India-France: Forging a Cyber-partnership

Archana Atmakuri and Karthik Nachiappan

Summary

Indian Prime Minister Narendra Modi's visit to France in August 2019 has expanded the India-France strategic partnership from issues like defence and security to technology, covering matters like the digital economy, data governance and protection, privacy and cybersecurity. Discussions on new technologies are driven by legacy of close strategic ties and bubbling domestic priorities. France's importance and value stands to rise in New Delhi with the inclusion of cyber and digital issues to the bilateral agenda.

That Indian Prime Minister Narendra Modi travelled to France about three months after a thumping re-election should not surprise anyone. Ruptures in international politics and the realignments it is feverishly spawning has driven New Delhi to shore up reliable international partners. France tops the list of preferred partners given its size, status and strategic value. New Delhi and France have forged a robust security and defence partnership since 2014; this partnership is now poised to move into areas like climate change, energy and, critically, technology.

When French President Emmanuel Macron visited New Delhi in 2018, both countries signed 14 agreements on issues like defence, nuclear, climate change, energy, space and multilateral issues. In 2018, both countries announced the development of a new generation jet engine through a project tentatively named INFRA. Both countries have pledged to support the freedom of navigation across the Indian Ocean; they have also reiterated the importance of the rule of law and for free and open navigation in the Indo-Pacific against threats like piracy, human trafficking, illegal fishing and smuggling. In fact, both countries announced a joint strategic vision in the Indian Ocean that entails positioning space technologies to enhance maritime awareness. Bilateral discussions now enter the technology domain that is awash with various challenges.

Technology issues like cybersecurity, digital communications, particularly misinformation and fake news, and the digital economy enter the bilateral agenda on its own merit. In August 2019, India and France released a joint roadmap on technology and cybersecurity that "affirms both countries' commitment to an open, reliable, secure, stable and peaceful cyberspace." The roadmap outlines collaboration in two areas – first, cybersecurity that includes fighting cybercrime, deterring cyberattacks and protecting data; and second, regulating digital governance by reducing misinformation, managing artificial intelligence, protecting data, minimizing terrorist and extremist content and reducing the digital divide within populations. That the initial agenda involves a litany of issues exemplifies the growing importance of technology to foreign policy. Besides the US, France is the only country with whom India has signed a detailed framework to further cyberspace cooperation.

The new impetus on technology comes when both countries are facing policy challenges from insecure cyber systems and the sweeping use of digital systems for commerce. Cyberattacks are a key challenge. France experienced about 19,000 cyber-attacks in the wake of the Charlie Hebdo attacks in 2015. Attacks on cyber systems in India are rising from state and non-state actors. Sectors like banking, critical infrastructure, telecommunications, defence and government websites are most vulnerable to cyber-attacks in India. To cleanse cyberspace, President Macron unveiled the 'Paris Call for Trust and Security in Cyberspace'- a global effort bringing governments, businesses and civil society to protect and defend digital infrastructures. The Elysee's initiative seeks to erect globally applicable norms for the internet with equal, if not more, responsibility placed on technology companies; the initiative, however, does not require countries to adhere to specific principles or amend its laws to prevent digital harm. The Paris Call does comport with India's proposed cybersecurity policy that expects public and private sector collaboration to deter cyberattacks. The roadmap also pushes both countries to "share information on the legal and regulatory framework and best practices," to help eradicate activities like hacking, phishing, worms and data theft.

The second plank of the bilateral focus on technology covers the regulation of digital activities. Unsurprisingly, this focus is driven by the rise of the digital economy in both countries. India's ongoing digital transformation is spreading across industries from traditional sectors like retail and telecommunications to other sectors like health, logistics and energy that have not been overtly digitised. Use of web platforms and apps to provide welfare benefits, transfer money, purchase goods and services, conduct business and perform other tasks is generating new challenges concerning citizen data and privacy; moreover, public cries to anchor data rules around privacy have risen. New priorities have surfaced; plans to launch 5G technologies trials is set to boost the Internet of Things (IoT) and machine to machine communications in both countries, promoting the development of driverless vehicles, tele-surgery and data analytics. That said, both countries are at different stages with respect to technology and cyberspace regulation with France ahead on the technological side. Despite different junctures, however, discussing issues like data governance and the digital divide, in the context of the digital economy, could bridge bilateral differences on data protection.

The scope exists to deepen bilateral cooperation on technology and digital issues. France and India have held three inter-governmental cyber dialogues and committed to share information between cyber agencies. With cases of misinformation rising, especially during elections, both countries reaffirmed the responsibility and accountability of social media platforms to moderate extremist content and hate speech. Broadly, both countries share a mutual desire to mitigate cyberattacks and find common ground on data protection rules. Whether technology talks could lead to policy convergence on key issues remains to be seen.

. . . . .

Ms Archana Atmakuri is a Research Analyst at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). She can be contacted at archana@nus.edu.sg. Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies, National University of Singapore. He can be contacted at isaskn@nus.edu.sg. The authors bear full responsibility for the facts cited and opinions expressed in this paper.