seminar


india
and
digital
world
making
july
2020
www.ipindia.gov.in
seminar

731

INDIA & DIGITAL WORLDMAKING

a symposium on

India and the global

governance of technology

symposium participants

The problem

RAPID globalization of firms and markets has inexorably accelerated through technology. As was the case in previous eras of globalization, countries will have to devise new governance mechanisms, rules and standards to regulate new patterns of technological interactions between states and non-state actors alike. Traditional rules are being questioned, reframed and broken. Private actors, both multinational corporations and 'cyber mercenaries' are acquiring increasing importance and relevance. Existing and emerging international regimes and frameworks are under pressure to mobilize countries to create rules to address problems wrought by new technologies related to artificial intelligence, big data, social media, automation, drones, autonomous weapons and malware incursions.

The growing chasm between the pace of technological change and their implications must be addressed through renewed international cooperation or by negotiating global rules and norms that could minimize their adverse effects. Traditional global governance frameworks have attempted to forge rules around the governance of emerging technologies. The United Nations is involved through the UN Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG) that seek to regulate state behaviour in cyberspace. Regimes like the WTO are discussing issues related to the digital economy, e-commerce and data. Multi-stakeholder frameworks like the Paris Call for trust and security in cyberspace, Christchurch call to eliminate terrorist and violent extremist content and the Prague 5G conference have surfaced, out of necessity, to manage issues under their remit.

India stands at the forefront of these debates for two reasons. First, India has a clear interest in shaping international technology rules to accelerate domestic technological transformations that have become integral to its economic trajectory. India is going through a period of extraordinary technological change measured through increasing rates of digitization, record digital penetration and use of the internet to structure patterns of political, commercial and social interaction. The most prominent marker of India's technological transition has been the smartphone around which several major initiatives like 'Digital India' have been devised. Besides Digital India, the momentum around and interest in the public development of technology has led to an array of targeted programmes around artificial intelligence, drones, blockchain, quantum computing and big data. No doubt, these technologies are having massive effects internally which are being addressed through domes-

tic laws and policies. India has an obligation to shape international rules covering these technologies like 5G development, artificial intelligence, data and digital taxation are vital to ensure they mesh with domestic rules. Incongruence or passivity vis-à-vis digital rulemaking globally will raise costs for Indian firms who have to readjust their business practices and models and New Delhi that will have to reorient its regulatory approach.

Broadly, international rules covering these emerging technologies could also affect how India chooses to regulate technology issues, specifically whether domestic rules would privilege the state or private sector. Thus far, India has placed the state at the heart of the current 'technological turn.' Yet, the dominant role of the state has only intensified questions around the use of these technologies that enhance state power relative to that of citizens. Several technology issues like data, 5G, autonomous weapons, artificial intelligence and digital taxation considered in this *Seminar* issue deal directly with how the Indian state should regulate technologies for the 'public good'. That said, the state is not alone here. The articles in this issue also point to a 'crowded' policy space where India's positions are being shaped and reshaped by private interests in India and those abroad whose material fates are tied to how Indian policymakers opt to regulate technologies.

Second, global technology debates matter for India because the costs of not actively engaging in shaping or influencing digital rulemaking are high. More than ever, India's economic, political and security future(s) hinge on procuring, availing and deploying technologies and having robust rules that accelerate the empowerment of India's vast demographics while deterring their use against India's strategic objectives. Existing conflicts and rivalries get mapped onto technologies as India's competitors rely on cyberspace to target India through cyber attacks or by closing the space India has to develop its own technologies and leverage global supply chains in that cause. Symmetric international rules that set clear and accountable standards matter when developing and deploying technologies. The alternative is living in a technological era with little clout, an untenable option for a country that will become more, not less, reliant on technologies to advance economic and security interests.

The articles in this 'Seminar' issue cover the teeming landscape of global governance mechanisms and arrangements, some formal and others inchoate, that seek to establish new norms, rules and standards

that countries can endorse and internalize to develop and deploy technologies for economic growth and minimize their pernicious social and political effects. Finding a balance between these objectives will not be easy but countries like India have no choice.

Galvanizing global consensus on a legal regime to foster responsible state behaviour in cyberspace has proved to be a tough challenge. In a detailed articulation of the various multilateral, multi-stakeholder and private sector efforts aimed at fostering this consensus, Gunjan Chawla argues that India's unwavering commitment to preserve its sovereign interests in this fragmented governance space is clear. Global governance is imperative for restraining, if not halting, the disruptive effects of weaponized cyberspace. Trisha Ray argues that India's 'long game' on Autonomous Weapons Systems adopts a similar trajectory. Evaluating India's stances on AWS, Ray believes that India's strategy seeks to protect national security interests while trying to balance regulation both with AI driven growth and India's democratic obligations.

While some countries have rushed to set up robust frameworks for 5G development and investment, India, as Manoj Kewalramani points out has opted to go slow. Kewalramani believes India's caution is driven by various factors including the economics of India's telecom sector, the unique nature of its spectrum allocation policies, and of course, security and strategic concerns. India's choice of not imposing a ban on Chinese telecommunication vendors, including Huawei, from participating in Indian 5G trials is to further strategic room for manoeuvre. Sooner, not later, particularly with the fraught geopolitical realities brought on by the COVID-19 crisis , strategic ambiguity will need to be abandoned with a decision taken.

Sameer Patil and Arun Vishwanathan trace India's fitful engagement with multilateral export control regimes with potential benefits to be accrued in areas like nuclear trade, defence modernization and civilian space. Going forward, Patil and Vishwanathan argue that India must reprise its role as a rule-shaper to ensure export control regimes like the Wassenaar Arrangement and the Missile Technology Control Regime regulate the nefarious impacts of dual use surveillance technology. Vidushi Marda sees a similar opportunity in the field of Artificial Intelligence where India can lead with the design, standardization and reasonable limits on the deployment of these systems, instead of rushing blindly into developing them to advance economic objectives.

India has been a fervent proponent of data sovereignty, a maxim that seeks to ensure global technology companies operating in India do not derive rabid profits from the data of Indian citizens. As we demonstrate in our piece, this idea has been pushed through impulsive measures on data localization and non-personal data governance; concurrently, India has also engaged in multilateral pushback against efforts that hasten the free flow of data. Divij Joshi shares our scepticism of this 'data sovereignty' push given the government's centralization tendencies and systematic undermining of individual sovereignty at the expense of what he calls 'other valid conceptions or imaginations of data governance.' India can do more to dismantle structures of technological power through domestic and global leadership on issues like competition, digital taxation and the liberalization of intellectual property protections.

The final frontier of global technology governance is the regulation of speech on social media platforms. Originally billed as the power to connect, social media platforms are now dividing and spreading hatred. The problem is a global one but the solution, as we argue with Torsha Sarkar, is local. Regulating free speech cannot be agnostic to the social, economic and cultural context and must be driven through law and policy that reflect these factors. Multilateral efforts, however noble, will likely be inadequate.

Finally, practitioners require academic knowledge as ammunition while articulating and defending India's positions within multilateral fora. In a riveting interview, Ambassador Asoke Mukerji, India's former Permanent Representative to the United Nations, discusses with great enthusiasm his multilateral experiences and how he sees India shaping global technology debates in the years to come.

As this issue of 'Seminar' demonstrates, there are no easy answers to these pressing global governance questions but there are clear interests, constraints and costs should India desist from influencing these multilateral discussions. Questions around curtailing state power with respect to technology will fundamentally rest on rules and laws that require careful deliberation and resolution but the desire to draft such rules has not been forthcoming partly due to the vacuum that exists globally vis-à-vis technology governance. As the world's largest democracy, India's distinct economic and demographic leverage places it in an unique position to shape global technology rules that serve its strategic interests. Simply put, India has the potential to play a significant role in the ongoing digital worldmaking.

KARTHIK NACHIAPPAN and
ARINDRAJIT BASU

Going slow on 5G

MANOJ KEWALRAMANI

AFTER a year of government-wide deliberations, late in December 2019, India's Department of Telecommunications (DoT) announced that it had taken a decision to allocate spectrum for conducting 5G trials in the country. The trials, Telecom Minister Ravi Shankar Prasad explained, would be open to all operators and vendors.[1] By mid-January, reports informed that four operators, Vodafone Idea, Bharti Airtel, Reliance Jio and state-run BSNL, had submitted applications for trials. Vodafone and Airtel were said to be partnering with four vendors, i.e. Sweden's Ericsson, Finland's Nokia and China's Huawei and ZTE. Reliance Jio and BSNL, on the other hand, had chosen a single vendor each in South Korea's Samsung and ZTE, respectively.

Since then, there has been no further progress. In comparison, around the world, countries appear to be racing ahead with 5G network development and commercial operations. A February 2020 report by Viavi Solutions found that commercial 5G networks had been deployed in 378 cities across 34 countries, with South Korea, China and the US emerging as leaders.[2]

At the heart of the global 5G rush is the promise of massive economic gains. The fifth generation of wireless networks will enable extremely high speeds of connectivity, significantly higher connection density and near-zero latency. These advantages are expected to enhance machine-to-machine connectivity, data analytics and automation, resulting in the development of new products and businesses, boosting productivity and enhancing state capacity. Studies estimate that by 2035, 5G technologies will enable $12.3 trillion of global economic output and support 22 million jobs. In India, a government study in August 2018 estimated the cumulative economic impact of 5G on the country's economy to hit $1 trillion by 2035.[3]

Considering the above, what explains the slow pace of movement on a 5G policy in India? This article argues that there are four underlying factors – economics of India's telecom sector, the peculiarities of the country's spectrum allocation policies, along with national security and strategic concerns.

The telecom sector is among India's biggest post-liberalization success stories. The breaking down of state monopoly and recasting of the regulatory structure, which began at the turn of the millennium, resulted in intense competition and expanded consumer welfare. However, with time, there have emerged certain structural problems that are plaguing the sector's future development.

Over the years, low-cost connectivity along with the increasing

1. 'India Allows Huawei to Participate in 5G Trials', *Economic Times*, 31 December 2019. https://economictimes.indiatimes.com/industry/telecom/telecom-news/govt-will-give-5g-spectrum-for-trials-to-all-players-prasad/articleshow/73033442.cms

2. The State of 5G Deployments, VIAVI Solutions, February 2020. https://www.viavisolutions.com/en-us/literature/state-5g-deployments-2020-poster-chart-en.pdf

3. 'Making India 5G Ready', Report of the 5G High Level Forum, 23 August, 2018. https://dot.gov.in/sites/default/files/5G%20Steering%20Committee%20report%20v% 2026.pdf?download=1

penetration of mobile phones fuelled subscriber growth. Consequently, India today is the world's second-largest telecommunications market in terms of subscribers. And, there still exists much scope for expansion. As of December 2019, the Telecom Regulatory Authority of India estimated overall teledensity at 88.56%, with urban teledensity at 156.26% and rural teledensity at just 56.67%.

Competing for this market share are largely three private service providers – Vodafone, Airtel and Reliance Jio – who together account for approximately 90% of wireless data users in the country. Jio's entry into the market in 2016, in fact, marked a turning point. Offering free voice calls and almost free data and messaging usage, it reshaped the economics of the sector. The ensuing competition led to a fall in Average Revenue Per User (ARPU), as competitors consolidated, slashed their offerings and invested in improving service quality.

Consequently, high levels of debt and low profitability now characterize the sector. Deepening service providers' woes is the Indian Supreme Court's October 2019 verdict interpreting Adjusted Gross Revenue (AGR) in such a manner that it added Rs 1.47 lakh crore to their liabilities. The verdict was the outcome of a 16-year-long legal battle between the DoT and service providers over assessment of license fees. What's worth noting is that the bulk of this burden fell onto Airtel and Vodafone, estimated at Rs 35,586 crore and Rs 57,000 crore, respectively. Jio, on the other hand, has already paid its dues estimated at Rs 195 crore. Considering the above, service providers' appetite for large capital investments that 5G networks will require remains questionable. What's likely to make it even more troublesome is the added cost of spectrum.

Over time, successive Indian governments have viewed spectrum purely as a revenue generating resource rather than from the perspective of economic value generated owing to the network effect. This position has complicated spectrum allocation policy. The 2G scandal added an ugly political dimension to these decisions. In November 2010, a report by the Comptroller and Auditor General of India argued that the DoT had issued 2G spectrum licenses to service providers at throwaway prices, resulting in a loss of Rs 1.76 lakh crore to the exchequer. The scandal marked the beginning of the downfall of the Manmohan Singh-led UPA II government. The subsequent years witnessed intense politicization of spectrum policy. Consequently, broader considerations about cost conundrums facing service providers and the multiplier effect of cheap connectivity have largely been ignored. In other words, revenue generation is prioritized over value generation.

This dynamic is also evident in the 5G case. Despite back and forth with DoT, the Telecom Regulatory Authority of India (TRAI) has stuck to its base price recommendation for 5G spectrum at Rs 492 crore per megahertz. The Cellular Operators' Association of India (COAI) believes that at this rate, Indian spectrum is 'overpriced by at least 30-40 per cent compared to international standards and auction in other markets like South Korea and the US.'[4] At a point in 2019, there appeared to be some sort of a middle path that was being worked out, with New Delhi potentially reviewing this figure. But no change was eventually announced.

At present, during its next auction, the Indian government plans to offer just over 8,000 megahertz of 4G and 5G spectrum, eyeing revenue of approximately Rs 5.86 lakh crore. This is likely to be the case despite the COAI suggesting that participation from their members is likely to be muted, owing to the 'unrealistic pricing of the key spectrum bands that are for 5G.'[5] Among the operators, Airtel has been the most vocal, suggesting that it might even skip the auction owing to concerns over the price. Consequently, the planned auction has witnessed a number of delays. Add to this the unfolding Covid-19 pandemic and the earliest that an auction will now take place is the end of 2020.

Another point of contention is the development of standards. Globally, 5G standards development is being carried out under the aegis of the 3rd Generation Partnership Project (3GPP). This is a consortium of seven major telecommunications standard development organizations, including the Telecommunications Standards Development Society, India (TSDSI), and a number of other associate partners. It is important to note that 3GPP in itself does not set standards. It develops technical specifications, which then get adopted and enforced by the standard development organizations that comprise 3GPP. Members, therefore, have autonomy in terms of final decision-making.

In this context, over the past year, COAI, the Global mobile Suppliers Association (GSA) and the Euro-

4. 'Price of 5G Spectrum in India 30-40 Per Cent Higher Than Global Rates: COAI', PTI, 04 January 2019. https://economictimes.indiatimes.com/industry/telecom/telecom-news/price-of-5g-spectrum-in-india-30-40-pc-higher-than-global-rates-coai/articleshow/69648788.cms

5. Devina Sengupta, 'Spectrum Sale May Fetch Only Rs 10,000 Crore Initial Payment', *Economic Times*, 10 February 2020. https://economictimes.indiatimes.com/industry/telecom/telecom-news/spectrum-sale-may-fetch-only-rs-10000-crore-initial-payment/articleshow/74053765.cms

pean Telecommunications Standards Institute have been discussing proposals of local standards put forward by TSDSI. While largely adopting 3GPP guidelines, TSDSI says that it wants to make global standards India specific with certain enhancements. COAI has argued that this creates hurdles for Indian industry. GSA believes that there will be interoperability issues going forward. Despite that, TSDSI has pressed ahead. It believes that local standards are needed to ensure rural connectivity and software adjustments can help industry mitigate any challenges. In March 2020, the TSDSI's Radio Interface Technology Proposal won the International Telecommunications Union's approval. It now says it is working to make sure that its proposal interworks seamlessly with the 3GPP proposal.[6] This too is likely to get delayed owing to the pandemic.

From a security and strategic perspective, these delays might prove beneficial, but only to a point. Washington increasingly views Beijing as a strategic competitor, with the tussle over 5G emerging as a critical component of this rivalry. On one hand, the Donald Trump administration has actively sought to decouple from the Chinese technology ecosystem. On the other, it has sought to persuade and even threaten allies and partners to ensure that they reject Chinese telecom equipment providers, particularly Huawei. Washington's core argument to partners has been that the Chinese Party-state uses its economic might to pursue strategic objectives, with private firms being used as instruments of statecraft.

The US's efforts have borne mixed results at best. Only a handful of American allies and partners, such as Australia, New Zealand and Japan, have formally barred Chinese equipment makers from their 5G markets. In contrast, European partners like France, Germany and the UK have refrained from an outright ban, arguing that the risk can be managed through a mix of regulation and technological solutions. Their approach is a product of a mix of economic and political considerations, such as switching costs, the cost-effectiveness of Huawei products and a desire to ensure strategic autonomy. Despite this, there has been greater agreement among the US and its allies and partners over the nature of security threats. This is evident in the proposals agreed upon at the 2019 Prague 5G Security Conference.[7]

The two-day conference, held in early May, brought together participants from 32 countries – including select EU and NATO member states along with Israel, Japan, Australia, New Zealand and South Korea – and four global mobile network operators. The objective was to arrive at a common approach towards cyber threats emerging from 5G technologies and recommending courses of action. The non-binding proposals that were finally agreed upon expand the definition of security threats to include non-technical aspects, such as political, economic or other behaviour of malicious actors, and supply chain security. The document also calls on taking into account the 'overall risk of influence on a supplier by a third country.' It further adds the need to consider the 'legal environment and other aspects of (a) supplier's ecosystem', along with transparency related to ownership, partnerships, and corporate governance structures of service providers.

The proposals provided the framework for the EU's new cyber security toolbox[8] and Britain's decision to keep high-risk vendors out of the network core and capping their access to non-sensitive parts of the network.[9] Going forward, participating states are expected to work on sharing concrete tools, instruments, measures and solutions to tackle 5G security threats, arriving at a set of best practices.

India is not a party to the Prague Proposals. However, the recommendations and tools that could emerge from the process hold particular salience for New Delhi. On one hand, they provide an opportunity for India to learn from the experiences of other states and examine the effectiveness of different models. For instance, there is an ongoing debate in the country over observing the feasibility[10] of European and British models and experimenting with local software solutions to tackle security threats.[11] On the

6. Danish Khan, 'India's Local 5G Tech Gets Traction Amid Opposition From Gear Vendors', 18 March 2020, ET Telecom. https://telecom. economictimes.indiatimes.com/news/indias-local-5g-standard-goal-gains-traction-amid-opposition-from-gear-vendors/74683214

7. The Prague Proposals, 3 May 2019. https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf

8. 'Secure 5G Networks: Commission Endorses EU Toolbox and Sets Out Next Steps', 29 January 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

9. 'New Plans to Safeguard Country's Telecoms Network and Pave Way for Fast, Reliable and Secure Connectivity', 28 January 2020. https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity

10. Anandita Singh Mankotia, 'Indian Telecom Companies May Leave Huawei Out of Core 5G Network', 12 August 2019. https://economictimes.indiatimes.com/industry/telecom/telecom-news/indian-telecom-companies-may-leave-huawei-out-of-core-5g-network/articleshow/70636358.cms

11. Amrita Nayak Dutta, 'India Can Secure 5G Networks With Local Technology, Top Security Advisor Raghavan Says', *ThePrint*, 22 October 2019. https://theprint.in/diplomacy/india-secure-5g-networks-local-technology-top-security-advisor-raghavan/309259/

other hand, the proposals, with clear political parameters for vendor participation, could constrain New Delhi's room for manoeuvre and thereby impinge on its economic interests.

India imports an overwhelming majority of its telecommunications equipment requirements. Dependence on foreign vendors, therefore, cannot immediately be wished away. Moreover, given the structural financial challenges within the sector discussed above, there is a strong economic rationale for partnering with suppliers providing cost-effective, yet cutting-edge equipment. Clear standards for partnering with foreign vendors, along with a focus on network resilience and redundancies are imperative. Thus far, however, the Indian government has not provided any such guidelines; this is underscored by Jio and BSNL partnering with one vendor each for trials, with the latter being state-run and choosing a Chinese vendor.

The economic benefits, however, must be weighed against security and strategic implications. Although the Prague Proposals do not name any vendor or state, the references to Chinese vendors are unmistakable. For New Delhi, the security risks of working with Chinese vendors are greater, given the issues over territorial integrity and sovereignty along with enduring strategic mistrust that characterize the Sino-Indian relationship. Moreover, Beijing has been rather blunt with New Delhi. It has warned of 'reverse sanctions' on Indian firms and broader consequences if Chinese vendors are banned by India.[12] Yet, India has allowed Chinese vendors to conduct trials. Moreover, in doing so, it is unclear if the government has conducted a thorough technical assessment of the risks and examined potential mitigation strategies.

At the same time, New Delhi has actively engaged with Washington on 5G network development. The issue featured in discussions between US President Donald Trump and Indian Prime Minister Narendra Modi in Osaka in June 2019 and during Trump's visit to New Delhi in February 2020. Mukesh Ambani's remark to Trump during his Delhi visit about Reliance Jio being the 'only network in the world that doesn't have a single Chinese component' is indicative of the significance of the issue for bilateral ties.[13]

India's choice of eschewing a complete ban has as much to do with economic concerns as it has to with strategic imperatives. Deepening Sino-US competition is resulting in the splintering of cyberspace and the global technology and innovation ecosystem. Being locked into any one camp, however, would entail significant costs for India. Therefore, New Delhi has sought to create room for manoeuvre to preserve its strategic autonomy. But a common approach between the US and its partners, which specifically targets China, as evident from the Prague Proposals process would make this a much more difficult task. Invariably, this could squeeze India into a position wherein it would have to choose a camp, undermining India's economic and security interests.

This strategic conundrum works well for those who believe that India should focus on complete indigenization of the 5G network, even if it entails further delays in roll out. Over time, the *await indigenization* community, in fact, has gradually expanded. There is, of course, diversity in the motivations of individuals who fall within this umbrella. For instance, some argue that indigenization is the only route to genuine security,[14] others blend the security concerns with protectionist impulses.[15] And then there are those who question the utility of 5G-powered systems in India, given the relatively weak ecosystem in the country characterized by low smart devices and 4G penetration.[16]

A confluence of the above factors has led to the Indian government essentially adopting a go-slow and wait and watch approach. While spectrum policy and sorting out the telecom sector are a matter of domestic policy, it is increasingly becoming clear that a decision on 5G network development will have strategic implications. Waiting and watching might work for a while, but sooner rather than later a decision must be taken. And in doing so, the tightrope walk that New Delhi is currently performing might prove to be very challenging in the long run as Sino-US ties continue to worsen.

12. Sanjeev Miglani, Neha Dasgupta, 'China Warns India of "Reverse Sanctions" if Huawei is Blocked – Sources', *Reuters*, 6 August 2019. https://www.reuters.com/article/us-huawei-india-exclusive/exclusive-china-warns-india-of-reverse-sanctions-if-huawei-is-blocked-sources-idUSKCN1UW1FF

13. 'Reliance Jio Doesn't Have a Single Chinese Component, Mukesh Ambani Tells Donald Trump', *Economic Times*, 28 February 2020. https://economictimes.indiatimes.com/industry/telecom/telecom-news/jio-doesnt-have-a-single-chinese-component-mukesh-ambani-tells-donald-trump/articleshow/74335119.cms

14. 'Only 100% Indigenization Can Make India Secure in 5G Era: IIT Professor', IANS, 11 July 2019. https://telecom.economictimes.indiatimes.com/news/only-100-indigenisation-can-make-india-secure-in-5g-era-iit-professor/70167675

15. Dhairya Maheshwari, 'Swadeshi Jagran Manch Protests Huawei Conducting 5G Trials in India, Writes to PM Modi', *IndiaTV*, 31 December 2019. https://www.indiatvnews.com/news/india/swadeshi-jagran-manch-protests-huawei-conducting-5g-trials-in-india-writes-to-pm-modi-575218

16. Brijendra K Syngal, '5G Shouldn't be Rolled Out in a Hurry', *The Hindu Businessline*, 24 February 2020. https://www.thehindubusinessline.com/opinion/5g-shouldnt-be-rolled-out-in-a-hurry/article30905507.ece

The legal contours of India's 'sovereign cyberspace'

GUNJAN CHAWLA

EARLIER this year, India gained the unenviable distinction of being the most 'cyber attacked' nation in the world. However, the legal tools deployed to mitigate the threat of cyber attacks so far have proved insufficient. This article provides a birds-eye view of India's policy positions in relation to recent efforts at various multilateral and multi-stakeholder for a seeking to upgrade interpretations of international rules, or formulate new ones to combat the growing malicious use of increasingly sophisticated information communication technologies (ICT).

In a short span of 20 years since the promulgation of the Information Technology Act, 2000 cyber attacks have become the most significant threat to the security of the state. Data released by the India's Computer Emergency Response Team (CERT-In) reveals a ten-fold increase in incidents like network scanning and probing between 2017 and 2018 alone. From 9359 incidents in 2017, CERT-In recorded 127481 such incidents in 2018. The National Crime Records Bureau (NCRB) reported a doubling of ICT-enabled crimes under the Indian Penal Code between 2016 and 2017. According to the NCRB, more than half of the reported cyber crime in India is economically motivated, causing great financial losses to citizens and perpetuating economic insecurity.

