domains outside cyberspace'. This construct fits exactly with the vision that Indian policy makers have espoused and aspired for historically, as is evident from the previous sections of this paper. The fact that India will be one of the largest online markets in the world, and is the world's biggest democracy, work in its favour and can substantially buttress Nye's point about 'cyber power'.

However, to attain 'cyber power' a nation needs to overcome a series of challenges that are caused by either a lack of capacity, or by a set of legacy issues. Some of these apply to India. In 1978, an Indian economist, Professor Raj Krishna, coined the term 'Hindu rate of growth'[108] to describe the low rate of economic growth against the back drop of a predominantly socialist economy. This theory continues to be used to understand the lack of progress on most issues in India, despite its post-1990 economic liberalisation that has witnessed a surge in its aspirations, individually and collectively. Thus, the road to developing a framework for cybersecurity in India has been a similarly slow and torturous process.

This slow pace of evolution in India's Information and Communications Technology (ICT) framework has impacted its policies abroad. While India lacked the wherewithal to address the domestic issue, it sought to make up internationally by exercising its political clout and building up alliances as discussed earlier.

Till the specific and statutory role of government agencies was spelt out in section 70 (A) and 70 (B) of the IT Act (Amended 2008), the bulk of the India's cybersecurity concerns were the responsibility of one single agency: the Computer Emergency Response Team – India (CERT-IN). Set up in 2004,[109] it mapped India's cybersecurity posture and was the sole point of contact for expertise on these matters to the government. Post its statutory role prescribed in the IT Act, it continues to play a dominant role in the cybersecurity space and serves as the single point of contact for international cooperation with other CERTS.

In more recent times, additional building blocks have been added to the domestic ecosystem. Three initiatives require attention in particular.

- [107] Nye, Joseph S (2010). Cyber Power. Cambridge, MA, Belfer Center for Science and International Affairs, Harvard Kennedy School, May, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. This framework adequately mirrors India's stated foreign policy aspirations and thinking on the lines of the sovereignty framework.
- [108] Siva, Meera (2013). What's a Hindu Rate of Growth. *The Hindu BusinessLine*, 8 June, http://www.thehindubusinessline.com/portfolio/technically/whats-a-hindu-rate-of-growth/article4795173.ece.
- [109] For more information on CERT-IN, please see its website, http://www.cert-in.org.in/.

a. The IT Act

While the Information Technology Act, 2000[110] had rudimentary clauses for protecting data, there was no comprehensive clause that looked at cybersecurity per se from a statutory perspective. This is because India was still at a nascent stage of its journey of embracing the Internet, and the computerisation of large government networks and processes was just beginning. The IT Act initially was actually drawn up to protect the business interests of the IT-enabled services (ITES)[111] industry. But clearly, the initial version of the IT Act failed to fully appreciate the power of technology and its impact in the years to come.

The fact that the original IT Act failed to mention cybersecurity is an indication of the inability of Indian law makers to fully grapple with the sudden growth of the IT and ITES industries. The original IT Act of 2000 has a rudimentary framework to address computer-related issues and appointed the CCA[112] as the major point-person for most data security related procedures and functions, emphasising data security, rather than cybersecurity. In fact, the Act did not mention cybersecurity even once, and had limited scope in looking at the issue of security. However, the Act did refer to ‘hacking’, defining it as an

> intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.[113]

The following years, however, showed that cyber risks rose dramatically as more systems began to be included in the ICT framework. As data[114] shows, the increase in threats and attacks grew in quantum leaps:

S. No	Event	2006 - 2007	2014 - 2015
1	Security Incidents Handled	552	130338
2	Security Alerts Issued	48	13
3	Advisories Published	50	69
4	Vulnerability Notes Published	138	290
5	Indian Websites Defaced	5211	25037
6	Open Proxy Servers Tracked	1837	2408
7	BOT Infected Systems	No Data Generated	7728408

Table 1. Growth in select cybersecurity threats, 2006-2007 to 2014-2015

- [110] The Information Technology Act, 2000. New Delhi, Gazette of India, 9 June, 2000, http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf.
- [111] Chanda, Rupa (2008). Trade in IT and ITES: Issues and Concerns in India-EU Trade and Investment Agreement. New Delhi, ICRIER, September, pp. 32-33. http://wtocentre.iift.ac.in/EU%20BTIA/EU%20BTIA/Report%20on%20IT-ITES-%20India-EU%20BTIA.pdf
- [112] Section 17 of the IT Act, 2000, appointed and defined the role of the CCA.
- [113] In addition to defining hacking, section 66 (1) of the IT Act, 2000, prescribed a punishment for hacking of imprisonment for up to 3 years and a fine.
- [114] See CERT-IN Annual reports, available on the website, http://www.cert-in.org.in/.