However, these statistics on malicious cyber activity and cyber crime do not reveal whether the origin of these cyber attacks against Indian targets can be attributed to another state, or non-state actors or individuals, who may be foreign or domestic. As a consequence of numerous barriers – including technological, strategic and legal – to decisive attribution of cyber attacks and incidents, India is faced with a kind of 'Schrödinger's cyberwar'. The state is defending itself against adversaries whose legal status, and consequently, rights and obligations remain unclear in law, often

due to technological obfuscation. This problem is further compounded by limited technological capacity of the government. In most cases, the identity of the adversary – which may be another state, non-state entity or individual – as perceived by the victim state remains in flux.

For a sovereign nation to build effective cyber defences, evolution of the applicable domestic and international law is essential to complement efforts to upgrade the technological capacity of the state and bolster avenues to strengthen international cooperation. Domestically, recent policy trends have been focused on 'digital sovereignty', manifested in policies like data localization, which was watered down under the 2019 Personal Data Protection Bill. Owing to the inherent nature of cyberspace as a borderless realm, such policies cannot be implemented without sovereign control over cyberspace, including its physical layer (DNS route servers, routers, fibre optic cables, hardware etc.) as well as logical layer (code, such as the Transmission Control Protocol/Internet Protocol, or 'TCP/IP'), or cooperation of the private sector, especially Big Tech corporations. Such a scenario poses serious hurdles for domestic law enforcement – an inherently sovereign function – and consequently, manifests as a government restriction on freedom of expression exercised through censorship, or 'moderation' of the content layer (e.g. Websites, social media, e-marketplaces etc.), that remains the most visible and accessible component of cyberspace. In extreme cases, cutting off access to this layer altogether by way of internet shutdowns tends to be the preferred mode of 'preventive policing' of cyberspace.

Additionally, the skewed global distribution of infrastructure and knowledge comprising the physical and logical layers of the internet, heavily concentrated in western nations, but under the effective control of private actors, poses insurmountable challenges for India's domestic legal system. The need for a coherent international legal framework to enable effective investigation and attribution of cyber incidents is apparent to effectively grapple with their international dimensions.

Although the IT Act mandates the exercise of jurisdiction beyond India's territorial borders, it is rarely implemented owing to difficulties in cooperation with foreign law enforcement agencies, incompatible legal regimes and red tape, as well as challenges in domestic regulation of Big Tech, especially social media intermediaries. A salient example is the WhatsApp traceability issue currently pending verdict, where the Indian government has mounted an offensive against end-to-end (E2E) encrypted communications. This attitude was also shared by the governments of the United Kingdom (UK), United States (US) and Australia, who jointly wrote an open letter to Facebook last year, in a bid to discourage the use of E2E encryption without providing for a backdoor to enable lawful access to content by law enforcement agencies.

This example is also useful to illustrate the pivotal role of the private sector in the global governance of ICT, stemming from their control over its infrastructure. The tussle for technological supremacy between pre-eminent cyber powers tends to drive technical know-how and expertise deeper into the opaque cover of national security. Additionally, the far-reaching influence of transnational private sector players like Facebook, WhatsApp, Apple on the one hand and Huawei, Xiaomi, ByteDance on the other, creates a 'cyber landscape' that is a potential minefield for governments to navigate, especially for those aspiring to become cyber powers themselves.

Although China has traditionally been the rival to India's claim to primacy in South Asia, India's domestic legal approach appears to mirror that of China, given our domestic policy emphasis on sovereignty in cyberspace and its manifestations. Huawei's entrenchment in the Indian telecom scene adds to the complexity of our posturing in the broader context of this struggle for technological supremacy. The question that remains is whether we will do the same in our strategy to engage with international institutions tasked with formulating these norms. The paradoxes of (cyber) war certainly appear to engender a 'reversal and even coming together of opposites'.[1]

Given international law's state-centric approach to the formulation and implementation of legal rules and norms, a borderless cyber space poses unique challenges to peaceful coexistence and cooperation among actors of the international community in cyberspace. Additionally, the existence of diverse models to regulate the private sector across jurisdictions and exacerbation of the 'digital divide' through rapid proliferation of technologies make it exceptionally difficult for governments to formulate and implement universally acceptable rules and norms.

Thus, India finds itself positioned rather awkwardly between the East and the West. While there is widespread agreement that international law applies in cyberspace, there is pervasive disagreement among nations as to exactly how it applies. Last year, India's External Affairs Minister S. Jaishankar spoke of a new approach to India's foreign policy with a

1. Edward Luttwak, *Strategy: The Logic of War and Peace*. Harvard University Press, Cambridge, Mass, 1987.

pre-emptive defence posturing that has abandoned its old policy of non-alignment, replaced by an issue-based 'multi-alignment'[2] to advance national interests and priorities. However, India is yet to clearly define its interests in cyberspace. So far, seven nations, including Australia, Estonia, France, Germany, the Netherlands, the UK, and the US have issued comprehensive national statements on how international law applies to cyberspace.

It remains to be seen whether India's National Cybersecurity Strategy slated for release in 2020 will employ the language of international law to articulate its interests and ambitions in this new domain of warfare. Meanwhile, the task before Indian negotiators is a formidable one – to reconcile two apparently incompatible approaches[3] in parallel processes currently ongoing under the aegis of the United Nations.

The United Nations Group of Governmental Experts on advancing responsible state behaviour in cyberspace (GGE) has pushed the agenda of a 'free, open internet' through voluntary, non-binding norms to govern state behaviour. On the other hand, the UN Open Ended Working Group (OEWG) on Developments in the Field of ICTs in the Context of International Security led by Russia, which has emphasized 'cyber sovereignty' and the development of a legally binding framework of rules to govern state behaviour in cyberspace. The GGE consists of a few states selected on the basis of equitable geographical distribution whereas the OEWG is open to all UN member states. It is noteworthy that the call for cyber norms is rooted in Russian-led arms control resolution dating back to 1998, focused on mitigating threats from information weapons and information wars, while pushing for the ability to retain control over information environments.

Certain commentators have termed this dynamic between western interpretations and Sino-Russian interpretations of international law as a state of 'Mutually Assured Diplomacy'[4] – predicting it is likely that both the GGE and OEWG processes will fail or both will yield results, creating two separate but overlapping legal frameworks or interpretations competing for universal acceptance.

The GGE, set up in 2004 and currently in its sixth iteration has issued consensus reports in 2010, 2013 and 2015. India has been a participating member state in all its sessions, except in 2015. The 2015 Report of the GGE is a significant milestone, in its affirmation of the applicability of international law in cyberspace, and the need to further explore how international law applies in cyberspace. However, in its 2017 session the GGE failed to arrive at a consensus. This failure was largely due to strong opposition from some states including Russia, China and Cuba on the inclusion of an explicit reference to the applicability of the right of self-defence, countermeasures and international humanitarian law (IHL) in the draft report. In their view, such provisions would legitimize the ongoing militarization of cyberspace and compromise its stability and security.

Soon after UNGGE talks broke down, two separate resolutions were passed in the UN – one US-led, pushing for a new GGE to be constituted, and one Russia-led, calling for an open-ended working group on rules, norms and principles for responsible state behaviour in November 2018. The OEWG is due to report to the UN General Assembly (UNGA) in its 75th Session in September 2020, and now appears to consider voluntary non-binding norms as complementary to binding obligations in international law, attempting to build upon the GGE's 2015 Report.[5] However, the scope of state sovereignty and the right to self-defence in cyberspace as well as the scope for the application of IHL remain unresolved issues.

Having voted in favour of both these resolutions, setting up the GGE and OEWG, India has yet to take an explicit stance on the divide between the two camps, or articulate a middle ground. Some have argued that India's ambiguous stance may create a strategic advantage; however, this is only partially true. A foreign policy aimed at 'multi-alignment' in search for a more prominent role in contested domains in a rapidly changing international order must identify and collaborate with 'like-minded nations' to distinguish between our allies and adversaries in cyberspace. There is little clarity to be gained from other states' legal interpretations tailored to serve their own interests.

2. External Affairs Minister S. Jaishankar's Speech at the 4th Ramnath Goenka Lecture, 14 November 2019. https://mea.gov.in/Speeches-Statements.htm?dtl/32038/External+Affairs+Ministers+speech+at+the+4th+Ramnath+Goenka+Lecture+2019.

3. Josh Gold, 'Two Incompatible Approaches to Governing Cyberspace Hinder Global Consensus', *Leiden Security and Global Affairs Blog*, 16 May 2019. https://leidensecurityandglobalaffairs.nl/articles/two-incompatible-approaches-to-governing-cyberspace-hinder-global-consensus

4. Dennis Broeders, 'Mutually Assured Diplomacy: Governance, "Unpeace" and Diplomacy in Cyberspace', *ORF Digital Debates*, 2019, at pp. 26-29. https://www.orfonline. org/wp-content/uploads/2019/10/Digital_Debates_2019_V7.pdf

5. United Nations Open-Ended Working Group, Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security, 16 March 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf

At the OEWG's June 2019 session, India's remarks were focused on encouraging bilateral and multilateral efforts aimed at developing a better understanding of international legal concepts that underpin the discussion on states' use of ICTs – including cyber sovereignty, jurisdiction, attacks, and threshold for invoking the right to self-defence under the UN Charter.[6] Undoubtedly, conceptual clarity is indispensable. Without a conceptualization of what category of cyber crimes and cyber incidents may constitute 'cyber attacks' and therefore, be treated as an infringement of India's sovereignty that necessarily merit a proportionate response in law, the roadmap towards build an 'open, secure, stable, accessible, interoperable and peaceful ICT environment' is akin to driving in the dark.

In seeking a more prominent role on the international stage, there are multiple hurdles before India on its path from an international rule-taker to a rule-shaper. The multiplicity of platforms for discussion of cyber norms is a major challenge in navigating international lawmaking processes. For instance, some states have also indicated a preference to refer to the task of codifying international law applicable to cyberspace to the International Law Commission. Other multi-stakeholder efforts have proliferated in recent times, in a bid to catalyse the crystallization of universally acceptable 'rules of the road' for responsible behaviour in cyberspace.

The expansion of the UN GGE mandate in 2015 to examine the question of how international law applies to cyberspace engendered a three-year long effort by NATO to gather a group consisting entirely of western international law scholars and cyber security experts to produce the 'Tallinn Manual' on the International Law Applicable to Cyberspace. A second edition, with nominally better representation was released in 2018, but appears to have found little support in actual state practice.

The Global Commission on the Stability of Cyberspace (GCSC) established in 2015, articulated eight norms dubbed as the 'Singapore Norm Package' in 2018. In its final report of 2019, the GCSC also recommended the protection of the 'public core of the internet' – originally proposed by the Government of the Netherlands that did not gain support from all members of the GGE. The GCSC comprised 26 Commissioners representing a wide range of geographic regions as well as industry, technical and civil society stakeholders. Many of its members are former officials with various governments, including India's former Deputy National Security Advisor, Ambassador Latha Reddy.

The Paris Call for Trust and Stability in Cyberspace of 12 November 2018 led by French President Emmanuel Macron, articulated nine principles to secure cyberspace. These principles reaffirmed the applicability of international law and norms to cyberspace and encouraged cross-sectoral collaboration in recognizing the role and importance of the private sector in promoting trust and security in cyberspace. The Paris Call has so far garnered the support of 78 states and over 400 civil society organizations. Notably, both India and the United States have not joined the call.

The Paris Call considers the Budapest Convention on Cyber Crime as a key tool to strengthen defences against cyber criminals. This reference to the Budapest Convention is an apparent reason for India's refusal to join the Paris Call, choosing instead to sign a bilateral digital partnership with France in 2019. India's hesitation to accede to the Budapest Convention is unclear but appears grounded in first, its perception of the Eurocentric process of negotiation and drafting through the Council of Europe, and second, its substantive concerns with provisions under the convention that seek a harmonization of domestic substantive and procedural criminal law of the states parties. This continues to hamper the effective investigation and the overall implementation of domestic law on cyber crime, including especially, the provision for extra-territorial enforcement of the IT Act.

Terrorism is another domain where India has struggled with the international dimension of crimes committed on its sovereign territory and has repeatedly called for greater international cooperation to tackle cross-border terrorism. New Zealand and France led the drafting and adoption of the Christchurch Call to Action in May 2019, two months after the terrorist attack that killed 51 people at two mosques at Christchurch in New Zealand was live streamed on social media**.** This call outlines 'collective' and 'voluntary' commitments from governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet. Notably, while India is a signatory to the Christchurch Call, the United States refused to join, citing its potential to impinge upon free speech rights protected under its constitution.

Similarly, private sector initiatives have mushroomed in the last few years since talks at the GGE broke down. It is unsurprising that corpora-

6. Statement delivered by India at the Organisational Session of the Open-Ended Working Group (OEWG) on 'Developments in the field of Information and Telecommunications in the Context of International Security', in New York on 3 June 2019. http://meaindia.nic.in/cdgeneva/?8251?000

tions have rushed in to fill the void where state governments are unable to arrive at a consensus, considering first, that the responsibility to implement any norms that may be agreed upon will rest on their shoulders; second, that their technological capabilities will supply nuance to an otherwise political debate; and third, that their financial resources may supplement states' limited resources that can be diverted to engagements at international platforms. However, a proactive role for the private sector has not equally palatable to all concerned parties.

Microsoft's call for a 'Digital Geneva Convention' in 2017 urged corporations to commit to not participate in cyber attacks; the call also urged governments to do more to protect civilians and called for an independent international body to investigate and attribute cyber attacks against countries which received only a lukewarm response. Some criticized Microsoft for venturing into what has traditionally been the exclusive prerogative of the sovereign state under international law.

Over a year later, Microsoft pioneered the Cybersecurity Tech Accord in 2018, which has now been adopted by over 100 companies who espouse four principles – stronger defence, no offence, capacity building and collective action with like minded organizations. The list of signatories includes Facebook, ARM, Cisco and FireEye among others. The establishment of the Cyber Peace Institute under Microsoft's leadership in 2019 to provide assistance and promote collaborations for responsible behaviour is yet another step forward in the direction of international cooperation for a peaceful cyberspace underwritten by the private sector. The Charter of Trust initiated by Siemens at the Munich Security Conference in 2018 started with eight signatory corporations who endorsed a set of principles broadly aimed at reducing cyber risks. Its membership grew to include corporations including Cisco, Dell Technologies and IBM and now stands at 16.

For greater engagement with such norm-shaping and norm-making processes, the government needs to guide and equip Indian companies through industry associations to play a proactive role. Improvement of international efforts to capacity building across the public and private sectors undoubtedly needs to be an area of focus for India in these multi-stakeholder forums. Necessarily, this will also help us to better understand the needs of the domestic cyber security sector specifically and the ICT and Information Technology Enabled Services (ITES) sector at large.

It is exceptionally difficult to decisively predict how the international order will change and evolve from the COVID-19 pandemic. In today's borderless, but gradually fragmenting cyberspace, one thing is clear – India's unwavering commitment to protect and preserve its rights as a sovereign state even when pitted against faceless adversaries. The broader political challenge in the formulation of an international cyber policy lies in preserving the international legal principle of sovereign equality.

The process of developing new norms and interpretations of existing law needs to recognize common interests and shared responsibilities in the face of differential access to the means and methods of waging cyber wars, along with other weapons of mass disruption. Whether voluntary, non-binding norms will be adequate to restrain, if not halt their disruptive effects is the question India's strategists have to answer to help India's negotiators navigate the paradoxes of cyber war.

Regulating the marketplace of ideas

TORSHA SARKAR, ARINDRAJIT BASU and KARTHIK NACHIAPPAN

SOCIAL media is one of the most important tools shaping political discourse all over the world. Over the last decade, we have seen online spaces being increasingly used to archive instances of humanitarian violence, carve out repose for historically marginalized communities and coordinate and communicate entire political movements. At the beginning of the last decade, therefore, optimists like Jack Balkin saw the internet and digital technologies, with their '[...] widespread distribution, their scope and their power' as having the potential of promoting the 'possibility of democratic culture'.

However, if the beginning of the decade heralded social media platforms for improving the participative nature of democracies for good, the later half has cast a doubt on this rosy narrative. In the last few years, both governments and civil society have accused these companies of manipulating elections, facilitating genocides and censoring the voices of historically oppressed communities. As Lawrence Lessig warned us, in our celebration of cyberspace as achieving 'liberty from the government' we overlooked the impact of code as the hidden regulator of the terms of our online liberty.

The changing nature of these online spaces and the ever-expanding number of services offered by social media has made governments enact stricter, more interventionist liability regimes for these platforms, often trampling upon the right to freedom of speech and expression. India is no exception.

In this article, we explore, *first*, the domestic interventions India has opted for in regulating social media; *second*, global, multilateral efforts undertaken by both state and non-state actors and *third*, highlight key questions on the applicability of global governance mechanisms to regulate free speech on social media for the Indian context. Regulating social media is a continuous battle between competing values – preserving and restricting speech that harms public order. The heterogeneity – social, economic and linguistic – of India's vast population could mean that India's regulatory

manoeuvres have the potential to shape free speech norms vis-a-vis social media governance globally.

India regulates social media under the broad regulatory ambit of intermediary liability. The term intermediary is defined under the Information Technology (IT) Act, 2000 as 'with respect to any particular electronic records, [...] any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record'. This broad definition therefore encompasses social media within its ambit.

One of the most critical aspects of regulating social media is the issue of regulating user-generated content, and navigating the liability regime for supposedly unlawful acts of users online. Article 19, in its report 'Internet Intermediaries: Dilemma of Liability', identifies three legal models of regulating the liability of intermediaries for content posted by its users. In the spectrum of holding intermediaries liable for third-party content – strict liability model (followed in China and Thailand) and broad immunity model (followed in USA under the Communications Decency Act) occupy the two ends, while safe harbour falls somewhere in the middle, though the exact contours of the model vary across jurisdictions.

India has traditionally followed the safe harbour model of liability. As provided for in Section 79 of the Information Technology Act, an intermediary would be granted a 'safe harbour' from the liability accrued due to third party content provided they follow certain legal obligations. While this system has not been perfect, the draft amendments introduced to the existing rules seem to overhaul the structural norms of the liability model. Specifically, Rule 3(9) of the draft amendments introduced in December 2018 require intermediaries to deploy 'technology based automated tools' to filter out 'unlawful' content. At first glance, this obligation seems to run into the constitutional 'void for vagueness' doctrine where the usage of ambiguous and broad terms throws up questions of the constitutionality of the provision.

Additionally, the rule ignores views that criticize the use of automated tools to filter speech. YouTube's Content ID, for instance, is a classic example of the faults of automated content detection methods. Content ID is an automated tool used for detection of content on the platform violating copyright, and despite the staggering amount of investment behind its development, continues to yield false positives, and has proven to be not infallible.

For every post under scrutiny, numerous nuances and contextual cues act as mitigating factors, none of which, at this point, would be understandable by a machine. Further due to the algorithmic 'black box', no decision made by automated filtering tools can fully be explained to human beings, even to the developer that trained the algorithm. This has crucial ramifications for due process and accountability if a decision needed to be scrutinized in a court of law.

Perhaps most importantly, this obligation leaves it up to the social media platform to arbitrate what comprises 'unlawful' speech, a decision that should be taken by a legitimate lawmaking body. In India, with its diversity of cultures and languages, what comprises unlawful speech would vary and require contextual analysis. It is impossible to expect such judgment from social media companies whose content moderation norms have always been a-contextual and agnostic to the socio-political realities of the terrain where they operate in.

One of the core conceptions of a liberal democracy is holding elected institutions accountable for the enforcement of our constitutional rights, including our right to life and right to free expression. If India's political institutions are shirking this duty in favour of corporations, then that leaves the common citizen without any recourse should they believe their fundamental rights of expression are violated online. This development is alarming.

Apart from this, section 69A of the IT Act and its allied rules also provide the regulators an alternate framework to effectuate content takedown. The procedures under this framework are required to be carried under a strict confidentiality clause, as mandated by the law. As a result, this framework has traditionally allowed the Indian government to carry out censorship in a completely opaque manner, and circumvent answering Right to Information (RTI) requests time and again.

An oft-overlooked aspect of regulating social media is the issue of holding them accountable for their actions, which may not be unlawful, but nevertheless limits the public participation of the users. As the decision of the US Supreme Court in *Packingham v North Carolina* states, participation in social media was equivalent to 'speaking and listening in the modern public square', and the same was protected under the First Amendment rights.

A similar legal question is currently being discussed in India where the suspension of Supreme Court advocate Sanjay Hegde's Twitter account and his subsequent litigation against Twitter has raised several important questions. One is, of course, regarding Twitter's arbitrary enforcement of its internal moderation norms, where perfectly legal speech (like the content

shared by Hegde) is censored while troves of hateful narrative remain online. The second, and possibly more important, question is the creation of an enforceable constitutional remedy of the fundamental right of free expression against social media platforms.

Why is this important? We have to remember that traditionally, the government's role in regulating speech is limited to the extent that speech is clearly violating a legal framework while ensuring that any restrictions on speech do not violate the fundamental right to free expression. This is a negative obligation on the part of the government – to *not* violate our rights. However, should legal jurisprudence develop to an extent where certain acts of social media companies are subsumed within the constitutional framework, our fundamental rights may cast a different duty upon the government to regulate these private actors on our behalf – thereby placing a positive obligation. Getting around this constitutional juggernaut will be critical for effective social media regulation in India.

While multilateral discussions covering the regulation of social media are new territory for India, it is becoming a fixture of political discourse in other parts of the world. Of late, several countries have begun seriously discussing whether the time has come to regulate and constrain the growing clout of social media companies like Facebook and Twitter. Some of these discussions cover issues related to privacy and copyright, particularly in the European Union where some tech companies have been sanctioned for violating EU laws. Other such discussions have been prompted by events, most notably the heinous Christchurch terrorist attack that was telecast live on Facebook. This senseless attack precipitated an eponymous global initiative to curb the deleterious impacts of social media platforms – Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online.

The Christchurch Call outlines 'collective, voluntary commitments' from both governments and internet service providers to reduce violent extremist and terrorist content online and, more broadly, to prevent the internet from being used for such nihilistic purposes. Through the call, eight tech giants, including Facebook and Twitter, the European Commission and 48 countries, including India, signed a voluntary call to remove the ability of social media platforms from being used for extremist purposes. The Christchurch pledge includes three specific commitments for governments, online service providers and for both combined.

Specifically, the call impels governments that have committed, to act by promoting social cohesion that resists and eradicates hate, enforce laws to prohibit the production of violent content online, encourage media organizations to behave ethically online and tighten domestic standards that heighten reporting of such malevolent acts. Yet, a bugbear of the initiative has been its innate conflicts with freedom of speech restrictions, which has prevented some countries, notably the United States, from supporting it despite Washington issuing support over the spirit of the call.

The Christchurch Call aside, tech companies have banded together to combat the use of their platforms for nefarious purposes. Twitter, Facebook and Microsoft announced the formation of the Global Internet Forum to Counter Terrorism (GIFCT) to disrupt terrorists and extremists from exploiting their services to promote terrorism, disseminate extremist propaganda and glorify violence. The GIFCT functions as a private initiative between its members to address the adverse public effects of their platforms, largely done through information and knowledge sharing, technical collaboration and shared research that could blunt that ability of terrorists from abusing digital platforms. What is patently unclear, even now, is how the GIFCT interacts with public authorities as it works to fulfil its mandate; moreover, concerns owing to transparency linger particularly as these firms tout information sharing as a key priority under GIFCT.

It also remains to be seen how the GIFCT will collaborate to reduce online extremist content without effectively balancing the need of its users who will seek to express themselves freely on their platforms; GIFCT members that now include YouTube, Pinterest, Dropbox, Amazon, Linkedin and WhatsApp, also have the right to resist governmental calls to remove online content from their platforms. Self-governance exhibited by tech firms through GIFCT appears to be a promising development but one that has to work in concert with other more stringent public efforts to root out online extremism.

European institutions and countries have been spearheading the global effort to cleanse social media platforms of hateful content. In March 2000, the European Commission established the European Internet Forum (EIF) to generate greater awareness among European Parliament MEPs on the question of internet governance and how the internet could impact European countries broadly. The EIF has evolved as a forum to help European parliamentary representatives respond to the social and economic effects of the 'digital transformation' sweeping Europe; the forum has since become a serious advocate for international cooperation

to contain the 'viral spread' of terrorist and violent extremist content online.

The need to facilitate this objective also featured prominently during France's 2019 G-7 presidency where discussions raised the issue of extremist online content and the responsibilities platforms like Facebook had to eliminate it. French President Macron initially hoped to get social media companies to sign a 'Charter for an Open, Free, and Safe Internet' that aimed to forge a 'collective movement' to ensure the internet remains a safe positive space for all. French initiative, however, was scuppered by the Trump administration that pressured their social media companies to demur.

Besides these focused initiatives, other intergovernmental organizations have joined the fray offering proposals and ideas to coordinate and regulate social media governance across borders. In 2018, the UN issued its first report on the regulation of online content which examined the role of both states and social media companies in ensuring an 'enable environment' exists for the expression of information and ideas. Going further, the report urged states to reconsider speech-based restrictions and, instead, adopt targeted regulation that helps publics make educated choices on online engagement.

Recently, UNESCO also issued a report calling for the modernization of electoral frameworks that could contain the spread of disinformation and 'fake news' on various platforms. These diffuse efforts, though somewhat ineffective, are gradually raising more awareness regarding whether the UN or OECD should lead efforts to devise clear rules, through an international convention or binding standards that point the way for countries to regulate their social media companies.

The growing landscape of actors and governance approaches to reduce hateful and violent online content also includes two multi-stakeholder networks – The Internet and Jurisdiction Policy Network and the Freedom Online Coalition (FOC) Advocacy network. The FOC consists of 31 member states that have committed to support internet freedom and protect fundamental human rights or freedom of expression, association, assembly and privacy when online. FOC's 31 member states work to achieve internet freedom by aligning diplomatic efforts and policies, sharing information and raising concerns when freedom is abridged online.

In terms of work, the FOC also partners with civil society and the private sector through working groups to advance interest freedom and digital rights. Compared to other groups, the FOC as a clear and avowed political mission – to keep the internet open and democratic for all individuals just as repression on the internet appears to be rising. Finally, the Internet and Jurisdiction Policy Network functions more as an arbiter, working to resolve conflicts that surface when the effects of the internet cross jurisdictions. The network's role and responsibilities embody the multi-stakeholder nature of the internet and internet governance that cuts across multiple silos and jurisdiction informing the public of the risks tied to dealing with internet problems narrowly.

The above discussion elicits two important questions that trouble the application of traditional global governance mechanisms to regulating social media. First, it is clear that the appropriate regulation of free speech online can only be devised and implemented in conjunction with private actors. The proliferation of multilateral bodies consisting of private actors, along with the growing jurisprudence of holding social media platforms accountable for discharging a 'public function' seems to support that observation. Private sector actors are not new to discharging public functions, of course. Microsoft, for example, along with the French government championed the Paris Call for Trust and Security in Cyberspace. While some scholars like Duncan Hollis argue that this sort of a public-private partnership is vital to effective global governance, questions remain about the public values at stake when a private company creates the norms that regulate them.

Further, arriving at a balance between two core competing values of free speech and public order should not be left to a handful of firms, largely based in the Bay Area. Private sector companies do not have the resources to frame regulations in a manner that render themselves scrutable to differing constitutional standards across the globe. Therefore, the only solution is for governments to devise regulations themselves while adopting an open consultative process to understand the concerns and needs of social media companies. After the Intermediary Liability Guidelines were released in late 2018, the Indian government did make it a point to put out a request for public consultation. Till the revised draft is made public, however, we will not know the extent to which the concerns put forth by social media companies were taken note of by the government.

Second, a daunting challenge for global governance in this arena is that one-size-fits-all strategies rarely work. Cultural contexts and constitutional protections of free speech differ across the world. The impact of online speech plays out differently in the Global South with its unique social cleavages. In 2017-18, there were fifty-six cases of lynchings of alleged child abductors in India, catalysed by videos spread through encrypted private mes-

saging platform WhatsApp. On the other hand, concerns in the United States or UK have centred around the spread of misinformation or hate speech on platforms like Facebook or Twitter – as was laid bare in the aftermath of the Cambridge Analytica scandal.

One of the best-known gambits to combat fake news by Indian Police Service (IPS) officer Rema Rajeswari utilized folk songs and ballads to spread awareness on misinformation in rural areas in Telangana. This method was customized and designed for governing misinformation at the grassroots level in a very specific context. Despite the noble intentions of global governance efforts like the Christchurch Call or the rigorous work of the Freedom Online Coalition, their impact on domestic regulations will likely be limited. The high-level regulatory guidelines and commitment to principles is dependent on how these principles are shaped and implemented across the world – something that depends on the action of the federal, and as we saw in Telangana district administrations.

This heterogeneity differentiates global governance on social media from other topics discussed in this issue such as 5G, data or autonomous weapons systems. Those are transnational problems that require well defined, robust and implementable transnational solutions. There is no transnational solution for governing free speech on social media. Any solution necessarily needs to be bottom-up and context-specific, and social media companies need to comply with the sovereign writ of any jurisdiction they are operating in.

Global governance arrangements can help by encouraging countries and social media companies to outline their commitments, share best practices and facilitate dialogue. Regulatory success, however, depends on local efforts – in India as anywhere in the world.

India and the global battle for data governance

ARINDRAJIT BASU and KARTHIK NACHIAPPAN

OFTEN touted as the new oil or electricity, data is playing a key role in shaping the political, economic and social trajectory of countries. Insights driven through analytics derived from the volume, velocity and variety of big data fuel industry, government and communication in many ways. The governance of data and its free-flow across territorial borders, however, continues to be a sticking point at global fora, with countries looking to unlock economic gains from regulatory efforts both domestically and globally.

Broadly speaking, the debate hinges on an ideological split between two coalitions. On the one hand, the US and the developed world are seeking to maintain the free flow of data across borders with minimal government intervention. On the other hand, emerging economies led by the BRICS countries are focusing increasingly on 'data sovereignty' or the sovereign right of all countries to regulate data, as they see fit, without external interference. Galvanizing this discourse is the cry of 'data colonialism' or the idea that foreign technology firms (based largely the US) are reaping profits from the data generated by citizens from the Global South, data that should instead be used for improving welfare and public service delivery and furthering economic development.

Through domestic regulatory efforts and outlining international positions, India has indicated a desire to take on a leadership role vis-a-vis global data governance. This article first frames the key global debates on data governance. Next, it analyses the politics and policy behind India's domestic efforts to regulate data and gauges how India can shape global debates by leveraging both its econo-

mic and demographic capacities and burgeoning domestic policy ecosystem.

Cross-border data flows are essential to the growth of digital economies. While states like India look to advance digitization trends, they also seek to protect their digital industries and firms through new data rules, issues that have increasingly acquired strategic importance. These regulatory processes, however, have not gone unchallenged. They are increasingly shaped, influenced and strained by global rules on data, notably free trade agreements, but also through other global rule-making platforms like the G-20 and specific laws certain powerful market powers, like the US, pass which are then used to influence domestic regulatory efforts covering data. In the section below, we look at the different global governance efforts that influence data rules across the world.

To prevent the domestic regulation of data from stymieing cross border trade and economic innovation, certain international organizations, like the World Trade Organization (WTO), have been relying on free trade agreements. For the past decade, trade agreements have entered discussions on data; ironically, trade agreements have renewed the WTO's focus to look at issues not saturated by conflict as has been the case since the latter's failure at Doha largely due to developmental issues. Besides the WTO, digital trade and data discussions have become an integral part of negotiations driving different types of free trade agreements, including some mega-regional trade agreements like the Trans-Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (TTIP).

Most WTO agreements covering issues like goods and services are the result of the Uruguay Round Trade Agreement in 1994; but these rules and those that followed under the WTO's remit did not keep pace with the rise of the internet which has, since then, revolutionized economic activity. Despite claims that WTO principles, like the Most-Favoured Nation and National Treatment, and existing mechanisms, like dispute procedures, subsidies and trade facilitation, were adequate for this transcendent cyber shift, it was clear that more specific rules and provisions were necessary to adjudicate, for instance, whether certain digital activities, like apps or related online activities, were a 'good' or a 'service'.

Classification proves critical given existing rules, like the General Agreement on Trade in Services (GATS) that govern that particular activity. For instance, slotting online platforms and services under the GATS will require compliance with the core National Treatment provision. This will diminish national control over digital industries since countries will have to provide equal access to foreign services suppliers, treating them like domestic firms which will likely be resisted given the growing importance of digital trade and the internet to economic growth.

Broadly, the consideration of digital trade, even data, has lagged at the WTO given the organization's pronounced inability to use existing rules like GATS to sort out issues pertaining to online commerce despite the creation of the WTO Work Programme on E-Commerce. The patent inadequacy of the WTO to multilaterally resolve questions surrounding data and digital trade have compelled countries to pass measures under the guise of 'localization' (forced storage or processing of data within national borders) that inhibit digital trade.

These localization rules generally favour domestic over foreign firms given the nature of obligations, particularly when it comes to data, that foreign firms must follow. Though WTO rules can discuss and resolve these matters under the rubric of digital trade, including data, the desire to move along these lines has not been forthcoming given long-standing political difficulties and little appetite from key countries like the US and EU. With the Doha round largely on life support, multilateral rule-making on digital issues has shifted from the WTO to other avenues – bilateral, regional and plurilateral.

Key economic powers like the European Union and the United States are now using trade agreements and domestic rules to export digital standards, some covering data protection and flows, to ensure their companies have sufficient access across markets and sufficient exemptions from local digital rules. The United States has been prolific at using the Free Trade Agreement (FTA) route to enact its 'digital agenda'; in fact, the US has reached free trade agreements with several countries that include WTO-plus provisions vis-a-vis digital trade, regulating issues like e-commerce, cross-border supply of services, protection of intellectual property rights and cooperation on ICTs.

Unlike the US, the EU has moved gingerly on using FTA's to manage digital trade issues, particularly data. The EU has sought robust commitments from its FTA partners like Canada, on data, expecting those keen to trade with the EU to internalize robust international standards on data protection. Besides bilateral FTAs, there has been a clear impetus to cover digital issues and data under mega-regional trade agreements – Transatlantic Trade and Investment Partnership (TTIP) between the EU and the US and the Trans-Pacific Part-

nership (TPP) between US and 11 Asia-Pacific countries. The TPP, which the US withdrew from after Trump's election, explicitly barred the use of data localization requirements while TTIP's discussions on data have been constrained by the EU's GDPR, which has a strong data protection standard.

Finally, the G-20, under Japan's leadership in 2019, entered global data discussions to generate consensus amongst countries that have different positions and stakes on how countries should draft and manage data policies such that it does not hinder trade and investment. At the G-20, Japanese PM Shinzo Abe formally declared the launch of the 'Osaka track' as a framework that advances the cause of cross-border data flows with sufficient protection. The core concept driving the framework was 'data free flow with trust' that called for a set of international rules which would enable the free movement of data across borders embedded with provisions that protect personal information, intellectual property and cyber security. Abe's initiative struck a chord amongst most countries present, especially the notion that supporting the growth of digital economies requires a reliable set of rules that hinge on data flows.

Though most countries, including the US, endorsed Abe's plan, the initiative did not pass muster with some vital Asian countries with booming digital economies including India who reserved judgment. Hurdles and divisions remain. The European Union feared whether the US and Japan were going to sacrifice privacy considerations at the altar of digital innovation while China, Russia and India demurred for other reasons. G-20 is not likely to find common ground on the issue of data flows. This fragmented global data landscape compels us to map what key actors like India are doing on the domestic policy front, as domestic developments are increasingly likely to shape the global regulatory agenda.

The past couple of years have seen the release of a number of policy interventions on data governance by various government ministries and departments in India. While connected by the common 'data sovereignty' vision or using data for pursuing economic development and empowering vulnerable communities, there are several inconsistencies and loopholes in these policies.

The first major policy move on data localization started with a notification from the Reserve Bank of India in April 2018 compelling the storage and processing of all payments data in India. WhatsApp, Google Pay and Mastercard, along with a number of foreign companies are prioritizing compliance with this directive to retain their position in India's burgeoning payments sector. The RBI directive was followed by several notifications mandating various forms of data localization across a variety of sectors including health care, e-commerce, and insurance.

The most sweeping of these was a draft of the August 2018 Personal Data Protection Bill. The draft bill contained a mirroring provision, which mandated that a copy of all personal data be stored in India. It also contained a provision restricting cross border transfers for all data that the government notified as 'critical personal data'.

While the Srikrishna Committee, which authored the draft bill, specified a number of reasons justifying this measure in its accompanying report, two in particular stood out. First is the long-winded process that Indian law enforcement agencies must go through to access data stored in the US. Indian law enforcement authorities have recognized this gap as a major fetter to running criminal investigations. Second, data localization could enable Indian companies that want to use data driven decision making tools to access and use data for their economic benefit.

Unsurprisingly, large Indian technology companies – Reliance, Paytm and PhonePe – already have data centres in India or can pay for their data to be stored in a local data centre. Large Chinese companies – Alibaba and Xilinx – have also taken pro-localization stances possibly because they too have data centres set up in India.

But this move toward data localization was vocally opposed by several US tech companies who abhorred the move. Facebook Public Policy Vice President Nick Clegg and Google CEO Sundar Pichai, along with lobbying groups such as the US-India Strategic Partnership Forum (USISPF), US-India Business Council (USIBC) and National Association of Software and Service Companies (NASSCOM) made several trips to New Delhi to bring home that message.

The industry-driven lobbying worked in tandem with the US government, as data localization became an increasingly vital part of the agenda in bilateral trade talks. In fact, Secretary of State Mike Pompeo reportedly contemplated limiting the number of H1B visas granted to Indian citizens if the localization provisions were not relaxed. President Trump himself made a public statement explicitly denouncing data localization at the G20 Osaka Summit. However, lobbying by the US and western government officials and the tech industry appears to have worked. When IT Minister Ravi Shankar Prasad introduced a revised version of the bill in Decem-

ber 2019, the mirroring provision was gone.

In its new form, the bill only requires the storage of 'sensitive personal data' in Indian territory, a subset of what was required under the mirroring provision. Sensitive personal data can be transferred abroad for processing if certain conditions are fulfilled. First, explicit consent must be obtained from the data user (called 'data principal'). Second, the transfer must be in pursuance of a contract or an intra-group scheme that safeguards user rights and plants liability on the data processor.

As an alternative, 'sensitive personal data' may be transferred abroad on a case-by-case basis if the data is accorded equivalent protection in that jurisdiction. Further, Indian law enforcement authorities must be granted access to the data if they need it for conducting criminal investigations. Like the previous version of the bill, the Indian government retains the power to notify any data as 'critical personal data', which must be *stored and processed* only in India.

Enabling the use of non-personal data for public service delivery meshes with India's policy objective of data for development. However, these efforts are often incoherent. For example, the Data Protection Bill defines non-personal data unhelpfully as 'anything that is not personal data', while providing the government the right to access both non-personal data and 'anonymized personal data' when it deems fit, although these two categories should be treated differently.

Further, various government entities follow varying conceptions of non-personal data. The draft e-commerce policy released in March 2019 by the Department for Promotion of Industry and Internal Trade (DPIIT) under the Ministry of Commerce (MOC) looks at non-personal data and anonymized personal data as 'community data', seemingly indicating that all Indians should benefit from data generated by each other. Chapter 4 of the Economic Survey of 2019 released by the Finance Ministry states that any data held by the government should be utilized for the 'public good' while strangely allowing private actors to bid for this data and use it for data-driven decision making.

A committee set up by the Ministry of Electronics and Information Technology (MEITY) was established to clarify the governance of 'non-personal data' but their report is yet to be released, thereby compounding the policy uncertainty. Given the public views of the members of this committee, it will likely prioritize state sovereignty over corporate ownership or individual control whenever the report is finally released.

India has significantly ramped up its engagement with global data debates this past year. India's positions have been an extension of their domestic policy ambitions, embracing 'data sovereignty', countering 'data colonialism' and retaining publicly generated data to aid state power particularly when it comes to public service delivery and welfare provision. India will likely push for global data rules that advances and shields the role of the state.

At the G20 Summit in Osaka last year, India, alongside BRICS countries underscored the critical role that data plays in the development of emerging economies, and did not sign the Osaka Declaration on Digital Economy that was the trigger for the 'Osaka Track' discussions. Foreign Secretary Vijay Gokhale reiterated that global rule-making on data transfers must not take place in plurilateral forums outside the WTO as doing so would reduce the say emerging economies could have in shaping the debates.

Since then, however, India appears to have softened its position given shifting interests. For example, while India's decision to opt out of the Regional Comprehensive Economic Partnership (RCEP) was driven by reasons other than data localization, disagreements on cross-border data flows occupied centre stage. At the Bangkok negotiation rounds in October 2019, India blocked both the financial services agreement and the e-commerce chapter because acquiescing to these rules would interfere with its 'essential security interest and national interests.' However, within ten days, reports indicated India moved away from its initial hardline stance and allowed the passage of the e-commerce chapter with exceptions provided for 'essential security interests' and 'legitimate public policy objectives.'

This flexibility on data localization was underscored through the revised Personal Data Protection Bill, discussed above, where the data localization provision was diluted significantly. It will be interesting to see how India approaches the data debate in upcoming bilateral engagements, most significantly as it negotiates a Free Trade Agreement (FTA) with the European Union.

Ultimately, robust global engagement on questions related to data will be difficult in the absence of settled domestic policy. The slew of incoherent and seemingly schizophrenic domestic policies diminishes the value of India's 'data sovereignty' message abroad. A better coordinated approach that resolves conflicts and uncertainty generated by piecemeal approaches adopted by several ministries is the need of the hour. International rules that embody and advance data sovereignty cannot eschew or compromise the individual sovereignty of Indian citizens.

Playing the long game on autonomous weapons

TRISHA RAY

THE term 'killer robots' is an oft-invoked shorthand used to describe Autonomous Weapons Systems (AWS), systems capable of detecting, selecting and engaging targets without human intervention.[1] However, this term glosses over the fact that no bright line separates the intelligent technologies used by the military and civilian sectors.

AWS governance must balance the strong interests countries have in their potentially game-changing battlefield applications, the economic growth potential of related AI technologies for countries preparing for the Fourth Industrial Revolution and questions regarding the ethics of AI decision making. As a result, AWS is a battleground where national, economic and ethical imperatives collide. India's stance on AWS at global fora is, accordingly, ambivalent by design, reflecting the complex interaction of economic considerations, national and regional security implications and concerns regarding democratic accountability.

1. This definition parses various characteristics proposed by experts at the UN GGE on LAWS, though there is currently no international legal definition of AWS. Further characteristics, highlighted in the 2019 report, include: self-adaption; predictability; explainability; reliability; ability to be subject to intervention; ability to redefine or modify objectives or goals or otherwise adapt to the environment; and ability to self-initiate.

This article will lay out the state of play on the global governance of AWS and highlight three defining characteristics of India's position on AWS which are driven by a need to first, meet its national security needs; second, balance regulation with AI-enabled growth; and third, meet its obligations as a democratically accountable government. In the context of the economic growth imperative, conflict amongst international stakeholders on the definition of AWS, and thereby the technologies that would come under stricter regulation, will also be explored.

Global governance of autonomous weapons falls under the purview of the UN Conference on Disarmament (CD). From 2014 to 2016, discussions were held at the CD's Informal Meetings of Experts that laid out the groundwork on areas of consideration including the importance of humanitarian law, responsibility, accountability and proliferation risk. Since 2017, discussions have been held at the Group of Governmental Experts on Lethal Autonomous Weapon Systems (GGE on LAWS).

The GGE has agreed upon seven broad principles. First, human accountability cannot be transferred to machines; machines and human beings cannot be treated the same way under law. Second, humans are accountable at all stages of the development, deployment and use of LAWS. Third, international humanitarian law (IHL) is applicable to the development, deployment and use of all emerging weapons systems. As stated in Article 36, Protocol 1 of the Geneva Convention, states are liable based on their obligations under international law, including IHL, to determine whether all emerging weapons systems are in compliance. Fourth, states are responsible for the physical and non-physical safeguards for LAWS. States must take measures to secure weapons systems against theft, damage and cyber attacks by other state and non-state actors.

Fifth, policy measures under the aegis of the United Nations Convention on Certain Conventional Weapons (CCW) should not hamper peaceful use of emerging technologies. Sixth, human-machine interaction at various stages of development, deployment and use of AWS should ensure adherence to IHL. Seventh, states are free to conduct independent legal reviews of AWS and allied technologies and are encouraged to share best practices.

Generally, country positions on AWS fall along a spectrum: from countries calling for a complete ban; to those who claim that any regulation beyond existing limitations set by international law is unnecessary or infeasible; and finally, others who propose regulated development of AWS. For the sake of brevity, this paper labels these groups the absolutists, the laissez faire-ists and the regulators respectively.

The absolutists demand a complete ban on the development and use of fully autonomous weapons systems. The African Group called for a moratorium on the development and manufacture of all AWS until a complete ban is in place. The absolutists have distinct priorities driving their positions. For some like Pakistan – which in 2013 became the first country to call for a ban – the primary concern is that developing countries without access to such technologies will be disproportionately harmed. For others, like Zimbabwe and Chile, the delegation of life and death decisions to a machine is unacceptable and inhumane.

Mexico believes that fully autonomous systems cannot, by definition, meet the standards of accountability and responsibility set by the Geneva Conventions. Morocco voiced concerns about the start of a new high-tech global arms race that would undermine non-proliferation and disarmament. As of October 2019, the Campaign to Stop Killer Robots lists 30 countries that have called for a prohibition on fully autonomous weapons.

The laissez faire brigade, consisting of twelve states including the UK, Australia, Israel, South Korea, Russia and the United States, oppose an international treaty on AWS. Russia and the US have both asserted that AWS will be less prone to error than systems with human operators hence reducing collateral damage and harm to friendly forces. A report from the NGO, Reaching Critical Will, on the August 2018 GGE meeting, noted that the US and Russia questioned whether IHL could apply to AWS at all, marking a reversal on declarations made by both countries during previous expert meetings.

Australia and the UK consider a sweeping prohibition of AWS, at this stage, premature. British officials state that, according to their own parameters, no existing weapons system qualifies as autonomous.

The regulators occupy the middle ground: many advocate for a new instrument, legally binding or otherwise, under the aegis of the CCW that establishes parameters such as meaningful human control and accountability. Austria, Brazil and Chile made a joint submission to the August 2018 session of the UN GGE proposing the negotiation of a legally binding instrument on 'meaningful human control over critical functions in lethal autonomous weapons systems.' China, too, appears to fall in the regulator category, although its declared position is equivocal, at best.

While the Campaign to Stop Killer Robots includes China in the list of countries calling for a ban, it comes

with an asterisk – stating that China opposes the use but not the development of AWS. China's official position paper at the April 2018 GGE simply calls for a 'uniform standard' on national reviews on the development and deployment of AWS. Elsa Kania, a prominent China analyst, noted 'China's apparent diplomatic commitment to limit the use of "fully autonomous lethal weapons systems" is unlikely to stop Beijing from building its own.'

India has been an active participant in the UNCD process on LAWS since its inception. India's Ambassador to the Conference on Disarmament, Amandeep Singh Gill, led the first UN GGE till 2018. On AWS, India functions as a regulator, taking a measured approach when it comes to governing AWS. India's submissions to the Meeting of Experts and the GGE are sparse in detail but have a couple of key attributes. First, India prefers an emphasis on *light touch regulation*. India's statements at the CCW have consistently cautioned against 'premature, unnecessary' prohibitions and emphasized that related technologies should not be 'stigmatized'. In other words, stringent prohibitions on AWS-related technologies could jeopardize innovation.

Second is a c*ognizance of geopolitical and technological inequities*. India's stance on the applicability of international law on AWS development and use is nuanced; it highlights the importance of accountability and transparency, as well as the principles of proportionality, necessity and distinction. At the same time, regulations should not exacerbate existing technological gaps between countries. This latter belief has been a mainstay of India's stance on international governance of technologies, as epitomized by earlier positions on nuclear weapons: Indian foreign policy emphasizes 'global, verifiable and *non-discriminatory* nuclear disarmament' due to a wariness of international regimes that limit its own ability to secure itself.

The two defining characteristics of India's stance on AWS – light touch regulation and acute awareness of existing inequities – are a product of the foreign policy imperative of having the latitude to develop technologies that may provide strategic advantages. This section posits that India's position as a 'regulator' on AWS is a product of, first, the exigencies of its security environment; and second, consideration of the effect such a ban would have on the development of India's fledgling AI industry.

India's grand strategy consists of three 'concentric circles': the immediate neighbourhood, the extended neighbourhood and the global stage.[2] India's conception of its security environment is similarly an interplay – manage relations with neighbours, create a stable regional security environment and maintain internal stability, all of which aid in its projection of itself as a military power. The 2018-19 Ministry of Defence (MoD) Annual Report mentions the following security issues: terrorism, insurgency, maritime security in the Indian Ocean region and land border security.

There are, therefore, a number of applications of AI in the Indian defence context. In its June 2018 report, the MoD Taskforce on AI made recommendations on applications of AI in aviation, naval, land systems, cyber, nuclear, and biological warfare. While the report itself was not made public, the following are potential uses for autonomous systems.[3]

Force multiplier and contested borders: India's Border Security Force (BSF) personnel endure extended exposure to extreme terrain and are under constant threat from unfriendly forces attempting to infiltrate the border. As a result, according to the Ministry of Home Affairs, between 2001 and 2016, 529 BSF jawans committed suicide and 491 died in combat. AWS can supplement human capabilities, and improve work conditions for soldiers on the ground thereby improving the border force's overall effectiveness.

Reducing human costs in urban theatres of conflict: Violence in Kashmir and Northeast India has resulted in 525 civilian deaths between 2014 and 2019, as reported by the Ministry of Home Affairs.[4] Fewer boots on the ground paired with continued improvements in AI-enabled situational awareness can greatly reduce civilian casualties and harm to friendly forces.

Defence in depth through persistent presence in the maritime domain: India faces three sets of maritime threats: the first is sea-borne terrorism as exemplified by the 2008 Mumbai attacks; the second, is piracy along important trade routes; and the third is naval incursions by hostile states. AWS can help maintain a persistent presence in areas that are difficult to monitor due to risks arising from climate, vast or difficult terrain, or unexploded ordnance.