This deeply impacted the national cybersecurity policy framework. In recognition of the rise in cyber vulnerabilities, threats and attacks and the emergence of new threats, the statutory framework was reworked with significant additions to the Act in 2008, with the aim of establishing a national cybersecurity policy framework. The Act now defined 'critical information infrastructure' (CII), through an amendment to section 70, as

> those facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation.

In addition, sections 70A and 70B envisaged the creation of particular agencies with clearly-defined roles for implementing cybersecurity measures. While section 70B designated the existing CERT-IN, section 70A laid down the mandate for the creation of a new agency to protect sectors designated as CII. The new agency was the National Critical Information Infrastructure Protection Centre (NCIIPC) and would be created through an official gazette notification issued by the Government of India.

b. NCIIPC

Although the IT Act was amended in 2008, the Gazette Notification that established the NCIIPC only came on 16 January 2014, almost six years later. NCIIPC's mission is

> to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders

and with a vision 'to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country.[115]

Though the establishment of NCIIPC as such is a positive step forward, several shortcomings continue to mark its implementation.

First, the sectors that have been designated as coming under NCIIPC's purview include defence; the banking and financial sector; ICT and telecommunication; transportation; power; energy; and the Ministries of Home Affairs, External Affairs, Heavy Industries and Niti Ayog (the erstwhile Planning Commission). These were chosen on the basis[116] of a combination of factors, including functionality; criticality of scale; degree of complementarities; political, economic, social and strategic value; and time duration – with the understanding that the list would be revised periodically.

However, as argued elsewhere, the method used to determine the criticality rating of each sector is severely lacking.[117] Rather than drawing on a comprehensive risk assessment that also factors in intent, capability and timing of an intended attack, the criticality rating of each sector at the moment solely depends on the number of interdependencies that a sector has.[118] Using this interdependency map, NCIIPC designated the power sector as the most critical. But other sectors, though with less interdependencies, might be more critical depending on the circumstances.

- [115] Please see the NCIIPC Digital Repository: https://nciipc.gov.in/.
- [116] NCIIPC (2013). *Guidelines for the Protection of Critical Information Infrastructure, Version 1.0, June 2013*. New Delhi: NCIIPC, p. 6, http://perry4law.org/cecsrdi/wp-content/uploads/2013/12/Guidelines-For-Protection-Of-National-Critical-Information-Infrastructure.pdf.
- [117] Datta, Saikat (2016). *Defending India's Critical Information Infrastructure: The Development and Role of the National Critical Information Infrastructure Protection Centre (NCIIPC)*. New Delhi: Internet Democracy Project.
- [118] Interview with Munish Sharma, Institute for Defence Studies and Analyses (IDSA), Delhi, 4 November, 2015. Mr. Sharma was part of the NCIIPC team that designed the CII interdependency map.

For instance, in the event of a war, a forward air force base may still be able to function without power supply, using backup generators using conventional fuel. However, a cyberattack on its mission computers and radar coverage could have a far more debilitating effect, even though, as a sector, it has a far smaller number of interdependencies than the power sector. In fact, sectors such as defence will remain prime targets of attacks, as has been amply demonstrated in the past.[119]

Another major deficiency in the current CII framework is the absence of sector-specific guidelines and standard operating procedures (SoPs) in the event of a cyberthreat or attack. The creation of sector-specific plans (SPP) ensures the development of 'a trusted relationship and true partnership between the government and the industry',[120] by setting several goals for industry and government to be achieved within a time-bound framework. While general guidelines have laid down a preliminary road map, the sectors identified by it are yet to evolve their specific charters. This creates a major vulnerability that is yet to be addressed. [121]

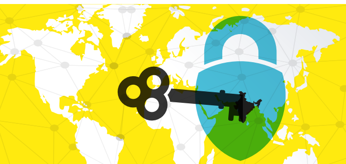
Currently, NCIIPC follows a framework of conducting a 'vulnerability/threat/risk' analysis (V/T/R analysis) for mapping the level of vulnerability of each designated sector during 'steady state operations', or the routine operations of an installation that follow a regular schedule.[122] Based on the V/T/R analysis, NCIIPC carries out a control configuration audit and brings in change management to mitigate any vulnerabilities.