The Defence Research and Development Organization (DRDO)

2. C. Rajamohan, 'India and the Balance of Power', *Foreign Affairs* 85(4), 0015-7120, 1 July 2006.

3. Trisha Ray, 'Beyond the Lethal in Lethal Autonomous Weapons', Observer Research Foundation, 14 December 2018.

4. For Kashmir, the reporting period stops on 31 March 2019. https://www.mha.gov.in/sites/default/files/AnnualReport_English_01102019.pdf. Unofficial estimates differ, with the Jammu Kashmir Coalition of Civil Society putting the death toll at 160 civilians in 2018 alone, as opposed to the MHA's 37 deaths. http://jkccs.net/2018-deadliest-year-of-the-decade-jkccs-annual-human-rights-review/

and a handful of Indian public sector undertakings (PSUs) are pursuing a number of projects on autonomous systems, including the *Ghatak*, a 'self-defending high-speed reconnaissance UAV', and unmanned combat aerial vehicles (UCAVs) in partnership with Israel Aerospace Industries.

Defence procurement has been dominated by PSUs, partly because procurement systems were skewed in their favour.[5] However, the armed forces have expressed their dissatisfaction with the glacial pace of DRDO's projects. One army officer told *The Print*, 'There needs to be a shorter incubation period. Many times, the forces have demanded a certain product, and by the time it comes out, it is more or less outdated, technology-wise.'[6] Acknowledging these concerns, the MoD AI Task Force's report emphasizes the role of the private sector, stating that innovative AI applications will emerge from private firms and start-ups. Accordingly, to foster partnerships with start-ups and MSMEs, the Government of India launched the Defence India Startup Challenge.

The Indian government, aware of the need for home-grown solutions to India's security challenges, is fostering research and development of autonomous systems and other AI-enabled military systems within the public and private sectors. Heavy-handed regulation of AWS would inhibit India's ability to foster innovative AI-enabled solutions for its chronic security challenges.

India's emphasis on light touch regulation and technological inequities at the UN GGE has an economic dimension as well. As Ambassador Amandeep Singh Gill said during an interview with the author at CyFy Africa in June 2019, '[India] is conscious not just of the security aspects but also the development opportunities, the economic transformation opportunities that are coming out of these technologies.'[7]

By 2025, the AI industry is projected to be valued at around $191 billion, which has driven many countries to draft national strategies that could increase their slice of this pie. India has done the same – the 2018 National Strategy on Artificial Intelligence highlights the transformative potential of AI for society, from expanding access to healthcare and finance, to improved agricultural practices, to easing the pressure on transport infrastructure.

One flaw with the UN GGE process is the absence of a single, meaningful definition of AWS that could coalesce country views. The Human Rights Watch defines AWS as systems that are able to select and engage targets, covering lower levels of autonomy, encapsulating functions present in many unmanned systems today. In contrast, the UK Ministry of Defence defines these systems as being 'capable of understanding higher level intent and direction.' The UK MoD defines AWS as being fully autonomous in that they require no human oversight or control. Fully autonomous systems with 'higher intent' presently exist only in science fiction. In the absence of clearly defined parameters for autonomy, AWS governance may cover a broad range of technologies that constitute these systems, including voice recognition, natural language processing, computer vision and sensor fusion, all of which have economic value beyond their military applications.

At the March 2019 convening of the UN GGE, the Indian delegation outlined the following five characteristics of AWS. *Autonomous*: Independent functioning till the terminal phase, following activation, deployment or launch. *Situational awareness and adaptability*: Navigate autonomously, track a target, and adapt function to changes in environment. *Target identification and differentiation*: Differentiate between friendly and opposing forces. *Decision-making*: Ability of a fully autonomous system to take decisions on its own, *as opposed to pre-programmed actions* as per a given set of conditions. *Learning*: AWS would possess complex self-learning and adaptive capabilities. Hence AWS can determine a course of action when encountering an unfamiliar scenario.

This characterization would put India's endorsed definition closer to that of the UK. Barring launch or deployment, human control is absent at all stages of AWS functioning and the system would be able to learn and adapt to its environment. When considering the growth potential of AI technologies, this definition is a natural progression on the official Indian position that AWS regulations should not curb innovation.

While acknowledging the economic growth potential and security

5. 'India's Gross Defence Budget May Reach $112 bn by FY27 Clocking 11% CAGR: ASSOCHAM-KPMG Report', Assocham, 27 May 2018. https://www.assocham.org/newsdetail.php?id=6838

6. Snehesh Alex Philip, 'Army Wants DRDO to Take in More of its Personnel on Deputation, Give Them More Access', *The Print*, 18 October 2019. https://theprint.in/defence/army-wants-drdo-take-more-personnel-on-deputation-give-them-more-access/307788/

7. '#CyFyAfrica | In Conversation on Encoded Lethality: The Effect of Autonomous Systems on National Security with Trisha Ray, Junior Fellow, ORF with Ambassador Amandeep Gill, UN Secretary General's High Level Panel on Digital Cooperation', Facebook video, Observer Research Foundation, 8 June 2019. https://www.facebook.com/ORFOnline/videos/332975220702468/

applications of AI, domestic support for the development of autonomous weapons is by no means unanimous. Thus, while a 2019 online poll by Ipsos had India recording the most support for fully autonomous weapons systems (50% of respondents) of the surveyed countries, 37% opposed AWS, with the primary concern being accountability.[8]

Accountability is central to a democracy like India and autonomous weapons epitomize the sharpest anxieties regarding the government use of new and emerging technologies for suppression and control. For instance, Home Minister Amit Shah stated during his speech in the Lok Sabha on 11 March 2020 that authorities used facial recognition software, in conjunction with driving licence and voter ID databases to identify protestors. India has also achieved the dubious distinction of leading the world on internet shutdowns, with more than 350 shutdowns between 2014 and 2019.[9]

Buried in India's statement at the 2014 Meeting of Experts on LAWS is an important driver of India's measured stance on AWS: 'From India's points of view, we would like […] increased systemic controls on international armed conflict embedded in international law in a manner that does not [...] encourage the use of lethal force to settle international disputes just because it affords the prospects of lesser casualties to one side or that its use can be insulated from the dictates of public conscience.'

For the Indian state, stability, whether one defines it in economic or hard security terms, is indelibly linked with the mandate of its people and the legitimacy gained at the global stage as a responsible actor. India's active participation and engagement with the CCW AWS process ensures that it will help shape global rules that best serve its interests as an aspiring global power while retaining the trust of its citizens.

References

Hayley Evans, Natalie Salmanowitz, 'Lethal Autonomous Weapons Systems: Recent Developments', *Lawfare*, 7 March 2019.

https://www.lawfareblog.com/lethal-autonomous-weapons-systems-recent-developments

Anja Dahlman and Marcel Dickow, 'Preventive Regulation of Autonomous Weapon Systems: Need for Action by Germany at Various Levels'. SWP Research Paper 2019/RP 03, January 2019.

Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects. ICRC submission to the LAWS expert meeting, Geneva, Switzerland, 26-28 March 2014.

Campaign to Stop Killer Robots. Stopkillerrobots.org, 'Shifting Definitions – the UK and Autonomous Weapons Systems', Article 36, July 2018.

http://www.article36.org/wp-content/uploads/2018/07/Shifting-definitions-UK-and-autonomous-weapons-July-2018.pdf

'Annual Report 2018-19', Ministry of Defence. https://mod.gov.in/sites/default/files/MoDAR2018.pdf

'Statement by Ambassador D.B. Venkatesh Varma at the CCW Experts Meeting on Lethal Autonomous Weapons Systems', 13 May 2014.

https://www.unog.ch/80256EDD006B8954/(httpAssets)/56839DAAD755FFC9C1257CD8003E65FD/$file/India+LAWS+2014.pdf

'Statement by Ambassador D.B. Venkatesh Varma at the CCW Informal Meeting of Experts on Lethal Autonomous Weapons', 17 April 2015.

https://www.unog.ch/80256EDD006B8954/(httpAssets)/FCCEC7D562B876E9C1257E2A0041E28D/$file/2015_LAWS_MX_IndiaConc.pdf

'Statement by Ambassador D.B. Venkatesh Varma at the CCW Informal Meeting of Experts on Lethal Autonomous Weapons', 11 April 2016.

https://www.unog.ch/80256EDD006B8954/(httpAssets)/2BE1A62650F95B8AC1257F920057AEED/$file/2016_LAWS+MX_General Exchange_Statements_India.pdf

'Statement by India – Characterization of the Systems under consideration in order to promote a common understanding on Concepts and Characteristics relevant to the objectives and purposes of the Convention', 25 March 2019.

https://www.unog.ch/80256EDD006B8954/(httpAssets) F8C1F0AEE961CA93C12583CC00353A09/$file/25+March+2019+-+5(d).pdf

'Statement by India: An exploration of the potential challenges posed by Emerging Technologies in the area of Lethal Autonomous Weapons Systems to International Humanitarian Law', 26 March 2019.

https://www.unog.ch/80256EDD006B8954/(httpAssets)/4C330E6B0BDD4C20C12583D2003C36AF/$file/5+a+26+Mar+2019+forenoon.pdf

'Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS) 13-17 November 2016, Opening Statement', submitted by the United States (13-17 November 2016).

https://www.unog.ch/80256EDD006B8954/(httpAssets)/6E9C8002759032A8C12582490031466C/$file/2017_GGE+LAWS_Statement_USA.pdf

'Potential Opportunities and Limitations of Military Uses of Lethal Autonomous Weapons Systems', submitted by the Russian Federation (9 March 2019).

https://www.unog.ch/80256EDD006B8954/(httpAssets)/489AAB0F44289865C12583BB0063B977/$file/GGE+LAWS+2019_Working+Paper+Russian+ Federation_E.pdf

'Australian Statement - General Exchange of Views', 13-17 November 2017.

https://www.unog.ch/80256EDD006B8954/(httpAssets)/E4B1B901E6728457C125823B0041DB57/$file/2017_GGE+LAWS_Statement_Australia.pdf

Ray Acheson, 'New Law Needed Now', Reaching Critical Will, CCW Report, Vol. 6, No. 9 (30 August 2018).

http://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/reports/CCWR6.9.pdf

Ray Acheson, 'Mind the Downward Spiral', Reaching Critical Will, CCW Report, Vol. 6, No. 11 (4 September 2018).

http://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/reports/CCWR6.11.pdf

8. It is important to note that opposition to AWS in India, as compared to a 2017 survey by the same organization, has gone up six percentage points.

9. Nikhil Rampal, 'More Than 350 Internet Shutdowns in India Since 2014', *India Today*, 18 December 2019. https://www.indiatoday.in/diu/story/more-than-350-internet-shutdowns-in-india-since-2014-1629203-2019-12-18

India's approach to global export control regimes

SAMEER PATIL and ARUN VISHWANATHAN

AFTER the end of the Second World War, as nuclear and other new weapons technologies began to be coveted by more states, western states that had advanced knowledge of these technologies, scrambled to control their spread. Dinshaw Mistry has described the aim of multilateral export control regimes as 'technological containment'. This description is particularly astute given the fact that in a majority of the cases, the technological 'haves' were the developed countries and access to these technologies was being denied to developing countries.

Therefore, the geo-political and geo-economic dynamics driving the export control regimes cannot be disregarded. In fact, during the Cold War, the dynamics of competition between the western and Soviet power blocs further hastened these efforts. Given its destructive potential, nuclear weapons technology figured at the top of their efforts. While India, along with other non-aligned states vociferously canvassed nuclear disarmament, western states concentrated on nuclear non-proliferation and shaping a safeguards system. For restricting the spread of other military technologies, they focused on harmonizing national export laws. This article will trace the evolution of the international export control regimes and the changing nature of India's engagement with these regimes.

These efforts materialized early on as the western countries in 1950 instituted the Coordinating Committee on Multilateral Export Controls (COCOM). It aimed to restrict transfers of military and dual-use goods and technologies to countries which were part of the Soviet bloc. It was followed by the formation of the 'Ottawa Group' in 1959, consisting of the United Kingdom, United States, Canada, South Africa and Australia. This grouping was primarily interested in assisting the creation of a nascent international nuclear safeguards system.

Initially, India led the global effort to create norms for nuclear non-proliferation and disarmament. Prime Minister Jawaharlal Nehru, as independent India's first Prime Minister, External Affairs Minister and Minister of Atomic Energy, utilized every available global forum to champion nuclear disarmament. Yet, with the emergence of discriminatory Nuclear Non-Proliferation Treaty (NPT) regime in 1968, New Delhi effectively found itself against the emerging consensus on non-proliferation. Its peaceful nuclear explosion (PNE) in May 1974 at Pokhran, Rajasthan, further solidified this exclusion, as it expedited the creation of the Nuclear Suppliers Group (NSG) – the most dominant of the current global export control regime. The roots of the NSG can be traced to the 'Ottawa Group' of 1959,

but both the International Atomic Energy Agency (IAEA) Information Circular 539 as well as the NSG documentation list out 1975 as the year of establishment of the NSG, initially known as the 'London Club'.

The aim of the 'London Club' or the NSG was to prevent the spread of nuclear material and technology for the development of nuclear weapons. However, it became clear to the US that for the group to be effective, it had to include western European nations like France and Germany, which had access to enrichment and reprocessing and other critical technological processes. In fact, France, which had not signed the NPT, was included as a member of the NSG. Moreover, as Yogesh Joshi has pointed out, India too was courted by the US in June 1977, just three years after the 1974 PNE. This shows the United States' interest in expanding NSG membership to all countries with access to nuclear and related technologies. The group continues to strike a delicate balance between proliferation concerns which were the US's focus, and protection of national and commercial interests of European countries.

Today, along with the NSG, there are three other regimes which seek to restrict proliferation, sale and transfer of different weapons technologies and their delivery systems. These include the Missile Technology Control Regime (MTCR), the Wassenaar Arrangement (WA) and the Australia Group (AG). The principal focus of the MTCR lies in the domain of rocket systems and unmanned air vehicles, seeking to limit the spread of missiles and missile technology. The WA seeks to restrict transfers of conventional arms and dual-use goods and technologies, while control of chemical and biological weapons (CBW) is the domain in which the AG focuses. In sum, these four groupings function akin to 'trade cartels' by controlling the supply of materials, technology and 'dual-use' items in their respective domains.

These regimes are informal associations of countries sharing a common interest and do not have the sanctity of an international treaty. They operate on a consensus basis – giving these regimes the needed authority to interact and cooperate. Accordingly, member states agree to voluntarily implement the national export controls, in compliance with these regimes.

The MTCR was established in 1987 by the United States along with six other founding members – the UK, France, West Germany, Italy, Canada and Japan. MTCR's establishment also saw the release of guidelines and annexe(s) listing technologies which MTCR members could not export. The regime focuses on 'rockets and unmanned aerial vehicles which are capable of delivering a payload of at least 500 kg to a range of at least 300 km and on equipment, software and technology for such systems.' Initially, these restrictions were voluntary and to be applied by members on an independent basis, especially if the technology or item was to be used in a nuclear weapons delivery system, which was subsequently expanded to cover all WMDs.

The initial MTCR membership mainly covered the western countries; after the Cold War, however, it expanded at a rapid pace. Currently, the MTCR has 35 partner countries and three adherents – Estonia, Kazakhstan, and Latvia.

The AG regime was established in 1985 following the UN investigation team's discovery in April 1984 that Iraq had used chemical weapons in its ongoing conflict with Iran, thereby violating the 1925 Geneva Protocol. Investigations revealed that Iran and Iraq had manufactured chemical weapons by purchasing materials from the chemical industry worldwide. To prevent such behaviour, the AG regime seeks to control the export of equipment, materials, technology and software that could contribute to CBW activities. It maintains six common control lists related to the chemical weapon precursors, dual-use chemical manufacturing facilities and equipment, dual-use biological equipment, biological agents and plant and animal pathogens.

After the end of the Cold War in 1991, these regimes have expanded in scope and coverage to accommodate former Soviet bloc states and tackle specific cases of proliferation like the illicit network of Pakistani nuclear scientist A.Q. Khan. In 1992, for instance, the NSG adopted the full scope Warsaw Guidelines, which ensured that only NPT members and states that had full-scope safeguards in force could engage in nuclear trade with NSG members. Similarly, after the 1991 Gulf War, the MTCR guidelines were updated in January 1993 to cover delivery systems for weapons of mass destruction not just for nuclear weapons delivery systems.

In 1996, the Wassenaar Arrangement was born, replacing the COCOM. Just like its predecessor, WA sought to harmonize export control policies and implementation of national controls related to the trade in strategic goods and technologies related to computing, aviation, sensors and the telecommunications sector. It specifically focused on rogue regimes and the terrorist groups' efforts to acquire these technologies.

India remained outside these regimes, but its unblemished non-proliferation record signalled adherence with the spirit of these regimes. Ironically, whereas the Pokhran 1974

PNE solidified the creation of the NSG, the Pokhran 1998 nuclear tests marked the beginning of efforts to integrate India into the global export control regimes.

The United States, which had imposed sanctions following the 1998 tests, quickly reversed gears to engage India. In 1999, India and the US commenced their dialogue on security, non-proliferation, disarmament and related issues between Jaswant Singh (then Deputy Chairman, Planning Commission and subsequently the External Affairs Minister) and Strobe Talbott (the Deputy Secretary of State), stretching to 14 rounds. The Singh-Talbott talks proved inconclusive as a key part of the deal that India will sign the Comprehensive Test Ban Treaty fell through due to domestic opposition. Nonetheless, the dialogue gave the Clinton administration and the Capitol Hill a better understanding of the Indian worldview and its security concerns.

One of the critical watershed moments in the evolution of the India-US relationship was the September 2001 terrorist attack. This event led to the de-hyphenation of US' relations with India and Pakistan, generating greater strategic convergence between New Delhi and Washington. In January 2004, the two countries announced the Next Steps in Strategic Partnership (NSSP) initiative, where both agreed to expand cooperation in the areas of civilian nuclear cooperation, civilian space programmes, and high technology trade.

This development was followed by the 2005 Joint Statement by President Bush and Prime Minister Manmohan Singh, which initiated the dialogue for an Indo-US civilian nuclear agreement which heralded America's intention to overturn decades of non-proliferation policy, ushering India into the global nuclear order. The July 2005 Joint Statement and the passage of the 2006 Hyde Act in the US Congress resulted in the Indian commitment to harmonize its export control legislations and adhere to the NSG and MTCR Guidelines.

The India-specific exemption secured from the NSG in 2008 as a result of the 2005 Indo-US joint statement was critical for the future success of India's nuclear power programme which was suffering from a fissile material supply crunch. In fact, the fissile material stockpiles had reached such critical levels that the Indian nuclear plants were operating at around 50% of their capacity in 2007-08 as opposed to a high of over 80% of plant capacity in 2003-04. This deficit was due to the NSG's stranglehold on the global uranium supply chain as NSG member states control over 80% of global uranium reserves and production.

With NSG's adoption of the Warsaw Guidelines in 1992, India could not trade with the group members. These guidelines posed a problem as India was neither an NPT member nor could it accept full-scope safeguards given its nuclear weapons programme. In 2001, when the Tarapur nuclear power plant faced fuel shortage, Russia stepped in to supply fuel using the 'grandfather' clause in the NSG guidelines. However, given the pressure from the American and other NSG members, Moscow was unable to re-supply the plant in 2004 using the same clause. Thus, for India, the only way out was to secure an exemption from the NSG full-scope safeguards requirements, which it obtained in 2008. This also enabled it to import uranium for its nuclear power reactors from various countries, including Canada, Kazakhstan, and Australia and sign civil nuclear cooperation agreements with close to 15 countries.

With the shift in American policy to treat India as a partner in strengthening non-proliferation and export controls, Washington also began to put its weight behind India's case by bringing New Delhi into the fold of these regimes. Consequently, New Delhi acquired the membership of these regimes barring the NSG, in quick succession.

MTCR was first off the block as India became its member in June 2016. India's entry into the group can also be seen as turning a full circle, primarily because the group's origin can be traced back to concerns within the United States of the Indian SLV-3 test in 1980. Then in December 2017, India became the 42nd member of the WA. Before this, India had updated its export control lists for SCOMET (special chemicals, organisms, materials, equipment, and technologies) items, to harmonize with international and WA standards. Similarly, India became a member of the Australia Group in January 2018. This was an important recognition for India because chemicals are one of the most significant Indian exports.

While India's responsible non-proliferation record contributed in securing these memberships, what also worked in India's favour was that unlike the NSG, China is not a member of the WA, AG or the MTCR. Hence, Beijing was in no position to stonewall India's membership as it did in the case of the NSG, demanding membership for Pakistan too. Interestingly, though China has provided the US with a written commitment to abide by the MTCR, its membership application has been pending since 2004.

There has been a remarkable change in India's engagement with the export control regimes, with concrete benefits of these memberships manifested in the nuclear trade, defence modernization and civil space sector.

In 2000, for instance, the US Bureau of Industry and Security (BIS) required export control licenses for close to 25% of exports to India. The change in the nature of the India-US relationship and India's growing acceptance in American export control frameworks is apparent from the fact that post-2009, a majority of the exports did not require any clearance from the US Department of Commerce with less than 1% of American exports to India requiring a BIS export licence.

Similarly, a few months after the AG membership, in August 2018, Washington granted New Delhi, Strategic Trade Authorization-1 (STA-1) status, enabling the latter's access to high technology items in the civil space and defence sectors. Traditionally, the US has placed only those countries in the STA-1 list, which are members of all the four export control regimes. This status helped to advance the already thriving India-US defence trade, which has added considerable value to the Indian military's power projection capability.

Moreover, MTCR partner states get access to the international market for space launch of satellites by the US and other countries. Given India's low-cost advantage in this sphere, MTCR membership can benefit the Indian Space Research Organization (ISRO), if it is able to ramp up its capacity. Also, while the MTCR formally does not make a distinction between members, adherents and non-members, several of the regime's adherents have restrictions on working with non-members due to their domestic export control rules and regulations. Now with the MTCR membership, India will have access to important technologies in the domain of avionics, diagnostics, testing and evaluation, which could have been denied to India by the US and other western countries, as a non-member.

Membership of the MTCR, WA and AG is undoubtedly expected to serve as a stepping stone for India's membership to the NSG. An important reason why the NSG membership is vital for India is the fact that the group's membership will allow India to influence future modifications in the group's guidelines. Having the right to do so is important given India's growing investment in nuclear power as part of its climate change mitigation strategy. Besides, the NSG membership will grant India ease of access to the global nuclear market and provide it with 'equal partnership' in the R&D of new reactor systems. Without NSG membership, India's integration in the global nuclear security order will remain incomplete.

While these regimes have had much success in controlling the exports of conventional and CBWs, controlling exports of emerging dual-use technologies has proved to be challenging. A case in point is the non-members' exports of dual-use surveillance software. The revelations in November 2019 about the use of Pegasus spyware in India, demonstrated how software sold by the private industry could be misused to target human rights activists and journalists. The Israel-based company NSO GROUP sold the spyware; it claims the software helps governments in tackling terrorism and serious crime. But many organizations have documented the misuse of the software to target human rights groups, activists and journalists by several countries, without any proportionate accountability.

Israel has informally complied with the WA control lists that cover the dual-use software. Yet Tel Aviv's approach to export controls has waxed and waned; in 2016 it adopted stringent controls, but subsequently reduced the scope and strength of the license requirements for intrusion software exports.

In June 2019, the United Nations Special Rapporteur on freedom of opinion and expression, David Kaye, highlighted the role of tools such as computer intrusions, mobile device hacking, network intrusion and facial recognition used by the states for surveillance, with severe implications for the right to privacy. Kaye called for an immediate moratorium on the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place.

Ensuring accountability for human rights violations caused by the dual-use software exports will remain the next big challenge for the WA. And India, given its own domestic digital experience, is in a position to shape global debates surrounding the issue. It also gives India an opportunity to reprise its role as a contributor in shaping global norms, seven decades after Prime Minister Nehru advocated the cause of universal nuclear disarmament.

References

David Kaye, 'The Surveillance Industry is Assisting State Suppression: It Must be Stopped', *The Guardian*, London, 26 November 2019.

Deborah A. Ozga, 'A Chronology of the Missile Technology Control Regime', *The Non Proliferation Review* 1(2), Winter 1994, pp. 66-93.

Dinshaw Mistry, 'Technological Containment: The MTCR and Missile Proliferation', *Security Studies* 11(3), Spring 2002, p. 91.

International Atomic Energy Agency, 'Information Circular 539', April 2000, pp. 1-11.

Leonard Weiss, 'Safeguards and the NPT: Where Our Current Problems Began', *Bulletin of the Atomic Scientists* 73(5), August 2017, pp. 328-336.

National Security Archive, '60th Anniversary of the International Atomic Energy Agency', October 2017, Briefing Book No. 609.

Yogesh Joshi, 'Between Principles and Pragmatism: India and the Nuclear Non-Proliferation Regime in the Post-PNE Era, 1974-1980', *The International History Review* 21(2), January 2018, pp. 110-149.

India and global artificial intelligence governance

VIDUSHI MARDA

ARTIFICIAL Intelligence (AI) systems are increasingly embedded in society – from curating social media feeds and assisting law enforcement, to deciding an individual's creditworthiness and aiding in healthcare. There are at least two possible explanations for this recent and substantial mainstreaming of AI in everyday life. First, there is more computing power and data today than ever before. Second, due to this the possibility of using AI systems to predict and classify large amounts of data makes it fertile ground for governments and industry alike.

At the outset, it is crucial to ask: what do we mean by AI? AI, broadly defined, refers to the ability of computers to exhibit intelligent behaviour. It has existed as a field of computer science for over sixty years. The most recent wave of interest in AI has been spurred by one technique of AI, called machine learning (ML) – where algorithms train on data, uncover patterns and predict future outcomes by learning from this data.

Given the speed and scale at which these systems work, a number of incentives are at play. Some stakeholders view AI as a business opportunity, and look at ways in which scale, efficiency and deployment can be encouraged. The Chinese government, for instance, has laid down plans to be the world leader in AI by 2030, referring to this technology as 'a new engine of economic development.'

Others view AI as a leveller in society, and look at ways in which inclusion and widespread adoption of AI will help us solve complex problems like financial inclusion and access to healthcare. An example of this at an intergovernmental level is AI for Good, an annual summit organized by the International Telecommunications Union (ITU), which aims at scaling AI applications like sentiment analysis and credit scoring for global and inclusive impact.

Still others view AI primarily as sociotechnical systems and look at ways by which these systems can be

regulated to ensure that negative consequences such as discrimination and surveillance do not occur. In its national AI strategy, Germany recognizes the economic potential of AI, but underscores that underlying the strategy is the democratic desire to anchor AI in an ethical, legal, cultural and institutional context which upholds fundamental social values and individual rights.

These competing interests have given rise to a growing and textured conversation around the nature and extent of AI regulation and accountability in societies; a conversation which I broadly term 'AI governance' for the purposes of this article. In this article, I will shed light on what AI governance looks like internationally, map key arguments and concerns that have emerged, and finally analyse India's engagement with this landscape.

Given the multiple ways in which AI can be used in societies, one approach to governance has been to erect normative ethical frameworks that guide how AI should be designed, developed, and deployed. These frameworks are used by various stakeholders to indicate their priorities, considerations, and in some cases, also explicitly spell out use cases and principles that will not be pursued.

Governments have discussed ethics to varying degrees of detail in AI strategies (at the time of writing this essay, at least 50 state-led AI strategy documents have been released by countries around the world). The United Kingdom, for instance, has explicitly stated its aspiration to become the world leader in ethical AI. Other states like China and the United States focus more on the competitive edge and economic opportunities that these technologies can generate.

Ethical frameworks are also in place at an intergovernmental level. The European Union has multiple ethics initiatives underway, including Ethical Principles for Trustworthy AI published by the EU High Level Expert Group on AI. In May 2019, forty two nation-states signed the OECD's Principles for Trustworthy AI. Nordic and Baltic governments issued a joint declaration on AI that explicitly recognized the importance of 'ethical and transparent guidelines, standards, principles and values to guide when and how AI applications should be used.'

Ethics has also been championed by the private sector globally. In June 2018, Google published its 'AI Principles' publicly stating their intention to build socially beneficial AI systems that would not create or reinforce biases and would be safe and accountable. Google also included a list of applications the company would not pursue, which include technologies that cause overall harm, violate human rights, etc. Microsoft published ethical principles under the umbrella of 'Responsible AI' and constituted the AI and Ethics in Engineering and Research Committee (AETHER), to make recommendations on what AI technologies the company should deploy. Facebook responded to the chorus of ethical AI by funding a research institute at the University of Munich beside a dedicated AI ethics team.

Technical institutions like the Institute for Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM) have produced ethical principles for autonomous systems that ostensibly feed into technical considerations when designing and developing AI systems. Civil society and academia have also engaged with ethical approaches to AI systems – either as respondents to government and corporate consultations, through institutional proceedings at the UN and other similarly placed intergovernmental processes, or through multi-stakeholder spaces like the Partnership on AI.

This mushrooming of ethical initiatives is accompanied by skepticism surrounding their utility. Critics point out that ethical frameworks are often posed as an alternative or preamble to regulation, a phenomenon political scientist Benjamin Wagner has termed 'ethics washing'. The lack of accountability and redressal mechanisms surrounding ethical frameworks is made worse by the fact that existing principles are vaguely worded with no grounding in law. Even ethical standards for technical communities do not materially affect the design or development of AI – research has shown that the ACM code of ethics had no observed effect on the work of software engineers who were explicitly asked to consider it. The lack of teeth in ethical frameworks is particularly dangerous in context of state use of AI systems, as this could lead to a significant dilution of state accountability.

The fear of hampering innovation through regulation is one of the main reasons for the popularity of ethical frameworks. This tension has been in the public eye most explicitly through the G7's effort to kickstart the Global Partnership on AI (originally called the International Panel on Artificial Intelligence). This partnership was launched by France and Canada in December 2018 to address ethical concerns, establish shared principles and regulations to generate international consensus on the human rights impact of AI systems. All G7 countries have expressed agreement with these overarching goals, with the notable exception of the United States, which has responded cautiously. Subsequently, the US in January 2020 published a list of 10 principles for government agen-

cies to consider while formulating governance mechanisms for AI, encouraging a light touch approach to AI governance, and cautioned against heavy handed innovation killing models of regulation.

As a result, the field of AI regulation is far from homogeneous. At an abstract level, there is a tendency to claim that AI systems are so novel that they operate in a regulatory vacuum. This is not the case. Existing laws (at both national and international levels) can and must find application in context of AI; it is the extent to which they apply, and the ways in which they need to evolve that are the crucial questions now. Jurisdictions like the European Union are grappling with how traditions of democracy, rule of law and human rights can act as a regulatory mechanism for emerging technologies like AI and how they need to evolve. At the same time, existing regulation, at both domestic and regional levels, is already adapting. The General Data Protection Regulation, for instance, lays down data protection rights broadly and carves out some specific safeguards in context of automated decision making.

New forms of AI regulation are cropping up elsewhere too. Legislative proposals like the Algorithmic Accountability Act introduced in the US Senate in April 2019 seek to establish accountability mechanisms for uses of AI in the public sector. Another form of regulation are use-case specific bans. For instance, San Francisco became the first city to ban law enforcement use of facial recognition in May 2019 which other cities in the US also followed. In January 2020, the Trump administration also announced a ban on the export of certain AI systems for reasons of national security.

Calls for regulation also occur at the intergovernmental level. In 2018, the United Nations Special Rapporteur on freedom of expression appealed to UN General Assembly member states to apply existing standards of human rights, constitutional guarantees and sectoral regulation to the design, development and deployment of AI systems. The EU is also considering more regulation for AI. Other stakeholders like Google and Microsoft have also expressed the need for regulation.

It is important to note that an often overlooked, but crucial part of the governance puzzle is the stage of technical specification and standard setting for AI systems. The design and development of AI systems is technically determined through standardization bodies such as working groups within the IEEE, through technical actors and researchers like the Fairness, Accountability and Transparency in Machine Learning (FaccT/ML) community's efforts at refining technical approaches to ethical standards of fairness, accountability and transparency in machine learning.

Mapping India's engagement with the global governance regime is not a linear or neat process as there is a patchwork of initiatives, developments and contestation related to domestic governance structures. The Indian government's prioritization of AI has steadily increased driven by rising budgetary allocations towards AI. This is hardly surprising as AI falls at the intersection of multiple flagship projects of the Indian government. Digital India aims at making India a digitally empowered society by providing every individual digital infrastructure as a core utility. Make in India seeks to transform India into an international manufacturing hub, spurring the incentive for domestic design and development of AI systems. The 100 Smart Cities Mission is another initiative closely related to the Union government's approach to AI given its focus on providing 'smart solutions' to improve the quality of life of citizens in a sustainable environment.

In the last three years, there have been several policy documents that also directly refer to the development and deployment of AI. In March 2018, the Ministry of Commerce's AI Task Force published a report identifying key areas for AI in India, including healthcare, agriculture, national security, retail, etc. While framing AI as a socio-economic problem solver at scale, the report did not attempt to comprehensively discuss ethical and social implications of these systems, instead focusing on how the government can encourage growth in these sectors.

NITI Aayog's National Strategy for Artificial Intelligence, published in June 2018, states that India's approach to AI should be one that will 'leverage AI for economic growth, social development and inclusive growth, and finally as a "garage" for emerging and developing economies.' In May 2019, NITI Aayog proposed (and subsequently received approval for) a Rs 7500 crore budget to set up an AI framework for India with a view to push for greater adoption and institutional oversight. In parallel, the Ministry for Electronics and Information Technology (MEITY) has set up four committees in February 2018 to draft a policy framework for AI after recognizing AI's impact on the economy and society. Unsurprisingly, a turf war between the two agencies with concerns about duplication of work and funding reached a peak in August 2019, when MEITY requested the finance ministry to intervene and resolve issues.

While the exact form and central institution (if any) to govern AI is still evolving, the substantive focus and outlook of India's approach to AI is clear. AI is primarily seen as a tool

to fuel economic growth. However, India's strategy does not take a cookie cutter approach. While the financial impact of AI the biggest motivating factor, aspects such as inclusion and 'greater good' also featured prominently in NITI Aayog's #AIFORALL strategy.

There have also been a steadily growing list of *ad hoc* regulation in context of AI systems, usually honing in on the idea of data being a key resource and driving factor of India's AI future. At the time of writing this article, India does not yet have a data protection law. However, the draft data protection bill provides significant insight into the government's approach. For instance, data localization was a flashpoint throughout the process of drafting and discussing provisions of the bill; with Section 40 of the draft bill mandating that a government-defined class of 'critical data' must mandatorily be stored exclusively in India. A primary justification for this provision was that Indian players – government, private sector and research organizations – should have access to this data to locally develop and deploy emerging technologies like AI.

While the bill contemplates principles like purpose and collection limitation, explicit consent in case of sensitive personal data, it raises privacy concerns in one fell swoop – the government *can* exempt its agencies from all protections subject to procedures and oversight from the agency in question. This objective resonates with the Economic Survey published by the Ministry of Finance which states that personal data collected by the government becomes a 'public good' once anonymized. This is not the appropriate place for an in-depth discussion on the fallacy of anonymized data in context of machine learning. However, suffice to say that this will have significant implications in terms of how AI is designed, developed and deployed in India.

The private sector shares and plays a significant role in the government's aspirations for AI. There are several sectors identified by policy initiatives discussed above – spanning healthcare, agriculture, retail, urban development, mobility, education, law enforcement, etc. Discussing plans for future AI prioritization, government officials have mentioned that economic viability of applications for private actors will determine deployments, bringing to the fore questions about private-public partnerships and their impact on governance.

Across AI policy initiatives, ethics and human rights (primarily privacy) are mentioned but as an afterthought or formality at best. It is clear from mushrooming of use cases that the use of AI systems will be more opportunistic and driven by executive decisions, than deliberate and guided by ethical or regulatory norms. The use of AI systems is considered an efficient, desirable and useful step, in and of itself, without meaningfully engaging with the limitations of these technologies.

The national Automated Facial Recognition System (AFRS) demonstrates these threads of analysis comprehensively. In July 2019, the Home Ministry announced plans for the AFRS – a system that will use images from CCTV cameras, newspapers, police raids to identify criminals by matching these to existing records under the Crime and Criminal Tracking Network System (CCTNS). It would bolster nationwide intelligence sharing between police departments by having a centralized system for face recognition. Here, the exceptionalism afforded to shiny and 'efficient' technology is made apparent. Even in the face of overwhelming evidence to show that facial recognition is an unreliable technology, the limitations of these systems are ignored in favour of the potential for enhancing law enforcement capabilities.

The Home Ministry has not taken a clear stance which would suggest that it considers the ethical and legal implications of using facial recognition, which is particularly concerning when governments around the world are putting in place bans or at least strict regulation. In fact, the legal basis on which the AFRS stands is unclear. Responding to a legal notice from the Internet Freedom Foundation, the Home Ministry traces the legal basis for the AFRS to a Cabinet Note from 2009, which is, at best, a document of procedure, not of legal consequence. Further, the AFRS is afforded an exception to regulatory and ethical standards that the government otherwise adheres to, and runs counter to the fundamental right to privacy reaffirmed by the Supreme Court in 2017 in *Puttaswamy v. Union of India*.

In *Puttaswamy*, the court laid down a four-part test that any action infringing the right to privacy must satisfy: it must be demonstrated to be in pursuit of a legitimate aim, bear a rational connection with the aim and shown to be necessary and proportionate. The AFRS does not meet this constitutional standard

India's approach to AI governance is layered and simultaneously evolving. Domestic developments suggest how India will engage with international processes as and when they evolve. While primarily endorsing the business case and social inclusion narrative of AI, India has a long way to go insofar as understanding it as a sociotechnical system with the capacity to drive inequality, exclusion, surveillance and an erosion of constitutional and human rights.

As of now, it is clear that opportunistic, ad hoc decisions from the state

and private companies reigns supreme in the context of AI deployment, development and use. However, AI governance in India needs to mature to acknowledge the limitations, potential and impact of AI systems on daily life. Civil society is structurally excluded from the AI governance space, with government consultations (if any) being the only window for engagement. A majority of key decisions and deliberations are made by permutations and combinations of industry, government, and sometimes technical actors, and civil society is yet to be included. This exclusion is misguided particularly as the societal impact of AI systems become more apparent every day.

While global debates around the impact of AI systems place emphasis on India, particularly in context of how AI systems will impact employment and the future of work, there has been limited explicit engagement from home with these intergovernmental or multilateral initiatives. Beyond the policy and economic realms, there is growing indication that India will engage with AI standardization. The International Telecommunications Union is meant to set-up an innovation centre in India to incorporate technologies from South Asian countries and emerging economies in standards for technologies.

India has the opportunity to position itself as a thoughtful leader in the context of AI by drawing from its democratic foundations and experience of deploying technologies at scale. Instead of buying into the AI race for economic power, New Delhi should engage with the strengths and limitations of these systems and institute a deliberate and future proof strategy for the design, development, standardization and deployment of AI technologies. While industry and state interests have played a leading role thus far, it is important to note that effective AI governance must be multi-stakeholder in nature.

Interrogating India's quest for data sovereignty

DIVIJ JOSHI

IN February 2019, the Government of India released the Draft National E-Commerce Policy, which claimed among other things that 'the increasing importance of data warrants treating it at par with other resources on which a country would have sovereign right. It is said that data is the new oil.'[1]

Political and business leaders ranging from Prime Minister Narendra Modi to industrialists Mukesh Ambani and Nandan Nilekani have made claims of sovereign control over the amorphous category of 'data' and declarations of its economic potential as a natural resource. Such claims are also increasingly reflected in legal and policy developments in India ranging from WTO negotiations to data protection legislation, particularly the Personal Data Protection Bill, 2019.

These developments are of tremendous social and political consequence resulting as they are in the creation of pervasive new standards and architectures for the operation of the internet, and accordingly, for India's increasingly networked society. These developments mark an important break from India's historical approach towards internet governance; moreover, they are heavily influenced by concerns of trade and security with significant implications for various stakeholders who assert claims and interests over the internet and over the kind of 'data' they seek to control. As a result, it is imperative that both the historical development of this trend and its implications for India's law and policy are interrogated. This article explores the history of 'data sovereignty' debates in their geopolitical context as well as its roots in Indian policy and law. I argue that the recent claims of data sovereignty by the Indian government attempt to reconfigure power and control over the information society through the central government while leaving out other valid conceptions or imaginations of data governance.

There is a long history of competing claims and assertions of 'sovereignty' or control over the internet and, more recently, over 'data'. While concerns of sovereignty – asserting power or control over some domain – have long been primarily driven by governments and state actors, the technical architectures and historical development of the internet did and continue to present challenges to unambiguous assertions of state-sovereign authority over information flows.

1. Draft E-Commerce Policy, Department for the Promotion of Industry and Internal Trade, 23 February 2019. https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_ 23February2019.pdf

The internet has long held an exceptional status vis-a-vis assertions over the jurisdiction and control over the network's infrastructure, and particularly over its information flows, owing as much to its fundamental technical structure as to its historical development. The peculiar position of the internet has resulted in a number of other stakeholders asserting both functional and legal control over it. Consider, for example, the international multi-stakeholder organizations which develop the technical specifications, standards and protocols for network and data flows, such as the Internet Engineering Task Force (IETF) or the International Corporation for Assigned Names and Numbers (ICANN) which have deeply influenced the structure and governance of the internet. As Julie Cohen notes, these reflect emergent networked 'legal-institutional' structures of governance, which appear to 'operate according to their own rules in ways influenced by states but not controlled by them.'[2]

These legal-institutional actors and structures have been embedded in and influenced by dominant geopolitical concerns of trade and security. The evolving paradigms and politics of economic globalization, in particular, have deeply influenced the governance of the internet and of information flows. Many of the institutions and norms for the governance of the internet developed as an expansion of the idea of standardized rules for international commerce, mirroring the development of '*lex mercatoria*', which governed trade routes and maritime navigation. International organizations such as the WTO, responsible for the administration of these legal norms embedded in treaties like the General Agreements on Trade in Services, and particularly the treaty on Trade Related Aspects of Intellectual Property Rights became intrinsic to the governance of rights in networks and information flows. Historically driven by OECD countries, the USA in particular, these institutions and norms sought to repurpose the internet as a vehicle for securing their economic interests and political values. These norms also found purchase in the recently liberalized Indian economy, which was undergoing 'structural adjustment' to integrate with the globalized economy.

This situation produced norms which strengthened trans-border intellectual property protection in information (such as copyright protection in digital works), while establishing norms encouraging the 'free flow' of information as integral to the growth of the network. In May 1998, for example, the WTO adopted a 'moratorium' on customs duties for electronic transmissions, which denuded the authority of national governments to tax trans-border e-commerce transactions.[3] Similarly, the emergence of bilateral and multilateral free trade agreements like the Trans Pacific Partnership or the Regional Comprehensive Economic Partnership have attempted to entrench the power of large technology firms and industrialized Asia-Pacific nations, through specific 'data free flow' obligations and assurances against allowing governments access to the source code of algorithmic systems which employ data analytics capabilities. Binding trade obligations like these have been compounded by the nature of international taxation regimes for e-commerce, which have allowed dominant digital platforms to evade fair taxation.[4]

The hold of 'data' and the networked information economy over economic globalization has radically developed since these norms first evolved. In recent decades, a new form of 'informational capitalism' has emerged where 'data' or information created or abstracted from material forms of labour or capital is considered a factor of economic production, distinct from intellectual property laws. The rise of 'big data' and the algorithmic creation of 'artificial intelligence' have increasing economic value and seemingly limitless economic potential. Consequently, this scenario has driven the urge for the 'datafication' of all aspects of social life and experience, and the commodification of data generated as an input for economic production.

Datafication has been accompanied by the emergence of 'platforms' as the dominant technical and economic framework for networked transactions. These platforms, which intermediate much of the internet, are largely operated by private, for-profit and multinational corporations including Google, Facebook, Microsoft, Amazon and Apple, each of which assert increasing dominance over different realms of our digital lives – from search, social networking to traditional 'e-commerce' and operating systems and software. The emergence and transnational dominance of platforms was abetted by prevailing institutional norms that prioritized uninhibited data flows. In the regulatory void of transnational data flows, platforms have become the dominant institutional actors shaping the norms of data col-

2. Julie Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press, 2019.

3. Declaration on Global Electronic Commerce, Second Ministerial Conference of the World Trade Organization, May 1998. https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

4. Arthur J. Cokefield, 'Tax Wars: How to End the Conflict over Taxing Global Digital Commerce', *Berkeley Business Law Journal* 17, 2020.

lection and use in a globalized information economy.

The accumulation of political and economic power by these multinational firms has been likened by Frank Pasquale to a form of 'functional' sovereignty – displacing strictly territorial state-sovereign power and control over the internet and shaping the rules that govern online data flows.[5] The central role of platforms in intermediating data flows and shaping network behaviour has, until recently, gone unnoticed by policymakers around the world, with market regulators and courts unable to comprehend or respond to the transformative role that network intermediation and accumulation of data plays in shaping markets, within legal frameworks like competition law.

Some scholars have suggested that claims of 'information sovereignty' have emerged in response to, and as a counter to, the dominant or hegemonic ideal of 'free flow' of data and information and the 'freedom to connect', driven by states and platforms, and particularly by 'Silicon Valley' and US trade and foreign policy. Certainly, historical evidence of assertions of 'information sovereignty', such as those in China and Russia, support the theory that both foreign and domestic internet and data governance policies in these countries have been driven by considerations of national security and trade protectionism, establishing greater restrictions on trans-border data flow as a means of asserting 'sovereignty' over the internet (or their internet). The emergence of the platform economy and informational capitalism as an economic structure has compounded these anxieties of governments and state agents in their assertion of technological sovereignty and 'data sovereignty' over the internet.[6]

The history of the internet and digital policy and laws in India indicate to some degree the concerns and anxieties about the state's role in the facilitation or governance of network access and data flow. The earliest attempt to regulate the internet, the Information Technology Act of 2000, explicitly addressed the need to facilitate transnational e-commerce through the standardization of legal and technical frameworks for the internet, with reference to the prevailing norms of standardized international e-commerce framed under the UNCITRAL. Subsequently, a series of amendments to the IT Act in 2008 were testament to the increasingly consequential social and political role played by the internet and online information, with the Government of India attempting to regulate online expressions primarily as a reaction to national concerns about unlawful or undesirable online expression.

More recent policy developments, however, are directly responding to the emergence of global informational capitalism and the platform economy. The language of the draft e-commerce policy signaled an emerging and urgent trend towards re-conceptualizing 'data' as a material resource for producing economic value, as well as the necessity of government interventions for ensuring that data flows are in line with state security or economic policy. The Economic Survey of India, 2018-19, dedicated an entire chapter outlining how data must be treated as a public good for social welfare, envisioning government-controlled platforms for processing and utilizing data as raw material for the generation of economic value, a sentiment also echoed in the March 2020 Draft Strategy for National Open Digital Ecosystems released. The Government of India has attempted to create the legal basis for this vision through mandates for data localization (the requirement that data be stored in servers within Indian territory) within various sector-specific regulations (like those of the Reserve Bank of India requiring payments companies to store data locally), as well as in the pending Personal Data Protection Bill. The current version of the PDP Bill also gives the central government a *carte blanche* to acquire any data not categorized as 'personal data', similar to claims of the 'eminent domain' of a nation state over land or natural resources within its territory.

Trade policy has similarly reflected concerns about trade sovereignty and economic self-sufficiency affected by data flows. FDI Press Note 2 of 2018, for instance, created new rules for the operation of 'e-commerce' platforms with primarily foreign investment, as a protectionist measure for domestic retail and e-commerce firms who have been affected by the dominance of platforms like Amazon. Similarly, India, along with other global South countries is attempting to renegotiate the WTO moratorium on customs duties on electronic transmissions. In March 2020, the government introduced an 'equalization levy', or an indirect tax for foreign platforms operating in India in an effort to balance the scales of global e-commerce, after similar attempts since at least 2016, including the use of data localization mandates to create a legal fiction for taxation of international flows of data by Indian tax authorities. The equalization levy has primarily been directed towards dominant platforms

5.Frank Pasquale, 'Digital Capitalism: How to Tame the Digital Juggernauts', *WISO Direct*, 2018. https://library.fes.de/pdf-files/wiso/14444.pdf

6. Michael Jablonski and Shawn M. Powers, *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, 2015.

like Google and Amazon, earning it the moniker of 'Google tax'.

Claims to data sovereignty have not received much judicial interrogation with the legal basis for laying jurisdictional claim or control over information being largely foregrounded in considerations of private international law and judicial comity or reciprocity. However, while no consistent standard for asserting legal jurisdiction appears to have developed in India, Indian courts have not shied from asserting an almost 'universal' jurisdiction over data flows and online transactions occurring or connected with India. In the recent case of *Ramdev v Facebook*, for example, the Delhi High Court asserted the extra-territorial applicability of Indian defamation law stating '*The material/information having originated from India, courts in India would have jurisdiction to direct removal of the same*.'[7]

India has, in the past, strongly pushed for technological sovereignty and the preservation of the government's rights to use technology for securing valuable social and economic goals, for example, in the negotiations for government use of patents and compulsory licensing under the TRIPS.[8] Recent policy and legislative developments appear to have paved the way for the Government of India to lay claim to 'Indian data' and data flows for the purpose of executing a vision for a centrally planned data economy. Undoubtedly, this presents one alternative to the neoliberal economic order produced by the current 'legal-institutional' frameworks governing data flows, which encourage the extractive logic of informational capitalism driven by digital platforms. Criticisms of data sovereignty, which attack the 'balkanization' of the internet, tend to ignore the social and political imbalances produced by these dominant geopolitical orders, as well as the state's obligation and central role in securing economic and social justice.