The audit maps the various controlling nodes of the sector's 'operational technology' (OT) or 'supervisory control data acquisition' (SCADA) systems that are critical to running automated plant operations in large-scale industrial plants. This audit of the control systems helps NCIIPC to map out various vulnerabilities, such as the logical and physical separation of OT/SCADA systems from the Internet and other information security measures that can significantly reduce risks and the threat of cyberattacks. While NCIIPC has so far approached the banking and power sectors for its initial projects, it is yet to look at the other sectors at this time.

It is clear, then, that India's CII protection framework continues to be a work in progress. Indeed, the NCIIPC guidelines acknowledge that 'time duration' is critical to mapping CIIs, and contain a stated aim to review each sector periodically. For the moment, however, the 2013 Guidelines continue to hold true.[123] Interestingly, the Gazette notification for NCIIPC came in January 2014, much after the NCIIPC guidelines had been created. In other words, the guidelines were developed when NCIIPC was yet to be born. Perhaps, a reason for the gaps in the evolution of a national CII framework could be attributed to the delay between legislation and implementation.

Finally, a comment on NCIIPC's command and control structure. The NCIIPC was placed under the National Technical Research Organisation (NTRO), a technical intelligence agency created as a part of India's security architecture reforms in the aftermath of the Kargil war with Pakistan.[124] The NTRO sought to incorporate and consolidate all the technical intelligence capabilities under one roof and deploy them for defensive and offensive operations.

- [119] The cyberattack on the Joint Strike Fighter programme of the United States in late 2006 is one good illustration of this. See Harris, Shane (2014). *@War: The Rise of Cyber Warfare. London: Hachette.*
- [120] US Department of Homeland Security and US Department of Energy (2010). *Energy-Sector Specific Plan: An Annexe to the National Infrastructure Protection Plan 2010*. Washington DC: US Department of Homeland Security and US Department of Energy, p. i.
- [121] Datta, Saikat (2015). The Deadly New Age War. *The Hindu*, 23 June, http://www.thehindu.com/opinion/op-ed/the-deadly-new-age-war/article7342982.ece.
- [122] Presentation on NCIIPC methodology by Director, NCIIPC at a CII workshop. Delhi, 4 November, 2014.
- [123] Interview with Munish Sharma, IDSA, Delhi, 4 November, 2015.
- [124] Chen, Liu CHuen (2015). What You Should Be Knowing about the Kargil War. *India Today*, 26 July, http://indiatoday.intoday.in/story/kargil-war-vijay-diwas-facts/1/454125.html.



While it has not been clearly explained why the task of protecting CII fell upon an intelligence agency, it was speculated that since cyberspace fell within NTRO's charter, the agency was deemed fit to oversee NCIIPC's functioning. However, protecting CII is a shared responsibility, with a major role for the private sector. This means that there is a need to create joint structures and SoPs to effectively deal with threats and exigencies, as and when they occur. A designated intelligence agency will have several issues with sharing of its SoPs or of information that could jeopardise its other ongoing operations, and therefore, it could be restricted in effectively carrying out its CII tasks. The same challenges also prevent the agency from naturally taking a full-fledged multistakeholder route, the need for which is inherent in a CII framework since many of the designated critical sectors lie in the private domain. In other countries, the protection of critical information infrastructure is situated with a civilian agency that works openly and without the restrictions natural to an intelligence organisation. In the US the responsibility lies with the Department of Homeland Security, along with sector-specific departments.

It has to be recognised, however, that NCIIPC does acknowledge the role of others stakeholders, with the draft framework stating that 'protection of CII involves a multi stakeholder approach'.[125] The draft guidelines under preparation recognises five principle stakeholders:

1. The CII owner
2. Service providers to the CII
3. NCIIPC
4. CERT-IN
5. Law enforcement agencies

Although this may still fall short of the commonly accepted norm of a multistakeholder approach, it does indicate a gradual recognition of the new realities of Internet governance, despite India's traditional emphasis on a multilateral approach, especially with regard to security issues.

c. National Cyber Security Policy 2013

The National Cyber Security Policy, promulgated in June 2013, built a cybersecurity framework that goes beyond CII. Its stated objectives included a mission to 'generate adequate trust and confidence in IT systems'[126] and to create a workforce of '500,000 professionals skilled in cybersecurity in the next 5 years'.[127]

Among the strategies that the National Cyber Security Policy 2013 describes to achieve its objectives are:

1. **Creating a secure cyber eco-system**
2. **Creating an assurance framework**
3. **Encouraging open standards**
4. **Strengthening the regulatory framework**
5. **Creating early warning systems, vulnerability management and response to security threats**
6. **Securing e-governance spaces**
7. **Protection and resilience of CII**
8. **Promotion and research & development of CII**
9. **Reducing supply chain risks**
10. **Human resource development**
11. **Creating cybersecurity awareness**
12. **Developing effective public-private partnerships**
13. **Information sharing and cooperation**
14. **Prioritised approach for implementation**
15. **Operationalisation of the policy**

- [125] NCIIPC (2015). *Draft on Framework for Protection of Critical Information Infrastructure*. New Delhi: NCIIPC. This document is currently under development by NCIIPC, and was forwarded to stakeholders for comments and suggestions.
- [126] National Cyber Security Policy. New Delhi, Department of Information Technology, Government of India, 2 June, 2012, p.3 ('Objectives'), http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.
- [127] *Ibid.*, p. 4.

Where the National Cyber Security Policy falls short is to understand the nature of next-generation-threats, which are complex and resemble 'Black Swan' events – disconnected at some levels, and yet connected enough to create critical failures.

Understanding of these has been necessitated by the rise of Next Generation Networks (NGN), packet-based networks, which are 'able to provide services including telecommunication services and able to use multiple broadband, quality of service-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies'.[128] These have been recognised as a major vulnerability by the Government of India.[129]

The arrival of NGNs and technologies has also given concomitant rise to the birth of 'Next Generation Security Threats' that are at times orchestrated, or at times driven by faulty algorithms. For instance, the 2008 assault on the Baku-Tbilsi-Ceyhan pipeline in Eastern Turkey was initially believed to be a traditional physical terror attack by security agencies. However, subsequent investigations have established it as an act of 'cyberwar'.[130] Although information about the attack in the open domain is still sketchy, these investigations revealed that vulnerabilities in the software running the IP-based security cameras were exploited by hackers who 'super-pressurised the crude oil in the line'[131] to cause a series of devastating explosions.

Clearly, such complex attacks have been enabled by the emergence of cyberspace. Yet, despite the creation of a national policy, these have failed to attract the urgency from Indian policy makers that they deserve.

Analysts and intelligence officials also see the emergence of the militant outfit from the Syrian civil war, the ISIS (a.k.a. Dae'sh, Islamic State, etc.), and its use of social media as a fascinating case study of a 'Next Generation Security Threat'[132] which, although traditional at one level, has grown in complexity, reach and ability due to the rise of NGNs.[133]

d. Too little, too late?

The fact that India took aggressive international positions because it lacked the domestic wherewithal is demonstrated in the official address by Arun Shourie, the then Minister for Telecom and Information Technology, at the World Summit on the Information Society (WSIS) in Geneva, in 2003. Shourie was clear that the rapidly modernising economies would increasingly depend on greater computerisation, which meant that they would be increasingly vulnerable to 'information technology' being used to 'disrupt'[134] these new integrated systems. The national cybersecurity policy and the national critical information infrastructure mandate emerged more than a decade after Shourie's impassioned speech for greater sensitivity to technology that could 'disrupt' systems, and therefore economies and even then, as this sections shows, is suffering from considerable shortcomings.

[128] Definition of NGN. Geneva, ITU Study Group 13,2004, https://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html.

[129] See Rai, Gulshan (n.d.). Cyber Security and Critical Information Infrastructure. New Delhi, Indian Computer Emergency Response Team (CERT-IN), no date, http://cris.org.in/CRIS/PDF/Cyber_Security_and_Critical_Information_Infrastructure-CERTIN.pdf.

[130] Robertson, Jordan and Michael Riley (2014). Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. *Bloomberg*, 10 December, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

[131] *Ibid*.

[132] Goodman, Marc (2015). *Future Crimes: A Journey to the Dark Side of Technology – And How to Survive It*. London: Bantam Press, pp. 317-348.

[133] Berger, JM (2014). How ISIS Games Twitter. *The Atlantic*, 16 June, http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[134] Statement by H.E. Mr. Arun Shourie, Minister for Information Technology, Communications, and Privatisation, Government of India, at the World Summit on Information Society. Geneva, 11 December, 2003, http://www.itu.int/net/wsis/geneva/coverage/statements/india/in.html.