However, the metaphor of 'data as oil' can only be stretched so far. Likening data to a material resource to be primed for the extraction of economic value ignores the violent politics and history behind competing claims to natural resources like oil which also encompass community rights to land and livelihoods and risks becoming a violent enterprise of its own. The emerging policies of laying absolute claims to data by the government ignores a multiplicity of rights and interests in all forms of data, claimed either by individuals, such as privacy and decisional autonomy; or by communities – including economic rights or group rights against discrimination. Subsuming this multiplicity of claims, rights and interests over data within one notion of state-sovereignty risks undermining such rights in much the same manner as dominant platforms currently do.[9]

The Government of India's policies do not reflect a vision of social and economic justice beyond the claims to control and power over data, limiting the discourse on privacy to a myopic vision of 'data security'. India's current approach towards 'data sovereignty' ignores the multiple possibilities of political organization in data governance. Even accepting the primary organizational role of the state, these policies and laws exhibit tendencies of centralization of power over data and the internet without the democratic involvement of communities in the manner in which data is governed. Alternative imaginaries remain unexplored, including organizing platform cooperatives, or forms of data stewardship organized around local self-governance, such as Barcelona's Decentralised Citizens Owned Data Ecosystem. Similarly, the Government of India has not been proactive in ensuring structural interventions in markets for dismantling the extraordinary market power of big technology firms, for example, through tools offered by the Competition Act.

Among the public responses to the draft e-commerce policy, mostly by lobbying groups and corporate federations, was the submission of the Bengaluru Jilla Beedhi Vyapari Sanghatnegala Okkuta, an association of street vendor unions from Bengaluru.[10] In its submission, the federation echoed concerns about the Government of India asserting sovereignty over data and likening it to mines, arguing that the history of mines was a history of the violent displacement of community rights and self-determination, and asking for the government to evolve a framework which allows communities to both control and benefit from economically valuable data. Taking this sentiment forward, as argued by Yarimar Bonilla, perhaps we must 'unsettle' the framework of 'sovereignty' itself, and examine whether it reproduces the violent and inequitable geopolitical order that the notion of 'data sovereignty' wants to respond to.[11]

7. Delhi High Court, CS (OS) 27/2019.

8. Jayashree Watal, 'Patents: An Indian Perspective', in *The Making of the TRIPS Agreement*. World Trade Organization, 2015.

9. Linnet Taylor, 'What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally', *Big Data & Society*, 2017.

10. Translation of the submissions on draft Ecommerce Policy made by Bengaluru Jilla Beedhi Vyapari Sanghatnegala Okkuta. https://www.medianama.com/wp-content/uploads/english_vendors_ecommerce_suggestions_objections.pdf

11. Yarimar Bonilla, 'Unsettling Sovereignty', *Cultural Anthropology* 32(3), 2017, pp. 330-339.

India and the global governance of cyberspace

Interview with Ambassador **Asoke Mukerji**, former Permanent Representative of India to the United Nations.

At the United Nations and other international organizations, what is your sense of the coverage and importance that emergent technology issues like cyber security, digital rights and data, and the role of ICTs in development received? Was there a tipping point when these debates became salient?

I think that emergent technology issues that you mention, including the role of Information and Communication Technologies (ICTs) in development, have become more prominent in the agenda of the United Nations and its specialized agencies over the past three decades. These issues have been placed on the negotiating agenda of the World Trade Organization (WTO) since 1997 onwards, underlining the desire to provide a legal framework for trade in emergent technology products and services. Obviously, so far, there has been no attempt to converge these activities into a holistic framework, which I feel is necessary to ensure the integrity and resilience of cyberspace activities.

In the UN system, the International Telecommunications Union (ITU) took the lead since 1992 to focus on access to ICTs on an equitable basis. This motivated wider discussions within the UN General Assembly (UNGA) on how to harness the immense potential of emergent technologies for meeting the objective of socio-economic development based on international cooperation described in the UN Charter.

The UNGA adopted its first resolution on ICTs in December 1998. This resolution noted the use of ICTs for both civilian and military purposes. It is worth emphasizing that this UNGA resolution prioritized 'civilian applications'. The three broad areas that governments have taken up since 1998 to develop international cooperation in cyberspace, relate to norms for cyber security, measures to counter cybercrime, and agreeing on cyber policies for accelerating effective governance. One part of the 1998 UNGA resolution mandated the definition of 'basic notions related to information security', while 'developing international principles' to enhance cyber security. This was also prioritized by another UNGA resolution adopted in 2002 on the 'global culture of cyber security.' That is why I believe we have an uneven implementation of the original balance of the 1998 UNGA resolution. Of course, in 2003 and then in 2005, the UN held the World Summit on an Information Society (WSIS), first in Geneva and then in Tunis. This process created the platforms for discussing internet governance issues through an Internet Governance Forum (IGF), including digital rights such as affordable and easy access, upholding fundamental human rights online, etc.

A third impulse in the UN came with the mandate given by the 2012 UN Summit in Rio de Janeiro to negotiate the sustainable development goals (SDGs). By 2014, it was clear that the scope of the SDGs would touch on all aspects of human activity, including on climate change issues, and that ICTs would be an integral means of implementing these SDGs. I think that the tipping point for the United Nations process was the adoption of Agenda 2030 in September 2015 with the 17 SDGs at its core. This event was followed in December 2015 by the UNGA agreeing to converge the WSIS Tunis Agenda with Agenda 2030. All stakeholders in the Agenda 2030 and Tunis Agenda process, i.e. governments, businesses, academia and civil society including youth and women, must take this convergence forward.

In the context of this discussion, I think it is important to focus public attention on another parallel process underway in the WTO that deals with emergent technologies including ICTs in multilateral institutions. Here, emergent technologies like ICTs became a part of the WTO Agreement in 1997, when a set of 'regulatory principles' were agreed to during the Basic Telecoms negotiations. These principles include

the use of 'scarce resources' such as spectrum and laid down clear guidelines on how these are to be allocated, viz. the process should be 'timely, objective, transparent and non-discriminatory.' The Basic Telecoms negotiations ushered in the era of global mobile telephony, as we know it, based on multilateral trade rules. Rapid developments in the technologies behind mobile telephony which created smartphones, and the transition from an ICT-driven world to a digital world, will throw up demands for broadening the way the WTO regulates trade in digital products and services.

This links with the concept of electronic commerce. The WTO became involved in electronic commerce discussions after the publication of an 'Electronic Commerce Strategy' paper by the United States in 1997. Two specific results have been the negotiation of an Information Technology Agreement (ITA) and adoption of an Agreement on Global Electronic Commerce of July 1998.

The ITA committed participating member-states who agreed to a zero-tariff for import of computers and related peripherals. The ITA was considered a catalyst for India's global ambitions in export of software especially with Y2K looming in December 2000. It opened the door for the WTO to look at issues relating to emergent technologies. The WTO has already issued legal rulings on issues relating to cyberspace involving both goods and services. These include rulings on tariffs levied on use of local-area-network (LAN) equipment and multimedia personal computers; alleged market access restrictions on electronic payment services; voice telephony services, among others.

The Agreement on Global Electronic Commerce committed WTO member states not to levy customs duties on electronic communications, which will be reviewed at the 2020 WTO Conference. I believe this will become a tipping point for emergent technology issues in the WTO. Today, there is a growing convergence and interest among major trading nations that the subject must be reviewed, and the WTO must begin negotiations to create a framework for Electronic Commerce. By its very nature, Electronic Commerce will raise the issues related to emergent technologies, and countries should be prepared to engage in this process if they want to be part of, and relevant to, the global digital economy.

Cyberspace debates, especially governance, are often painted as a binary between the US with their NATO/OECD partners, who prefer an open borderless internet, pitted against China and Russia who prefer more control, restraints and order. Is this binary an accurate depiction of global governance debates around cyberspace?

When we look at multilateral debates on the governance of cyberspace, the perception of there being two options based on democratic or authoritarian political systems is often spoken about. However, the nature of control and governance of cyberspace is much more complex. It involves both governments as well as corporations. More than the nature of governments, this debate needs to focus on data flows.

Participants need to speak more of how cyber data flows around the globe including through fibre optic cables and using root-servers. Once you look at this core infrastructural dimension, it becomes clear that both governments and corporations play a major role in regulating cyberspace governance issues. Of course, this activity is being conducted without an agreed multilateral framework, which makes it vulnerable to individual priorities whether of governments or corporations.

Some major corporations active in cyberspace also seek to control the flow and storage of data, or impose restraints on access etc. They use emergent technologies to do so, including Artificial Intelligence, and Cloud Computing. Multinational corporations in cyberspace know that government policies regulating their access to the market of a country can restrict their profits, including from the collection and sale of data. This awareness has not prevented such corporations from cooperating with governments considered authoritarian to ensure revenue streams from their market access. A new dimension to this activity is the emergence of clearer data privacy laws by some major players, such as the European Union, which will impact corporate policies regarding the flow and storage of data.

General discussions on the 'binary' between democracies and authoritarian states miss this dimension altogether. There is another dimension to this issue. Debates on the governance of cyberspace tend to ignore the views of developing countries of the 'Global South', especially those countries which have prioritized the use of cyberspace for realizing their national development objectives.

Stakeholders have discussed cyber governance issues within the Tunis Agenda framework of the United Nations. At the core of the Tunis Agenda is the functioning of the Internet Governance Forum (IGF). The IGF became a platform to enable multi-stakeholder discussions on how society should respond to the potential of cyberspace. The Forum witnessed a spirited debate between advocates of a business driven model,

whose policies would conform to the market-driven priorities set by the growing number of cyber technology corporations (often referred to as the 'multi-stakeholder' model), and votaries of a more assertive role for government policies, i.e. both for law enforcement as well as for empowerment of societies, in order to bridge 'digital divides' (referred to as the 'multilateral' model).

The fact that both approaches were convergent was finally acknowledged when the UNGA conducted its High-Level Review of the implementation of the Tunis Agenda in December 2015. The Review emphasized the importance of the need for effective international cooperation in cyberspace to achieve globally agreed goals of sustainable development. This included using cyber technologies to bridge the digital divide; equitable access to cyberspace; the creation of an enabling cyberspace environment for development; public-private partnerships in financing the growth of cyberspace; the protection of human rights online including the freedom of expression and privacy.

On the management of the internet, the agreed multilateral approach is that its governance is a 'multilateral, transparent, democratic and multi-stakeholder' process with the 'full involvement of governments, the private sector, civil society, international organizations, technical and academic communities and all other relevant stakeholders in accordance with their respective roles and responsibilities.'

The UN has set up the sixth iteration of the Group of Governmental Experts (GGE) through a resolution sponsored by the United States; in addition, there exists a more inclusive Open Ended Working Group (OEWG), a more consultative framework to discuss growing cyber threats. Where do you see these norms formulation processes ending up? Are there key issues both frameworks do not cover?

The focus for developing norms for cyber security through the GGE is to focus on the responsibilities of UN member states to ensure the resilience and integrity of critical national infrastructures used for cyber activities. The discussions in the GGE since its inception in 2004 (following the 2002 UNGA resolution on global cyber security), was to agree on a normative framework, which would be implemented through mutually beneficial international cooperation. However, due to the emerging polarization between the United States and China on these obligations, the GGE norms which were agreed to in 2015 are now back on the drawing board.

In terms of current GGE meetings, new areas include the emergence of new cyber technologies and platforms for the application of technologies such as social media. Obviously, these technological developments may require the GGE to review the relevance of some of the norms it recommended in 2015. Apart from its core mandate for recommending norms for cyber security, the GGE discussions encouraged the identification of voluntary confidence-building measures and capacity building to enhance cyber security. The outcome of this GGE is to be reported to the UNGA in 2021 underscoring the increasing urgency being felt by governments for effective international cooperation in securing cyberspace.

In response to growing criticism that a majority of UN member states and other stakeholders in cyberspace were being excluded from contributing their perspectives to a global dialogue on cyber security, the UNGA also adopted a resolution in December 2018 establishing an Open-Ended Working Group (OEWG) to make the discussions 'more democratic, inclusive and transparent.' The OEWG established by the UNGA has met from June 2019 onwards. The OEWG is scheduled to hold its final substantive session on 6-10 July 2020 in New York.

Besides governments, the OEWG discussions on cyber security have brought in businesses, non-governmental organizations and academia. The multi-stakeholder discussions held so far have revealed important gaps in securing cyberspace on the ground. These include 'lack of data sharing and informed awareness of cyber threats', as well as 'lack of will at the highest political levels.' The discussions have noted that the GGE process had not fully considered the impact of new technological developments in cyberspace, which significantly enhanced cyber threats. Advocating a 'holistic' approach to enhance cyber security, participants have drawn attention to the linkages between economic and cyber security. Most significantly, discussions on cyber security have emphasized 'a human-centric, rights-based approach that also emphasizes shared responsibility and accountability.'

This is the broader context for the popular debates over new ICT technology like 5G, issues of ethics in applying Artificial Intelligence for cyber activities, and assertions of sovereignty over the flow of data derived from traditional national jurisdictions ('data localization'). It is important to recognize the explicit incorporation by the UNGA of a 'multi-stakeholder' approach. As highlighted by the Chair of the OEWG to member states, such a multi-stakeholder approach can poten-

tially integrate such issues into ongoing UNGA discussions on international cooperation in cyberspace.

Of course, both the 6th GGE and the OEWG are restricted by their mandate, which is given by the First Committee of the UNGA. The charter of the First Committee is 'disarmament, global challenges and threats to peace that affect the international community' and 'solutions to the challenges in the international security regime.' In that sense, the broader application of emergent technologies on issues of fundamental human rights and sustainable development are not addressed by either of these two processes. Nor are the outcomes of the GGE or OEWG expected to lead to any comprehensive framework under the UN for regulating cyberspace.

It is in this context that the UNGA resolution of December 2019 launching a process for negotiating a legal framework to counter cybercrime is significant. It is the first step within the UN system for a legal framework on one aspect of cyberspace activities. However, it must also be recognized that this initiative, laudable as it is, will not address the vulnerabilities of cyberspace in a holistic manner. At some point, the UNGA must bring in the possibility of using discussions on a cybercrime legal framework to broaden the mandate to negotiate a comprehensive convention on cyberspace.

India is yet to advocate a clear position on these technology issues except being stridently against 'data colonialism' and unrestricted data flows across borders. A 2018 report by the New America Foundation has regarded India as a 'digital decider' in global governance and India's stance is therefore critical in navigating the ostensible binary between democracy and 'digital authoritarianism'. Can India carve a leadership role for itself on cyber governance and how?

In my view, looking at global cyber governance in terms of a binary (either democracy or authoritarianism) is not sustainable on the ground. In the case of India assuming a leadership role in the global cyber governance framework, it is necessary to look at the factors that favour such a role for India.

One is India's self-interest in upholding effective international cooperation for the continued growth of her exports of information-technology enabled services. The current instability in the world due to Covid-19 has perhaps created an opportunity for India to increase her share of the global market for such services. India's revenues from the information-technology enabled services sector in 2017 were estimated at more than $140 billion annually, of which export earnings are close to $120 billion.

Second, India has prioritized the associated movement of skilled Indian manpower to cyber markets abroad, who contribute to developing cutting edge technology in cyberspace through research and innovation in major transnational businesses. Remittances from this highly paid group are an integral part of the annual inflow of almost $80 billion in remittances to households in India in 2018. India is uniquely placed to be an advocate for issues relevant to this rich pool of global human talent in cyberspace governance.

Third, India has a huge volume of data derived from her prioritization of using ICTs for accelerated socio-economic development. India's Digital India platform, with its twin impacts on bridging digital divides and empowering citizens, has been multiplied significantly with the increased use of Aadhaar, which is the world's largest national biometric database. This makes India a sought-after market for foreign partners, who want to use this pool of data for traditional and digital market activities. India can influence the way in which global digital trade rules are written based on the size of her digital data resources.

Such a leadership role can come if India joins in the formulation of global policies and rules on the digital economy. One such platform, which already exists, is the impending WTO negotiations on electronic commerce. India can join hands with her strategic allies among her major trading partners, like the United States, the European Union and Japan, to influence a rules-based framework on global e-commerce. It may be of interest to recall that when the WTO was being created, India did play such a leadership role in the negotiations on the General Agreement on Trade in Services (GATS) along with the United States and European Commission.

As a major repository of the global pool of digital data, India can take the lead in some areas. One such area is in proposing the creation of a Harmonized System of Nomenclature for Digital Data, which would encompass both digital products and services. The importance of the use of the existing Harmonized System for goods has been amply demonstrated, whether for reducing costs to international trade, internal taxes, trade policies, monitoring functions, dispute settlement, economic research and analysis etc. As the world moves into a digital economy, it is necessary for countries active in this new economy to encourage the creation of such a Harmonized System of Nomenclature, which will act as an incentive for all stakeholders.

Will non-state actors (private sector and civil society) become more influential in shaping multilateral and domestic debates on internet governance? How do you see this trend affecting technology policy-making in India given the range of institutions involved in regulating technology matters?

The experience so far on cyberspace discussions in India and abroad illustrates that it is necessary to involve a range of stakeholders. Of course, the government is at the heart of this activity, but significantly governments have themselves acknowledged the role and influence of other stakeholders in contributing to cyberspace activities.

At the national level, the most recent example of the importance and relevance of multi-stakeholder participation was during the consultations for the Justice Srikrishna Committee on the Data Protection Bill in 2018.

At the global level, apart from our multi-stakeholder participation in the meetings of the Internet Governance Forum, we need to build on our contributions to the Global Conferences on Cyber Space. This is important because the importance of effective international cooperation has been raised by the five multi-stakeholder Global Conferences on Cyber Space held so far, beginning with the London Conference in 2011 and ending with the New Delhi Conference in 2017.

Five broad themes for international cooperation in cyberspace have been identified by these multi-stakeholder Conferences. These are economic growth and development, social benefits, international security, tackling cybercrime and ensuring safe and reliable access to cyberspace. In addition, the importance of capacity building in cyberspace, the linkage between internet security and internet rights, as well as the role of civil society in cyberspace policies, and universal access to cyberspace to accelerate development have been prioritized.

It is worth recalling how India converged her national priorities in cyberspace governance with her role as host of the 2017 New Delhi Conference. In her vision statement, India emphasized that the goal of this multi-stakeholder meeting was to 'promote the importance of inclusiveness and human rights in global cyber policy, to defend the status quo of an open, interoperable and unregimented cyberspace, to create political commitment for capacity building initiatives to address the digital divide and assist countries, and to develop security solutions in a balanced fashion that duly acknowledge the importance of the private sector and technical community.' This needs to be followed up by us to institutionalize multi-stakeholder participation.

Books

MIDNIGHT'S MACHINES: A Political History of Technology in India by Arun Mohan Sukumar. Penguin Viking, Delhi, 2019.

Arun Mohan Sukumar's book, *Midnight's Machines: A Political History of Technology in India* documents the fraught relationship between successive Indian governments with technology – or, to put it more specifically, with the problems of crafting policies that can provide widespread access to technological advancement in India. While governing a nation whose foremost characteristic is an enormous population, whose livelihoods, social outlook and community structure perceive technological solutions to be threatening, successive governments have awkwardly attempted half solutions that occasionally manage, but also sustain the problem.

In many ways, the central puzzle of Sukumar's book is interesting in itself: technology, the argument goes, is a critical ingredient in finally freeing the individual from the shackles of community and caste. After all, the great debates about the transition from feudalism to capitalism – and thus a shift from lives lived according to birth based identities, to modern individualistic living, all acknowledge that the advent of technological advancement decisively shifted the balance in favour of a more progressive society. Theoretically, then, technology should provide a further means of transcending that central question that dominates so much of India's social realities: birth.

But the answers to this question – as any Indian social scientist will know – are tricky, and the fate of technological access, in many ways, share the same problems. The concern was that too much freedom in enabling access to technology might divest India of its identity and turn it into one more cog in a fast food machine. Sukumar's first chapter deals with the complexities of Nehru's tussle with this question. While on the one hand, being famous for declaring the Bhakra Nangal Dam as being a 'temple for modern India', Sukumar argues that Nehru took a cautious view of the potential of technology, arguing that the medium of technology per se was unimportant, as compared to the ways in which technology could be harnessed to develop a better sense of societal conscience. Convinced, Sukumar writes 'that Indians, if exposed overnight to the awesome power of technology, would become beholden to it'; Nehru followed domestic policies which would try to prevent this outcome.

The state's insistence on carefully regulating the access to technology to its citizens, and its monopolization over its production – as well as consumption – meant that access to this medium by the citizen was heavily restricted. Yet, this insistence produced curious contradictions. Because of the Nehruvian state's uneasiness with technology there was a curious gap in the kinds of development in science in India. A genuinely mass based technology, such as access to the television or radio was markedly delayed in India and

resulted in its citizens lagging behind in their ability to transcend the challenges of underdevelopment. Yet, in other spheres – such as research on space, atomic energy – to use Jahnavi Phalkey's phrase, 'Big Technology', India in fact displayed considerable achievements. The problem with this, though, was that there was never any societal support from the rest of the food chain – and these devices never truly touched the average citizen. A striking demonstration of this is the fact that IIT alumni were unable to find employment within the country and, almost to a man, had to look outside the country for their job prospects.

In fact, these contradictions also hampered the working of the Community Development Scheme created by Nehru, which 'was trying to create an uneasy equilibrium between increased productivity in villages and small-scale industries, ensuring its users understood the tools given to them, and limiting the use of unnecessary machines altogether.' But, in many ways this was an artificial distinction, and the scheme, unable to overcome the artificial impositions imposed by the state based on political and social considerations, largely ended in failure, resulting, Sukumar notes, in 'A great psychological and material distance arose between the citizen and the machine.'

This uneasy coexistence between two opposing requirements continued to manifest itself during the Indira Gandhi years. Dealt a rude shock by the military defeat to China in 1962, it became clear, the Bhabha committee report pointed out, there remained urgent repairs in the transport, defence and communications sectors. Yet, 'even where circumstances required the intervention of the state to bring new technologies closer to the people, the Indian government proceeded in the opposite direction.' For one thing, the specter of job losses due to technology raised its head in political rhetoric, and Indira Gandhi chose to come out as an advocate of this argument to secure her own electoral interests. One idea which seemed to provide a convenient route out of this conundrum was the concept of 'appropriate technology'. For instance, a young Amartya Sen suggested, a distinction could be made between adopting 'landesque' and 'labouresque' technologies – for India, landesque technology would be more appropriate than labouresque, which would deprive agricultural workers of their living.

On the whole, though, Sukumar shows, the Green Revolution occurred in spite of, rather than because of, Indira Gandhi's attitudes to technology. Although regarded as a great success story today, the idea of introducing more mechanization and seeding technology to agriculture produced a great deal of resistance. The arguments against introducing tractors and combine harvesters, moreover, were more or less in sync with Indira Gandhi's concerns: it would gobble up the wages of the labourers, increase disparity between rich and poor landowners in addition to upsetting the ecological system. The reason that it was set into motion, Sukumar notes, was a combination of factors that threatened Indira Gandhi's premiership: the devaluation of the rupee, two successive years of drought, and a poor electoral performance.

The introduction of computers into India was also subject to the same vexed tussle. Rajiv Gandhi's tenure saw a proliferation of the use of Information Technology in the government. An early form of this was the building of the platform 'CRISP' (Computerized Rural Information Systems Project) introduced under the supervision of a civil servant who spotted the potential of building a computerized data set for the work of the District Rural Development Agency. This later developed into the NICNET project, designed to enable a national network of micro computers for digitizing and sharing data amongst public institutions. Its implementation, however, was impeded by the unwillingness of state governments to share information with the Centre. Its creation, moreover, Sukumar notes, required the breaking of over 300 regulations before it could be launched. Local administrations being unable or unwilling to learn how to enter data, turf wars within government departments, and hostility from bureaucrats who saw the project as a threat to their fiefdoms, ensured the project's failure. Indeed, Sukumar notes, the eventual flowering of the Information Technology sector in India was 'hardly the culmination of some aggressive effort by the state to bring computing to the masses. It occurred overnight, and almost entirely by accident.'

Sukumar's last chapter, and amongst the most interesting, details the story of India's technocrats, Mokshagundam Visvesvaraya, Vikram Sarabhai and Nandan Nilekani. In many ways, the diverse history of these men was unified by a single theme: an attempt to develop a systematized and uniform method that could collectively uplift the standard of living, while being bogged down by the complexities and variedness of the reality of the lived experience in India. While developing the platform for Aadhaar to be expanded in government, Nandan Nilekani found that the technology could be deployed in a variety of ways that may not necessarily ring true with its original ideals, but do align with the direction of politics, government and the state in India. Thus the Aadhaar debate has 'suffered from ram-

pant politicization and bureaucratic meddling, not just from Delhi, but also from the states.'

Indeed, Sukumar argues that the concept of technology itself is politically fraught: 'If, for decades the Congress has been inclined to see Technology as the Great Corrupter, it is, to the BJP, the Great Disruptor.' Modi himself is far less squeamish about being seen to be technologically advanced than his predecessors and also has been able to 'marshal Hindu pride through technological platforms in a way that the RSS itself, with its emphasis on 'swadeshi' values, is ambivalent about.

Sukumar's book is a rich *tour de force* of the history of the Indian state's relationship with technology, as well as the accompanying social and political issues around it. It will definitely serve to enliven the debates about progress, advancement and development around India's 'rise'. Yet, the question remains: some three decades after the liberalization of the economy, the interface between technology and the average Indian citizen remains relatively limited.