Conclusion

India today stands at the cusp of a major opportunity. As has been brought out in this paper, India has always viewed technology as a means to not only make up for lost time on economic and political progress, but also to arrive on the world stage as a major power. However, the disconnect between India's aspirations and the actual capacity, be it technological or otherwise, has prevented it from achieving its true potential.

This is a framework that plays out consistently. If the Bhabha Committee recommends rapid computerisation and automation in 1963, the Dandekar Committee recommends the opposite a decade later. Even as mass computerisation is recognised as a successful means of delivery of public services (such as the computerisation of the railways) in the 1980s, it takes more than a decade to give information technology a statutory framework. Even then, there is a gap in recognising security as a major concern and it takes another eight years before a comprehensive legal framework for cybersecurity emerges. Obviously, such gaps not only delay processes, they also defeat the stated aspiration of harnessing technology as a means to achieve great power status.

This is starkly evident as India continues to search for options on its evolving position on Internet governance. It has been deeply influenced by the overarching footprint of its security concerns. This precludes its economic well-being on one hand, as well as its position in the current global order, which it intends to influence using technology and diplomacy.

As has been articulated in this paper, there are historical reasons for India's predilection towards using a government-to-government approach (both bilateral and multilateral), as opposed to a multistakeholder approach. Even though India has formally adopted a multistakeholder approach, it is unlikely that this will be applied to the security concerns that drive the Internet governance debate in India. At best, India will look at the private sector for advice or capacity-building. But the chances that academia or civil society stakeholders will also be involved in these debates remain limited.

However, this could change significantly as India builds more capacity as a producer of the Internet rather than just a consumer. As e-commerce and e-governance takes root in India, it is also enhancing connectivity and bringing in more people into the Internet every day. This is creating a volume of stakeholders who are vocal and have the ability to use their digital footprint to impact public policy in a major way. This was clearly visible in the recent debates on net neutrality and the campaign against Facebook's Internet.Org (a.k.a. Free Basics) as well as differential pricing and zero rating. These debates saw millions of online submissions being made by stakeholders on both sides to the Telecom Regulatory Authority of India (TRAI) in a bid to press home their point of view in support of either side. This is a clear indication that there is a silent majority that is beginning to speak up and make an impact. Clearly, they will shape the future and in turn, ensure that the multistakeholder approach to Internet governance is here to stay. It is just a matter of time.

The Way Forward

Many of these gaps can be quickly addressed, if the government, as the pre-dominant player and the trusted arbitrator, recognises the role of multiple stakeholders who can help India achieve its true potential. To start with, there are several stakeholders within the government who need to work far more closely than their current protocol allows.

This means all stakeholders within the government – be it the Prime Minister's Office, the National Security Council and its Secretariat, the Ministry of Communications and Information Technology, the Ministries of Law and Home Affairs, the security agencies, etc. – establish institutional mechanisms to work with each other rather than at cross-purposes. This seems to have been addressed to an extent but there remains a vast scope for improvement.

That said, there is a much bigger set of stakeholders who reside outside the government. They wield varying degrees of influence and capacity, but are all critical for meeting India's true potential to play a leading role on the global stage. In many ways, if the collapse of the Soviet Union created a new world order, then the advent of the World Wide Web has now, once again, ushered in a completely new framework for the next world order.

This means that India needs to harness every stakeholder at its disposal to achieve its true potential, while this new global framework is still evolving. These stakeholders – the private sector, civil society, academia and the technical community – are all waiting to be tapped and used to bring about a new paradigm that has enormous benefits for India. For a number of historical reasons, as documented in detail in this paper, these groups of stakeholders continue to be outside the realm of policy making in India, which works to its disadvantage. If this great set of resources/stakeholders can be harnessed in a meaningful manner, then India's stated objective to emerge as a global power can be achieved.

CYBERSECURITY, INTERNET GOVERNANCE & INDIA'S FOREIGN POLICY: HISTORICAL ANTECEDENTS

India's stances in global Internet governance debates have often been noted, and criticised, for their strong preference for multilateral models of engagements, as different from the multistakeholder approaches that are so well-established in the field. But where does this predilection towards multilateral engagement come from? This paper maps the economic, political and historical antecedents of India's evolving positions on global Internet governance as they are shaped by its concerns on cybersecurity, by its domestic context and by its overall influence on global events as they unfold. Through this analysis, the paper hopes to contribute to a greater understanding of both India's cybersecurity concerns and of the ways in which India approaches global Internet governance as it has emerged as one possible venue to address these pressing issues

internet
democracy
project

SAIKAT DATTA