A startling statistic that emerged during the tussle over 'net neutrality' between Facebook and India's telecom regulator was that less than 30% of Indians had access to social media – and possibly the internet. The direction of the government's policy with regard to technology – discouraging or otherwise – may not be the only reason that this is true. Partly, the lack of development of technological solutions may well be a product of various governments' specific policies that could and should be changed, but may also be indicative of a structural feature of the Indian landscape: the entrenched, and unchanging fact of its poverty.

Pallavi Raghavan
Assistant Professor of International Relations,
Ashoka University, Sonipat

THE NETWORKED PUBLIC: How Social Media is Changing Democracy by Amber Sinha. Rupa Publications, Delhi, 2019.

OUR typical conceptualization of democratic overthrowing carries drama: a military coup, one swoop of an executive usurping, or a flagrant abuse of voting fraud. With our guard against these spectacles, we perhaps did not realize the vulnerabilities of long-standing constitutional norms until these structures began to slowly decay. Although it is true that India has always felt the fragility of its deliberative democracy, new eras bring in new facets of concern. The current moment of 'democratic backsliding' – 'the gradual dismantling of institutions and mechanisms that check and balance the powers of the executive in liberal democratic constitutional frameworks' – both gives life to and is given life by a new digital medium overlaying the sovereign public as researcher Amber Sinha describes in his book *The Networked Public*.

'The move from full-blooded coups to democratic backsliding means that democracies erode gradually rather than implode rapidly', Sinha argues. 'If we have to have any chance of arresting this slide, it is important to recognize that current trends are not random events but natural responses to local and international incentives.'

These incentives, he finds, are mismanaged by corporate and state powers equally, culminating in the technological dimension of today's democratic backsliding. Sinha manages to piece together seemingly disparate topics to examine this backsliding's undercurrents, albeit with some amount of meandering away from his original thesis. For readers unaware of the major technology threads of the day in India, the book presents a useful recap.

On the private player front, the platforms have created not 'a marketplace for ideas' but 'an information architecture... designed to show information which an individual may find most engaging, to serve the advertiser interest.' Sinha snakes through corporate issues of social media misinformation, short-term thinking algorithms, the targeted ad economy, the illusion of authoritative content on WhatsApp's closed networks, and the half-hearted, ineffective attempts at fact-checking. 'Although they are run by private corporations, these platforms have become public squares for discourse without any public accountability, and have consequently blurred the lines between public and private', he notes.

On the public front, Sinha integrates political micro-targeting, government data collection, polarizing electoral speech, and the necessary ingredients of platform liability to showcase that the government is no benign bystander. In fact, the authoritarian state can reap more benefit from a networked media than meets the eye.

Ultimately, the book's stroll through the newsworthy technological topics of the past few years ends at his acceptance of some amount of government regulation of technocrats, but he ruminates for something much larger. Sinha relies heavily on the foundational work of John Dewey, who spelt out a logical belief in the possibility of a deliberative society. To reach such a state, in the technological age, Sinha

champions structural reforms to fix democracy and capitalism.

Deriding the Chicago School of weak competition laws as focused only on consumer harm, Sinha argues that the monopolistic nature of technology behemoths need to be reigned in by a new age of global antitrust reform. In addition, campaign finance reforms can put an equal amount of accountability on state accumulation of power. Sinha is not the first to call for these structural reforms, nor will he be the last. More interestingly, he places them at the forefront of a technology discussion, linking the symptoms to the true underlying causes.

A fundamentally more competitive market and competitive democracy will lead to a Dewey's imagined public, wherein individual choice of information will inevitably lead to a cooperative, informed public: a sum of its parts that overshadows its bad apples. 'Perhaps Dewey's ideal of the public's social existence, and the ability to form associations, is where we need to look. The way a democracy can work is if the public can organize itself in a way that it can use the information that it drew from its social environment to inform its collective action. This would require a competitive market where the public can choose its sources of information and recognize privately owned platforms as public forums and have meaningful mechanisms to engage and associate with', he writes.

Right now, the pie remains mostly bad apples because of the growing authoritarian powers that be, in Sinha's eyes. Information arenas of passive thinking, echo chambers, political micro-targeting, polarizing speech, and the like overwhelm the market. They have become the features caused by and causing the democratic backsliding of the recent moment.

While Sinha's ability to understand the citizen's precarious positioning between corporate and state influence allows for an even-handed prescription, if a reader fundamentally disagrees with Dewey's optimism and freedom in choice, they might find the remedy shallow even if the diagnosis is clear. Sinha does dissect the beliefs of Dewey's foil, Walter Lippman, who saw an informed citizenry as an unattainable goal. But this Dewey-Lippman dichotomy does little to illuminate the realistic manipulations that even an open marketplace of information platforms would still grapple with. If any platform were built with the most addictive features of a casino, would the citizen's choice in platforms be any different? Would enough people choose platforms that prioritize the aspects of deliberative democracy that Sinha illuminates? Does one as a reader have similar faith and trust in an individual's desire and strength for an informative public?

The merits of such a campaign remain debatable. Nonetheless, Sinha reminds us, it is a goal worth fighting for, attainable or not.

Karishma Mehrotra
Journalist, 'The Indian Express'

PRIVACY 3.0: Unlocking Our Data-Driven Future
by Rahul Matthan. HarperCollins, Delhi, 2018.

INDIA'S large state apparatus has always been Janus-faced: holding out the promise of greater public good often at profound human cost. Our newer digital infrastructures repeat this motif: harnessing our data to deliver services, but raising the price that we pay – the cost of our privacy. How might the law help navigate this tension?

In this context, Rahul Matthan's provocatively titled book, *Privacy 3.0: Unlocking Our Data-Driven Future*, sets out on an ambitious project: to trace the evolution of privacy in society, connect it to recent Indian developments and provide an alternative framework for privacy regulation. Ultimately, the central thesis of his book is that a certain inevitable pattern emerges in the way that society reacts to new technologies: first rejecting them because of privacy concerns, but eventually accepting them to harness their benefits.

This optimistic belief in the synthesis that technology can create for society from the dialectic between surveillance and privacy, is in many ways aligned with Matthan's long career as a prominent technology lawyer in India. He co-founded Trilegal (a leading Indian law firm) in 2000, and headed their technology, media and telecommunications practice until March 2020. He advised technology firms throughout his career while also keeping up a healthy engagement with policymaking on various aspects of technology. This book is therefore deeply personal: part memoir, part policy proposal and partly an assertion of Matthan's views on privacy given his experience. It is written engagingly with a pacey narrative style that can reach a cross section of non-specialist readers.

Privacy 3.0 is structured in three parts – 'Privacy 1.0' paints the evolution of privacy in broad strokes from the times of early humans to the 20th century; 'Privacy 2.0' begins the more serious intellectual engagement with the reader taking us through the expansion of the legal right to privacy with a particular focus on India. Here, Matthan deftly weaves his own role into the narrative, charting the behind-the-scenes race to create a

privacy legislation for India between 2010 and 2014; 'Privacy 3.0' sets out Matthan's proposals for an alternative framework for data protection regulation.

If Matthan's own story is mingled with the narrative arc of this book, the other protagonist pervading its pages is the Aadhaar project. Many of the motivations for writing this book are drawn from the Aadhaar architecture which forced India to confront the question of whether privacy is a fundamental right guaranteed by our Constitution. The book's prologue frames its relevance powerfully against the Aadhaar debate, but this framing remains unfulfilled: the book does not directly lay out a stance on the Aadhaar project's privacy features.

No doubt this was because the Supreme Court's judgment on the constitutionality of Aadhaar had not been delivered when the book was released in July 2018. Matthan's view will need to be complemented by other parallel stories of bureaucrats, technologists and activists that are beginning to emerge, such as Reetika Khera's edited volume, *Dissent on Aadhaar* and N.S. Ramnath and Charles Assisi's *The Aadhaar Effect*. The result in this book however, is that the long, unresolved shadow of Aadhaar extends across the book after its bombastic prologue, leaving the reader yearning for more: an unexpected homage to our ephemeral privacy rights.

The strongest parts of this book are those that draw out the legal history of privacy, as the transition from Matthan's construct of 'Privacy 1.0' to 'Privacy 2.0' takes place. Before this, despite the striking imagery (most notably of a pair of zebras in the Masai Mara), the early chapters exhibit an unnerving oversimplification of the development of pre-modern societies and privacy. Privacy is cast as non-existent in hunter-gatherer societies based on generalizations about the human development of certain tribes and broad assertions about social development in all early societies. For instance, the book asserts that the concept of a 'self' did not exist in early societies and it was created (along with the need for privacy) by the invention of walls.

Can such generalizations be made across all pre-modern societies? Are they rooted in political theory, history, philosophy, psychology or all of these disciplines? This heavy-handed approach is discarded as the book proceeds into the more modern history of privacy in 17th-20th century Britain and the United States. This story is recounted through the personal lives of key figures in the evolution of privacy law including Queen Victoria and Prince Albert in Britain, and Samuel Warren and Louis Brandeis who co-authored one of the most influential legal articles in privacy jurisprudence in 1890 – 'The Right to Privacy' – in the US to highlight the human sides of many legal milestones. For instance, Matthan draws on a little-known fact that Samuel Warren had a sibling who was homosexual. This was particularly sensitive in 19th century America which was openly hostile to homosexuality, throwing new light on Warren's motivations for writing this article.

The most compelling part of the book relates to constitutional choices relating to privacy rights made by members of the Constituent Assembly of India in the 1940s. The impact of these choices are traced through the ages until, six decades later in 2017, a 9-judge bench of the Supreme Court pronounced that privacy is a right guaranteed by the Indian Constitution. Matthan's research into the role of various members of the Constituent Assembly, B.N. Rau in particular, are a delight to read. They reveal eerily familiar trade-offs that policymakers continue to confront when considering how (and how *much*) to protect individuals' privacy against state imperatives, including the trump card of national security.

Finally, Matthan sets out his Accountability Model for data protection regulation. He seeks to move to a more permissive approach for firms using personal information, focusing on 'remediation rather than on punishment.' This view can seem disconnected or overindulgent given the growing global recognition of the enormous scale on which technology failures can harm individuals as well as political, social and welfare systems. By placing the onus on a class of 'data auditor' intermediaries to keep firms honest, Matthan proposes abandoning the existing, ineffective approach of user consent-led regimes. The focus on accountability of providers is welcome, although the framing belies the author's forgiveness of data-driven systems making 'small algorithmic mistakes' that create 'inadvertent errors.'

Optimism and advocacy for technology-friendly regulation emerges as a clear theme from the book; although privacy is cast in the title role, it appears that technology is the real star. Some concerns would arise for privacy advocates in the 'technology versus privacy' framing; indeed, many (including this reviewer) see privacy as an enduring value like others in society such as fairness, accountability and security which technology can be built to accommodate to varying degrees, rather than as a zero-sum game.

Overall, Matthan has written an edifying, readable book which blazes a trail for more accessible books on Indian law to follow. Popular science, popular eco-

nomics and even popular history have created pathways into disciplines that are often inaccessible. With Privacy 3.0, Matthan strikes out to create a niche for 'popular law' writing in India – on a topic as complex as privacy – which will continue to raise byzantine conundrums for regulation in the years ahead. That is no mean feat.

Malavika Raghavan
Dvara Research, Mumbai

DOES INDIA NEGOTIATE? by Karthik Nachiappan. Oxford University Press, Delhi, 2019.

FOR years we have been battling to understand how Indian officials negotiate abroad. So far, there has been little more than inferential and anecdotal analysis. There have been suggestions that Indian negotiators reflect cultural and religious traits, based on the Hindu caste hierarchy or the strategic principles of the *Arthashastra*. Others have pointed at ideological drivers, based on India's post-colonial, anti-imperialist and non-aligned rhetoric. In Stephen Cohen's seminal book, India is described as a perpetual naysayer, a country that 'can't say yes.' Many retired officials in the West, in turn, have described India's negotiation style as obstinate, defensive or even obstructionist.

But the proof is in the pudding – and in scholarship that means evidence. Karthik Nachiappan's book is a formidable feast of empirics based on four in-depth case studies. He helps us understand the 'logic' of India's multilateral behaviour, which he describes as 'sober, rational, driven by interests and institutional capacity' (p. 10, 191). India may not be a proactive rule *maker*, but it is also not a passive rule *taker*. Indeed, in some cases it has been a rule *breaker*, but in most instances, the book argues, India's dynamic negotiation style presents the country as a rule *shaper*.

He forwards that Indian officials negotiate based on flexible interests that adapt, varying institutional capacity, and different degrees of influence from domestic interest groups. His four case studies are short but specific and deeply researched, based on multilateral archives, interviews and other primary sources, reflecting the value of historical and case study methodology to understand the many undiscovered logics of Indian foreign policy.

On the WHO's Framework Convention on Tobacco Control (FCTC, 2003), he defines India's negotiation approach as 'pointed and pragmatic' based on a 'fortuitous partnership' (p. 37) between the government and domestic lobbies, leading to simultaneous changes in domestic tobacco control legislation (COTPA). On the UN's Framework Convention on Climate Change (FCCC, 1992), he describes the political rationale of India's 'defensive strategy' (p. 54), which helped to reframe negotiations to focus on equity and financial assistance for developing countries.

On the Comprehensive Nuclear Test Ban Treaty (CTBT, 1996), India 'strove to negotiate a tough CTBT that placed symmetric expectations on all [Conference on Disarmament] member states' (p. 99), and its position only hardened *after* the indefinite extension of the Non-Proliferation Treaty. Finally, on the World Trade Organization's Uruguay Round (1993), India's negotiation was 'tough but pragmatic and rational' based on a 'practical, yet sober, approach' (p. 143).

Overall, Nachiappan's superb book throws light on four different dimensions in India's negotiation processes that deserve further research. First, coordination issues: the case studies show how the interests and organizational cultures of different ministries have at times either aligned or clashed. For example, on the FCC, the ministries of External Affairs (MEA) and Environment and Forests had different mandates abroad, which were eventually harmonized. As international negotiations become increasingly complex, for example on data governance, artificial intelligence or the outer space, it is unlikely that we will see the MEA remaining in the lead as it used to.

Second, the role of external expertise in shaping the government's interests: on the FCTC, for example, evidence based research from civil society experts helped negotiators internalize that the tobacco industry benefits were outweighed by long-term health costs of tobacco consumption. Similarly, in the case of the FCC, think tanks like TERI and the Centre for Science and Environment played a determinant role in shifting India's initial 'defensive position' to a more informed focus on 'differentiated responsibilities'. On trade, the book illustrates the influential role of the Federation of Indian Chambers of Commerce and Industry (FICCI) or the National Association of Software and Services Companies (NASSCOM) and other organizations as sources of technical expertise, rather than just political lobbying. With the Indian Foreign Service and the overall bureaucracy more constrained than ever, a variety of domain specialists will have to step in to help bridge new knowledge gaps and support India's negotiation stance.

Third, the case studies also show the crucial role of political leadership of Prime Ministers, whether Vajpayee's personal interest in regulating tobacco use or Narasimha Rao's determination to join the Agree-

ment on Trade-Related Aspects of Intellectual Property Rights (TRIPS) despite fierce domestic opposition. Eventually, the buck stops with leaders, and to assess the salience of public opinion it would help to focus on a few case studies under weak coalition governments. Do governments cave in to political pressures to ensure re-election, or do they sometimes also use these domestic forces as an excuse to increase their diplomatic bargaining power?

Fourth, how much of a proactive role should India take in negotiation processes? For all the talk about India as a 'leading power', Nachiappan's book shows us that multilateral negotiations are complex and costly, consuming vast diplomatic resources and often stretching on for years. He argues that India may, therefore, not want to bite off more than its negotiators can chew. On the other hand, many regional neighbours and other developing countries also expect India to represent their interests, more than ever: in the case of the FCTC, for example, WHO/SEARO countries delegated negotiation responsibilities to India because it was 'relatively more knowledgeable on tobacco control' (p. 33). Will India be able to balance its restrained approach, limited capabilities and rising demands to shape global governance?

Nachiappan's book not only offers extraordinary insights into four multilateral negotiation processes, but more broadly also offers an excellent contribution to understand how Indian officials seek to maximize their country's international influence. However, beyond skill and expertise, India's negotiation capacity will hinge on its crude capabilities at home, whether economic, military or scientific. Both in the CTBT and WTO negotiations, Nachiappan mentions that Indian officials at times 'implored' their counterparts to accommodate India's interests (p. 122, 160): a more prosperous and powerful India will hopefully equip its negotiators to henceforth be in a better position at the diplomatic high table.

Constantino Xavier
Fellow, Foreign Policy and Security Studies,
Brookings India

THE NEW WORLD DISORDER AND THE INDIAN IMPERATIVE by Shashi Tharoor and Samir Saran. Aleph Book Company, Delhi, 2020.

THE book, while analysing the new world disorder, discusses some of the most significant developments of global significance in the post-Cold War world prior to the Covid-19 pandemic. By engaging readers in several macro concerns, the study interweaves innumerable issues and events around the themes, including the decline of the rules-based international liberal order promoted by the USA, challenges to peace building and sustainable development, problems associated with regulating cyberspace, normative foundations of a new world order and the Indian imperative.

The authors, with their diverse experience in policy-oriented work, have presented an eminently readable discourse on the central theme by marshalling abundant wealth of empirical and statistical evidence to sustain most of their arguments. Two recurring arguments, however, that virtually bind this entire effort together could be placed thus. First, there are diverse, continuing and growing tensions between the forces of globalization, on one hand, and those of national sovereignty, on the other. In fact, whenever the forces unleashed by globalization are incompatible with the national interest of powerful states, the latter deploy national sovereignty to combat them. Second, asymmetrical power relations between the developed and developing countries that characterize the disorder need to be placed in a historical context of the colonial past of the latter countries. Evidently, the normative foundations of a new world order can be built with concrete economic assistance of developed countries to developing countries. Keeping this in view, let me proceed to take a quick overview of this travail.

The term 'global governance' is often used to describe processes and institutions by which the world is governed. In contemporary times, it has witnessed a plethora of discontents. For instance, developments like 9/11 and the financial crises of 2008 had global ramifications in terms of dealing with transnational terrorist outfits such as Al Qaeda and handling recessions the world over. Similarly, the major powers, in their own ways, have contributed to the discontent. The USA's military interventions in Iraq in 1991 and 2003 as the United Nations (UN) almost became complicit in war crimes; Russia's annexation of Crimea and exercise of the veto in favour of an aggressive Syria, and China's refusal to designate Masood Azhar as a wanted terrorist are cases in point.

Besides sovereign states, regulating non-state actors like the multinational companies (MNCs) too have added to the problems of governance. Ironically, the MNCs by 2019 had $40 trillion in revenues and $186 trillion in global assets. Further, Wal-Mart had emerged as the 24th largest in terms of GDP, and 75% of the Fortune Global 500 MNCs belonged to G7 countries. Moreover, the rapid spread of deadly diseases such as SARS and HIV have allowed the MNCs to monopolize

intellectual property rights over the corresponding drugs used for their treatment. In a word, the post-Cold War order built on democracy and free markets has been facing a queer intersection of problems stemming from internet and AI related technologies, politics of identity and growing inequalities between and within the states.

The challenges to the US-led order have also been accompanied by a gradual shift in power centres from the West to the East with the spectacular rise of China as an economic powerhouse. Apart from making a reference to new groupings like G20, Asian Infrastructure Investment Bank (AIIB), Shanghai Cooperation Organization (SCO) and the Brazil Russia India China and South Africa (BRICS), the authors draw attention to the lack of adequate representation of the emerging countries within institutions like the UN and the International Monetary Fund (IMF). In fact, in order to gain greater legitimacy most of the institutions related to global governance require drastic restructuring.

As far as maintenance of peace is concerned, the USA strove to restore peace and order in Somalia, Iraq and Syria. Under Responsibility to Protect (R2P) the USA and its allies intervened in the domestic affairs of developing countries to restore peace in Afghanistan and Libya although the UNSC resolution on Libya failed to get the endorsement of BRICS countries. Further, the Human Rights Council Resolution of 2018 was downplayed by China, so far as individual rights are concerned, by emphasizing the role of the state in socio-economic development. This stance covered up for China's repression of human rights in Tibet and Xinjiang. In essence, while implementing projects of peace, powerful states are difficult to discipline. Strangely, personnel from Afro-Asian and Latin American countries contribute 90% to the UN peacekeeping force.

Furthermore, unfettered industrialization, unsustainable consumption patterns, rising temperatures and emission of greenhouse gases only underscore the urgent need to resolve climate related problems while managing sustainable development. The authors delve into history, and place developed industrial states and their asymmetrical ties with post-colonial states in the context of imperialism. Despite the adverse role played by the MNCs, especially oil companies and the commercial banking industry, in plundering the resources through a form of ecological imperialism, the developed world seems disinclined to part with even a slightly greater share of their GNP through aid to boost prospects of environmental development. The so-called principle of common but differentiated responsibility continues to be hotly contested owing to the unwillingness of the developed world to take on the problems of the planet. On the contrary, instead of legally shouldering responsibilities to clean the planet, the developed world was keen on forcing reforms on developing countries by adding to their burdens in the failed Copenhagen Earth Summit of 2009.

By grappling with the emergence and possibilities in regulating cyberspace, the authors vividly portray an ongoing clash between the natural drive of the Internet to capture global space in a libertarian order and protectionist impulses of state directed capitalist economies like China to bring the activities of the Internet within the jurisdiction of a sovereign state. The analyses cover a gamut of issues related to wars in cyberspace such as the Arab Spring and l'affaire Snowden that affected social movements and influenced the functioning of governments. It refers to the functioning of several search engines and explicates how 'data is the new oil' and can be used after refinement. The discussion on ongoing Sino-US struggles for cyber hegemony and possibilities of digital authoritarianism also find a place. The book concludes by situating India in this disorder. It takes an optimistic view of India and its steady rise by discussing India's role as a torchbearer of the liberal order, a balancer and a development power.

In the end, let me make two critical points. First, since the dependency theories began to enjoy a sway over social science literature in the 1970s, it became an accepted norm and practice to trace the origins of the development of underdevelopment to unequal relationships between the developed and developing countries. However, how long can one keep on blaming external powers and forces for the lack of development in post-colonial states? The question as to why people in most of the post-colonial states did not succeed in building robust institutions by organizing their states and societies in a manner that synthesize social cohesion and overall development still begs an answer. Of course, one needs to take a differentiated view of developments in the heterogeneous range of countries that constitute the global South. Second, a substantial proportion of the last chapter dealing with the Indian imperative is repetitive. Brevity could have driven the central arguments more sharply. On the whole, the text is remarkable and a must read for scholars in policy studies and students of global politics.

Rajen Harshé
Founder and former Vice Chancellor,
Central University of Allahabad

BACKSTAGE: The Story Behind India's High Growth Years by Montek Singh Ahluwalia. Rupa Publications, Delhi, 2020.

THIS is a long, rich, stimulating read written in an engaging style with superbly clear capsule explanations of complex policy issues. Insider accounts of the making of economic policy in India (indeed anywhere) are not all that common. The accounts of I.G. Patel, Duvvuri Subbarao and Venugopal Reddy are the ones that come readily to mind. This volume is closest to Patel's in that it is written by an outsider inducted into government service, rather than a career civil servant. This is a breed that is common in both the US and in France but still all too rare in India. In the book, the author adds Manmohan Singh, Vijay Kelkar and Bimal Jalan to this select group. Perhaps they too will one day oblige.

I cannot claim to be a disinterested reviewer, although I trust I am not uncritical. The book's chronology has reminded me of my own association with the author over more than a half-century. I first knew Montek, as he is universally called, at Oxford. He reached there two years before me, and was a celebrity for the triple distinctions of being a Rhodes Scholar (housed at the same college as me), earning a rare congratulatory First (division) in his undergraduate finals in Philosophy, Politics and Economics (also my field, so I heard tales of his brilliance from college tutors whom we had in common) and for attaining the Presidency of the Oxford Union.

I followed him next to a World Bank transformed by Robert McNamara's arrival as President in 1968. Montek had recently married Isher Judge who worked at the International Monetary Fund and we met frequently in the same circle of friends. As he describes, Manmohan Singh encouraged him to apply from the World Bank for a vacancy as Economic Advisor in the Ministry of Finance. Once selected, Montek, Isher and their two-year old son returned to India in 1979 arriving at a time of political and economic turmoil which lasted for much of the following decade.

The first half of the decade included Indira Gandhi's return to power, a programme with the IMF following the second oil shock, Operation Bluestar against the sanctity of the Golden Temple, Mrs Gandhi's assassination, and anti-Sikh riots in Delhi. This was a deeply distressing time, particularly for a Sikh couple living in Delhi. The massive parliamentary victory of Rajiv Gandhi in the 1984 election led to a move in 1985 from the Finance Ministry to the Prime Minister's Office (PMO) as Additional Secretary (later Special Secretary), the first step in the transformation into a government decision-maker.

The sustained decline from Rajiv's triumph to his tragic assassination and the political and economic debacle of 1991 was witnessed by Montek first from the PMO and then a move to Commerce Secretary in 1990 in the Chandra Shekhar government, with Subramanian Swamy as his minister. Much in the book about this period was new to me as I worked and lived abroad at the time. The sympathetic depiction of Rajiv Gandhi was one surprise. Despite (or because of) his prior reluctance to get involved in politics, Rajiv was able to envision the India that now surrounds us: youthful, middle-income (if not yet middle class), tech-friendly and aspirational. He also assembled a loyal team, inside and outside the bureaucracy, to implement some of his ideas. His lack of political experience was his undoing: the handling of Bofors; the response to the Shah Bano judgement; his differences with V.P. Singh among others in his initial cabinet and his inability to force change within his own party despite a parliamentary triumph of his making.

The book also helped me to see V.P. Singh in a new light; I had previously only associated him with the decision to implement the recommendations of the Mandal Commission on reservations for the Other Backward Classes (OBCs), the politics of which Montek explains. As Finance Minister with Rajiv Gandhi he articulated a long-term fiscal policy framework, designed to help the private sector anchor its investment decisions. This *inter alia* can be seen as recognition that the private sector needed to be enlisted as a partner in India's development rather than just a goose to be plucked. He concurrently initiated a series of indirect tax reforms in 1987 which set India on the road to the constitutional amendment enabling the Goods and Services Tax (GST) in 2017.

Also interesting is the discussion of the so-called 'M document': labelled as such when a version of the document was leaked in the press with the identity of the author being guessed at but not known. To my knowledge this is the first full account of how this influential document came to be written, and acknowledgement by Montek of his authorship. V.P. Singh commissioned the document in his brief year as prime minister from Montek (still at the PMO despite the change in government). The request followed a joint visit to Kuala Lumpur where Malaysia's evident economic progress impressed the prime minister. Despite complicated coalition politics which were left-leaning,

the PM directed that the document be scheduled for formal inter-ministerial discussion at the secretary level, chaired by the cabinet secretary, a further indication of V.P. Singh's open-mindedness on reform. Montek graciously notes that the two-day discussion of the paper among his bureaucratic peers was 'among the most stimulating discussions I have had in government' (p. 109).

The 34-page document (titled 'Restructuring India's Industrial, Trade and Fiscal Policies') allowed Montek to apply his experience of a decade in government to address what he had long regarded as India's central economic challenge: 'how to break out of the low-growth trajectory and ensure that higher growth would benefit lower-income groups in sufficient measure' (p. 40). The paper itself is succinctly summarized in the book. Its core argument was that the fight against poverty could advance more quickly through greater integration with the global economy. Thirty years later these ideas are more widely accepted, if once again under challenge. At the time external engagement was still seen by much of the Indian policy elite as leading to economic and diplomatic vulnerability and not a way to attain enhanced economic resilience.

The paper argued that policy coherence required coordinated action across several central government organs, particularly the Ministries of Finance and Commerce as well as the Reserve Bank of India. Such coordinated action was incompatible with the machinery of government decision-making where proposals rose vertically to a single minister. The instruments of coordination at the apex level (the PMO, the Cabinet Committee on Economic Affairs and the Committee of Secretaries) were political mechanisms for brokering inter-ministerial differences, rather than instruments for creative, collaborative problem solving at the working level. These issues, serious enough when a single party dominated government, were even more intractable when a coalition was in power.

The moment was not yet propitious for these ideas. Chandra Shekhar replaced V.P. Singh; the first Gulf War intensified a balance of payments crisis already underway through fiscal excess; the Congress party withdrew its outside support and fresh elections were held in May and June 1991.

The above accounts for the first third of the book. The remaining two-thirds covers the high noon of Montek's professional career, continuing as Secretary in Commerce and then moving to Secretary Economic Affairs in the Finance Ministry while Manmohan Singh was Finance Minister. This was during the full-term, if fragile, government of Prime Minister Narasimha Rao (1991 to 1996). That term was deeply impacted by the demolition of the Babri Masjid in December 1992 and consequent Mumbai bombings in the following year, as well as division within the Congress party. The result was defeat in the parliamentary elections at the end of its term. These political developments, as well as the fraud in government securities markets perpetrated by Harshad Mehta in 1992, overshadowed the remarkable recovery of the economy, allowing the government to exit from its IMF programme within two years.[1] Over this period Montek was designated Finance Secretary and continued to serve as such in the two brief successor United Front governments until the full-term government of the National Democratic Alliance (NDA) helmed by Prime Minister Vajpayee was voted into office in 1998.

With the change in government Montek elected to move to the Planning Commission as Member, then a brief stint in Washington DC when selected by the IMF Board as the founding Director of the Independent Evaluation Office (IEO). There he was instrumental in setting up procedures and protocols that have helped that office mature over the last twenty years despite an inherently tricky relationship with management and staff.[2] His term there was cut short by an invitation in 2004 by Prime Minister Manmohan Singh to return to India as Deputy Chairman of the Planning Commission (with Cabinet rank) and he served the nation in that role for a decade. While Manmohan Singh has continued in public life, Montek has chosen not to do so.

The later parts of the book are as much thematic as chronological. They provide an insider's view of the 1991 reforms, as well as of the achievements of the two UPA governments led by Manmohan Singh: fast growth, reduced poverty, elevation to the top table of economic diplomacy as a member of the G20 Leaders' Group to respond to the 2008 global financial crisis

1. I was witness to these economic and political developments in Mumbai on a two-year leave from the World Bank (1992-94) working with Governor C. Rangarajan and S.S. Tarapore at the RBI on the monetary, banking and capital markets follow-up to the 1991 reform package. This engagement led later to my participation in the 2007 Committee on Financial Sector Reforms convened by Montek from the Planning Commission and chaired by Raghuram Rajan, then teaching at the University of Chicago.

2. As the book observes, this experience motivated Montek's attempt to set up an independent evaluation function in India, which, like the Planning Commission, was abolished by the Modi government soon after it took office.

(with Montek serving as the PM's G20 'sherpa'), rapid recovery (without IMF help) from the shock of that crisis; and the major strategic breakthrough of the civil nuclear deal with the (surprisingly sympathetic and far-sighted) Republican administration of George W. Bush. This was in the face of stiff ideological resistance from the left parties in the UPA-1 coalition.

These were largely achievements of UPA-1. Re-election in the midst of a global crisis was an achievement but in a reprise of the Rajiv and Rao governments, the latter years of UPA-2 were marked by a souring of public perceptions which led to the convincing victory of Narendra Modi in the 2014 election, a mandate renewed with equal vigour five years later. Multiple explanations are available for this defeat: need for a change after ten years, slowing growth, rising inflation, shifts in ministerial portfolios, the compulsions of coalition politics and allegations by important constitutional bodies of large losses to the exchequer in the allocation of natural resources. The book provides a stout defence against these charges but in politics it is perception that matters. The book ends with an epilogue commenting on the economic management of the first Modi government and the economic priorities at this time. It was written literally days before the enormity of the Covid-19 crisis in multiple spheres – medical, social and economic – was recognized.

In an already long review, space permits reflection on only a few of the themes that run through the volume. The book's advance publicity highlighted an occasion when the prime minister asked Montek if he ought to resign. They were on an official visit to New York when, at a public briefing in Delhi, then Congress Vice-President Rahul Gandhi rubbished the government's decision to introduce an ordinance that would have spared Lalu Prasad Yadav, a Congress ally, from having to resign his seat in Parliament as instructed by the Supreme Court. Montek dissuaded the prime minister from doing so, a recommendation he does not regret, and which he defends in the book. This episode speaks to the long personal and professional association between these two talented, reserved and occasionally controversial individuals. Each of them started out as a cosmopolitan technocrat at a time when India was suspicious of foreign engagement. Working with others they chose their moments to persuade the political class to follow a changed path on both the economy and in foreign policy.

Despite these considerable achievements, at several points in the book Montek rues that political support for liberal reform has at best been hesitant. He pithily describes the cautious continuity of policies as: 'a strong consensus for weak reform' and the mechanics of achieving change as 'reform by stealth'. As Australia's Ross Garnaut[3] has noted, it takes committed leadership for any political party to reject policies associated with its past leaders even as the world changes around them. China was lucky with Deng Xiaoping who had the skills and power to reframe the legacy of Mao, and Australia's Labour Party rejected four decades of inward-looking policies under Bob Hawke and Paul Keating not soon after. The Congress party left reform to the technocrats who made as good a fist of it as they could. More puzzling has been the caution of the BJP, less encumbered as it is by the political baggage of the past.

Despite this political hesitancy the India of 2020 is a very different nation from the India of 1990. The Vajpayee government (NDA-1) marked the start of a run of five consecutive full-term governments with coalition leadership rotating between the two national parties. This marks impressive maturity for a polity of India's diversity and demography in the face of the stresses of fast growth, urbanization and dramatic shifts in social and gender status. The epilogue to the book reminds us of the large unfinished economic agenda (agriculture, human development, transparent banking, labour-intensive manufacturing, infrastructure and labour market informality among them) after fifteen years of Congress-led coalitions and eleven years under the BJP. Equally the continued opacity of electoral finance and the ills that it breeds, our creaking judicial and policing systems, and an unreformed senior civil service are all fixable drags on our progress. Despite these infirmities, and a fair amount of bloodshed along the way, this seemingly ramshackle structure has so far proven resilient. The Covid-19 virus will test this resilience as perhaps never before.

Suman Bery
Global Fellow, Woodrow Wilson
International Centre for Scholars,
Washington DC

3. Ross Garnaut, 'India, China and Australia: Lessons from Different Paths in Economic Reform'. The 2004 Sir John Crawford Lecture, National Council of Applied Economic Research (NCAER), New Delhi, 28 September 2004. https://cpb-ap-se2.wpmucdn.com/blogs.unimelb.edu.au/dist/a/142/files/2016/01/India-China-and-Australia-2004-1lxg97x.pdf. Last reviewed 17 May 2020.

Advertisement

In memoriam

Ashok Desai 1932-2020

IT was Madhu Dandavate, Minister of Finance in the Janata government, who, in December 1989, brought Ashok Desai from Bombay to Delhi. Ashokbhai came to the capital as the Solicitor General of India, in what was part of Soli Sorabjee's (the then Attorney General) team in the V.P. Singh government. Once here, he never went back.

Ashokbhai's shift to Delhi left behind a void in the Bombay Bar, which was never quite filled. To fully understand his place in the pantheon, a little digression is required. The Bombay Bar (to the unfamiliar) was the premier Bar of India from the 1950s all the way till the mid-80s. It gave to independent India its first Attorney General, Motilal Setalvad, and its first Chief Justice, Justice Harilal Kania. In the fifties, its unquestioned leader was Sir Jamshedji Kanga, who in turn made way for his two Chamber Juniors – Nani Palkhivala and H.M. Seervai.

Active private practice, however, soon eluded both of them, as Seervai went on to become Advocate General of Maharashtra, and thereafter, spent many years as A.G., away from his practice, writing his magnum opus, *Constitutional Law of India*. Nani too, soon left active practice and settled down in the comfort of the fourth floor (management) of Bombay House. He would occasionally leave the Tata boardrooms to argue important constitutional cases: R.C. Cooper (the bank nationalization challenge), Madhav Rao Scindia (the privy purses case) and, of course, Kesavananda Bharti (the fundamental rights case). He also would step out once a year to address a large crowd, in one of Bombay's maidans, to speak on the Union Budget.

So, with the partial exit of these stalwarts, the baton was handed over to two other chamber mates from Kanga's stable – Fali Nariman and Soli Sorabjee. Theirs was a fierce rivalry that lasted through a large part of their lives, and propelled both to the pinnacle of not only the Bombay Bar, but also the Supreme Court Bar. However, Fali left Bombay for Delhi in 1972, and Soli in 1977. The void post Soli's exit, left the Bombay Bar without any one undisputed leader. Anil Divan in the Writ Court, along with young Atul Setalvad, a brilliant K.S. Cooper, a successful Ashok Desai, and a very young Iqbal Chagla, all made their mark, but none quite dominated the scene.

All this prevailed till the middle of April 1982. The date is clearly etched in my memory because my friend Navroz Seervai could not come to Delhi on the 17th of April 1982, to attend my wedding with Manik. He was instructing Ashok Desai in the Antulay case. Ashokbhai, despite a large commercial practice, had been no stranger to fighting for public causes. He had fought the case against the banning of Vijay Tendulkar's play *Sakharam Binder*; appeared for Piloo Mody in the Backbay Reclamation case; and during the Emergency had appeared for the *Bombay Law Reporter*. But, the Antulay case was to define Ashokbhai more than any other. Justice Lentin's judgement not only unseated a Chief Minister, it also coronated Ashokbhai as the undisputed leader of the Bombay Bar.

Those in the know inform me that after the Antulay case, Ashokbhai, with his shrewd eye for the big chance, increased his fee fourfold and, despite that, doubled his practice. He would charge 100 GMs (gold mohors) before the Antulay case; post that, he increased his fee to 400 GMs and never looked back. From 1982 till 1989, he remained the unquestioned king of the Bombay Bar. His affable nature and acute advocacy made him the darling of both the Bar and the Bench. Legend has it that when he shifted to Delhi, it took five Senior Counsel to come forward and absorb his practice.

On a personal note, though I had worked with Ashokbhai in the Swadeshi Polytex matter quite closely, in the year 1983 in the Supreme Court (the matter had gone on for months), it was not till the early '90s, when he began private practice in the Supreme Court, that he and I became really good friends. It was from '91 onwards that Ashokbhai and I began a regular, and later, a constant interaction, both on professional and personal fronts. The two cases that I personally remember interacting with him on extensively, were the Simbhaoli Sugar Mills case in the Delhi High Court and the Sharad Pawar election case in the Supreme Court.

Ashokbhai's style of advocacy was quite unique. He was pleasantly pushy and quietly persistent. If the judge did not bite on a particular point, he adroitly

sidestepped to another one, in order to pierce the judge's defences. He rarely got flustered, no matter how hostile the judge was to the arguments advanced and would always keep the atmosphere in court pleasant. As he once said to me, 'Raian, I never like to be told that a judge is against me, because I don't want it to subconsciously make me more defensive or aggressive when I address him.' Like all great advocates, he was able to ensure, many more times than not, that his client came out of court better off than when he went in.

Getting to know him at the personal level, as well as I did, I realized that Ashokbhai was a man of many parts and varied interests. His love for music encompassed both western and Indian classical. He was fond of literature. He married Suvarna, who, along with her sister, was one of the most famous Manipuri dancers of her time. Socialist in his political ideology and tending towards Buddhism in matters of religion, Ashokbhai was also a practitioner of Vipassana meditation. His simplicity and austerity encompassed a modern mind. Popular with all, he was admired, respected and loved by those who worked with him, especially his juniors. He was a very kind and caring friend, offering help when needed in the most unobtrusive and gentle kind of way. His friendship was rock solid.

Ashokbhai was a man of quiet principle, setting for himself very high standards of probity. I was particularly pleased that when the United Front government came to the fore in 1996, Vinod Pande, former Cabinet Secretary, and I, in some small measure, were able to persuade V.P. to speak to the then PM, Deve Gowda, to make Ashokbhai the Attorney General. Both Vinod and I felt it would be a fitting culmination to a glorious career. The Prime Minister agreed on one precondition, that he would first offer it to Fali Nariman, and only if Fali declined, would he appoint Ashokbhai. Factually, the then PM offered Fali both the position of Attorney General and also the post of Law Minister. It was only when Fali declined that Ashokbhai became Attorney General.

On the point I raised earlier, of Ashokbhai holding himself quietly to the highest standards, I remember years later Arun Jaitley, as Law Minister in Atalji's government, telling me that he had personally examined the records and found Ashokbhai was the only AG who had never once asked for special exemption as AG to appear for a private party.

Before I end this tribute, I want to allude particularly to one aspect of Ashokbhai's personality, and that was his ability to get along and be at ease with any kind of person, rich or poor, important or inconsequential. I mentioned this to him once and the explanation he gave me was fascinating. He pointed out to me that despite being the son of Haribhai Desai, one of Bombay's leading criminal lawyers, he had studied till class 6 or 7 in a municipal school, which was called Bai Kabibai. 'You see Raian,' he said to me, 'I am, therefore, equally at home with a managing director of a large company as I am with the tonga boy's son.' With his passing away, the Bar has lost one of its true stalwarts, and both Manik and I have lost a true and good friend.

Here, I owe the reader an explanation, and the family an apology. This remembrance is a couple of months late. I had agreed to write for another paper a few months ago, but kept procrastinating. I am glad that Mala cajoled and bullied me to put pen to paper. More so because *Seminar* is a magazine that was close to Ashokbhai's heart, and he would have been glad to find himself being celebrated and remembered for posterity in its pages.

Raian Karanjawala
Founder and Managing Partner,
Karanjawala and Co, Delhi

Vijaya Ramaswamy 1953-2020

THE academic world in Delhi was an exciting and challenging one in the 1970s. Amongst those who lived and breathed that excitement, and carried it with her to the very end, was Vijaya Ramaswamy.

Born in Delhi in 1953, Vijaya graduated in History from the prestigious Lady Shri Ram College, Delhi University, before joining the very first batch of MA students enrolled at the Centre for Historical Studies, Jawaharlal Nehru University. This was a time when new courses were being introduced, marking a shift away from programmes dominated by political/dynastic histories to ones which were oriented towards asking fresh questions, primarily from the point of view of economic history, but also opening up possibilities of fresh investigations in social and cultural history. Vijaya absorbed everything that was on offer, and more, with a zeal and enthusiasm that enabled her to make the most of interdisciplinary approaches and adopt and adapt these in her future work.

Vijaya went on to do her PhD, subsequently published as *Textiles and Weavers in Medieval South India* (Oxford University Press, New Delhi, 1985; second revised edition, 2006). This work was remarkable for a variety of reasons. It cut across the conventional chronological divides, tracing developments over a long

period, from the early historic to the colonial context. Also, the engagement with crafts and craftspersons would become a lifelong interest, bringing ordinary people and their lives centre stage. These investigations were based on the use of a wide variety of sources – textual, inscriptional and ethnographic. Vijaya's ability to empathize with crafts workers allowed her to reach out to them. These bonds proved to be enriching and enduring. They found expression in *The Song of the Loom* (Primus,New Delhi, 2013), and *In Search of Vishwakarma: Mapping Indian Craft Histories* (Primus, New Delhi, 2019).

Almost simultaneously, in the 1980s, Vijaya developed a deep and abiding interest in feminism and women's studies, inflected by her own quests. These led her in a variety of directions, and, typically, she pursued them with enthusiasm, returning to them time and again, in the decades that followed. One of the most sustained of these, and perhaps closest to her heart, was the attempt to recover and share the experiences of women in search of enlightenment, spiritual, mystical pursuits that often eluded cut and dried categories of analysis. The insights she obtained culminated in *Walking Naked: Women, Society and Spirituality in South India* (Indian Institute of Advanced Study, Shimla, 1997). This, like *Textiles and Weavers,* worked with a long chronology, beginning with Sangam texts, engaging with Buddhist and Jaina traditions in South India, as well as the many strands of Bhakti, both Vaishnava and Shaiva, including the Virashaiva movement. The last was something that she found compelling, devoting a separate monograph to it, *Divinity and Deviance* (Oxford University Press, New Delhi, 1996). Several years later, when she joined the faculty of the Centre for Historical Studies, JNU, she returned to the broad contours of these investigations, and introduced a course on devotion and dissent, which familiarized students with a range of traditions that were not part of mainstream histories.

Vijaya also succeeded in combining her diverse interests. This is perhaps best exemplified in the anthology that she edited, *Women and Work in Precolonial India* (Sage, New Delhi, 2016), documenting the evidence for the participation of women in a range of economic activities in different regions of the subcontinent through the centuries. The anthology showcased the work of both young and established scholars, drawing attention to an area that was relatively neglected. Another edited anthology, *Migrations in Medieval and Early Colonial India* (Routledge, Oxon, 2016), also opened up fresh areas of investigation.

In both her work on weavers, as well as on devotional traditions, Vijaya drew on the resources of Tamil. Her deep and abiding engagement with the language enabled her to produce the *Historical Dictionary of the Tamils* (Scarecrow Press, Lanham, 2007/2017), at once lucid and wide-ranging.

A prolific scholar, Vijaya contributed papers and made presentations at seminars and conferences throughout the country and across the globe. She was the recipient of several awards and fellowships. These included the Fulbright Fellowship, the Commonwealth Fellowship, fellowships at the Indian Institute of Advanced Study, Shimla, where she was Tagore Fellow till the end, and the Nehru Memorial Museum and Library Fellowship. She used each of these opportunities fruitfully, and productively, as occasions to explore, work on cross-cultural comparisons, and expand her academic horizons in a variety of directions. The Indian History Congress recognized her as the best woman historian in 2001.

As, if not more remarkable, was the fact that Vijaya combined this prolific academic output with a deep commitment to teaching. She began teaching undergraduate classes in Gargi College, Delhi University, where she taught for several years. She adapted to the bilingual teaching modes that were often in demand, switching from English to Hindi and back as and when required. Vijaya also learnt Sanskrit diligently, and could use Malayalam and other languages as and when required.

Vijaya taught postgraduate classes in Delhi University, before returning to the Centre for Historical Studies as a faculty member, where she served till her retirement in 2018. In all these institutions, she endeared herself to her students by her almost contagious excitement about what she was teaching and what they were doing. Her affection, warmth and concern for students was palpable, and was more often than not reciprocated. She also shouldered administrative responsibilities, often onerous, in these institutions.

Vijaya's relationships with her colleagues were more complex. She could be determined, if not stubborn, transparent, where people may have preferred tact; but what shone through, at the end of the day, was her compassion. She extended herself, effortlessly, to people in distress. She also had an immense ability to laugh at herself and others.

Vijaya's sudden and untimely passing has left us all impoverished. We will miss her laughter, warmth, zeal, passion, and her commitment to research, publica-

tion and dissemination. But her legacy will remain, sustained by enthusiastic young students and researchers whom she nurtured with affection and encouragement.

Kumkum Roy
Professor, Centre for Historical Studies,
Jawaharlal Nehru University, Delhi

Ajay Singh 1950-2020

BAPTISM by fire is an irresistible temptation on the brink of a second life. On a wintry morning in 1989, a few minutes before 11, Ajay Singh and I, very conscious of new beginnings, entered Parliament as newly elected members of the ninth Lok Sabha. We drove up in the same vehicle and stepped through those dream-gates together, quite determined to make a point that might seem minor in the larger scheme of things, but which mattered to the two of us. We were headed for opposite sides of the House: he towards the fragile Treasury benches, and I towards a badly mauled opposition. Our assertion was uncomplicated. A political divide, in the parlance of common sense, did not mean a fractured friendship.

We knew that yet another season of fireworks was upon us, for the intense friction of power had already lit flames, fanned by electoral rhetoric, which threatened to go out of control. What neither of us expected was the astonishing conflagration that consumed the House and ravaged India's political environment.

The difference between amused and bemused seems clear enough in a dictionary. In Ajay's continual rather than continuous engagement with public life over the following three decades, an overlap prevailed. He seemed more amused than angry at the mercurial behaviour of leaders without a cause, who banded and re-branded at the whiff of self-interest. He was bemused at the consequent havoc upon his personal trajectory across the political horizon, which got trapped due to circumstances beyond his control. It was a slow seepage of opportunity that could have made far better use of his deep commitment and considerable talent. He was too soft-spoken to be rancorous, too gentle to be angry. His regret would, at worst, turn into melancholy during an evening's attempt to ameliorate the injustices of the day.

But he had the grit to rise above the mishaps of an erratic destiny. He created a constituency much larger than the sometimes claustrophobic limits of a Parliament seat, a socio-economic expanse which he nursed with a soft touch and hard resolve. His singular asset was a caring smile which spoke eloquently to the thousands of mainly villagers who came to seek his help through the association he chaired.

Two national leaders truly understood his values and value: George Fernandes and Kunwar Natwar Singh. The latter gave Ajay the three best years of his career, when he became India's High Commissioner in Fiji. His father Bhagwan Singh had once served there as well, but there was a better reason. Fiji was also his sasural, where he met and married his beautiful and vivacious wife, Shiromani. Ajay's greatest shock was the catastrophic loss of Shiru three years ago. That scar never could heal.

Ajay, a brilliant swimmer, once mentioned to me how he and Shiru would swim far out into the ocean around Fiji to measure their youthful prowess. Hindsight, always convenient during consideration, now seems to suggest that behind the gentle demeanor of Ajay hid a man constantly in search of some shore on the opposite side of convention. He was never a radical or an extremist, and had abandoned the siren symphonies of maverick ideology even during the persistent call of a Delhi college campus. But he was an activist with a conscience. He did not believe he could change the world but he did want to melt the iron cuffs of casteism and communalism that had fettered so many Indians.

All lives end. That is an unsentimental truth. But for friends every funeral is a journey into the past on the rollercoaster of might-have-beens; every tinge of sorrow is leavened by the memory of evenings resplendent with sensible and senseless laughter. We first got to know each other in that informal club which met in the heady ebullience of March 1977, when the Indian voter humbled an empress who had imprisoned democracy. For us, despite the turbulent aftermath, the 1980s were prime time.

Now, as dusk deadens the evening with obituaries, there is but one prayer. Friends should not leave without saying goodbye.

It strikes me, as memory skips through innumerable conversations, with the difficult balance sheet of religion in politics a regular point of debate, that I never asked Ajay if he believed in God.

No matter. Ajay Singh believed in himself. It is a sound maxim for this life. We can leave the next life to God.

M.J. Akbar
Author and BJP MP, Rajya Sabha