11

Stacking Up for Resilience

Digital Public Infrastructure: The India Way

Ravi Nayyar

The word "democracy" literally means "rule by the people" (Dahl & Shapiro, 2024, para. 1). Democracy is underpinned by the right and power of people in a jurisdiction to shape their collective destiny. This is enshrined in international law. Article 21 of the *Universal Declaration of Human Rights* (1948) defines the authority of government as stemming from the will of the people who elected it, the right of the people to participate in their government, as well as the right of the people "of equal access to public service" in their country.[1] Article 1 of the *International Covenant on Civil and Political Rights* (1976) similarly enshrines the right of all to self-determination and thus their right to "freely pursue their economic, social and cultural development."[2] The United Nations generally advocates for democracy as a system of governance where the "freely expressed will of people is exercised," and which enables greater security and human development (United Nations, 2019, para. 4). Therefore, democratic rights comprise both specific human rights such as freedom of expression and peaceful assembly and association (United Nations, 2019, para. 5) and, more generally, to enable the people of a jurisdiction to determine how they are governed and how they pursue the development of their society and economy.

Economic development – the process followed by an economy in becoming more advanced, "especially when both economic and social conditions are improved" ("Economic development," 2023) – and the promotion of human rights, including democratic rights, share a symbiotic relationship. For example, Articles 23 and 25(1) of the *Universal Declaration of Human Rights* (1948) protect one's entitlement to what are arguably the fruits of economic development, including the

The author profusely thanks Associate Professor Chinmayi Sharma for advising him of the opportunity to be a part of this wonderful project on defending democracy in the digital age and for her help in conceptualizing this chapter.

[1] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, UN Doc A/810 (December 10, 1948).

[2] International Covenant on Civil and Political Rights, opened for signature December 16, 1966, 999 UNTS 171 (entered into force March 23, 1976).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

right to an appropriate standard of living, food, the best of health and certain employment protections (Feldman et al., 2016, p. 7). Sen (2001, p. 36, emphasis in original) argues that conferral of human rights (the "expansion of freedom") functions "as both … the *primary end* and … the *principal means* of development." In underpinning economic growth, economic development is among "the most reliable means for advancing human rights," which include democratic rights (Feldman et al., 2016, pp. 6–7; Marslev & Sano, 2016, p. 15). For instance, economic development enables richer participation in societies by citizens, given that they feel more secure in their ability to express their political views if they are confident about their financial and food security, and having a home to go back to. Therefore, economic development (and subsequent economic growth) can bolster the trust and confidence of citizens of democracies in democracy itself as a means of delivering tangible benefits for them; and thus, the capacity of democratic institutions to promote and preserve their human rights through their roles in the making and/or adjudication of law and/or policy concerning economic development.

As enablers of economic development, and thus growth by providing essential services for citizens to live and flourish, critical national infrastructure (CNI) assets play a vital role in the promotion of citizens' human rights, including their democratic rights. Indeed, citizens' ability to do anything in modern societies depends on the availability of, for instance, electricity, telecommunications, and water treatment that are provided by CNI assets (Parliamentary Joint Committee on Intelligence and Security, 2022). Their protection is a "sovereign necessity," given the relevance of the assets' functioning to these societies' national security (Parliamentary Joint Committee on Intelligence and Security, 2022, p. 6). Indeed, the very definition of CNI assets under national laws invokes their key role in the preservation of social or economic stability, national defense, and security (see, e.g., *Security of Critical Infrastructure Act 2018* (Cth) s 51(c); *Critical Infrastructures Protection Act of 2001* (2001) 42 USC § 5195(e)).

A species of CNI is digital public infrastructure (DPI). Given that this chapter is focused on the Indian approach to DPI, it will define DPI as per the definition agreed upon by the G20 under India's presidency of the multilateral grouping, that is, a "set of shared digital systems, built and leveraged by both the public and private sectors, based on secure and resilient infrastructure, and can be built on open standards and specifications," and open-source software (OSS), as well as an enabler of "delivery of services at societal-scale" (G20 Leaders, 2023, para. 55). The systems used to operate DPI (that this chapter refers to as "DPI Backbones") are CNI assets that are delivering digitally native essential services, promoting the human rights of users of those services and thus, if regulated by democratic systems of government, helping maintain the citizenry's confidence in democracy itself and the resilience of their democratic institutions. One should also note, for instance, the G20 countries' call in 2023 for DPI to be "human-centric, development-oriented" and be governed in a way that "respect[s] human rights and fundamental freedoms" (G20 Digital Economy Ministers, 2023, paras. 6, 7, Annexure 1, para. 6.j). These calls reflect the role

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

of DPI as an enabler of the preservation and promotion of human rights, including democratic rights, of citizens reliant on the services delivered through DPI.

In this vein, any threat to the operational resilience, including the cyber resilience, of CNI assets, such as DPI Backbones, is a threat to the human rights of the population they serve, including their democratic rights (see, e.g., Newbill, 2019, pp. 766, 771). Indeed, such a threat is also to their confidence and trust in the ability of democratic systems of government to regulate the functioning of CNI assets and thus promote their human rights. The United States acknowledges this in referring to cybersecurity as "essential to … the operation of our critical infrastructure, [and] the strength of our democracy and democratic institutions" (The White House, 2023, p. i). Similarly, the G7 Digital and Tech Ministers (2023, para. 15) defined "secure and resilient digital infrastructure" as "a key foundation for … an open and democratic society."

One should also note that two of the norms of responsible state conduct in cyberspace, approved by the United Nations General Assembly (UNGA) by consensus, called on states to appropriately protect their CNI assets, which would include DPI Backbones, from cyber-enabled threats, and – in ensuring they respect specific UN Human Rights Council resolutions on human rights in the digital age – to "guarantee full respect for human rights, including the right to freedom of expression," a democratic right (United Nations, 2021, pp. 8, 11, 13). This is complemented by how CNI assets themselves enable human rights promotion, as mentioned, and the implementation of international law and norms by which elected governments would give their citizens confidence in democracy as a mode of government itself. Therefore, work by governments to tackle cyber-enabled threats to CNI assets and thus boost their cyber resilience would promote and operationalize the UNGA-approved cyber norms, one of the themes of this book which adopts a wide, holistic approach to exploring how to defend democracy.

The conceptual relationships outlined in the preceding paragraphs are summarized in Figure 11.1.

This chapter focuses on India's DPI, the platforms and systems that deliver a range of digitally native essential services to the citizens of the world's largest democracy (Guterres, 2022, para. 10). As it highlights, Indian DPI has enabled an extraordinary level of economic development and growth. The cyber resilience of DPI Backbones is vital to Indians' trust in the democratic institutions that define, run, and/or oversee this infrastructure (such as the elected federal government) as bodies meant to promote their welfare and thus their human rights. This feeds directly into the resilience of Indians' faith in democracy as a concept. Any work by the Indian government to ensure the cyber resilience of DPI Backbones would also be implementing the aforementioned UNGA-approved norms for responsible state conduct in cyberspace.

In exploring Indian DPI, this chapter also argues that the bedrock of India's DPI, the actual open Application Programming Interfaces (APIs) and protocols called the "India Stack," make the latter fundamental to India's resilience as an increasingly digitally enabled democracy (iSPIRT, 2021). The chapter hones in on how the software dependencies of the India Stack and DPI Backbones invite systemic cyber

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

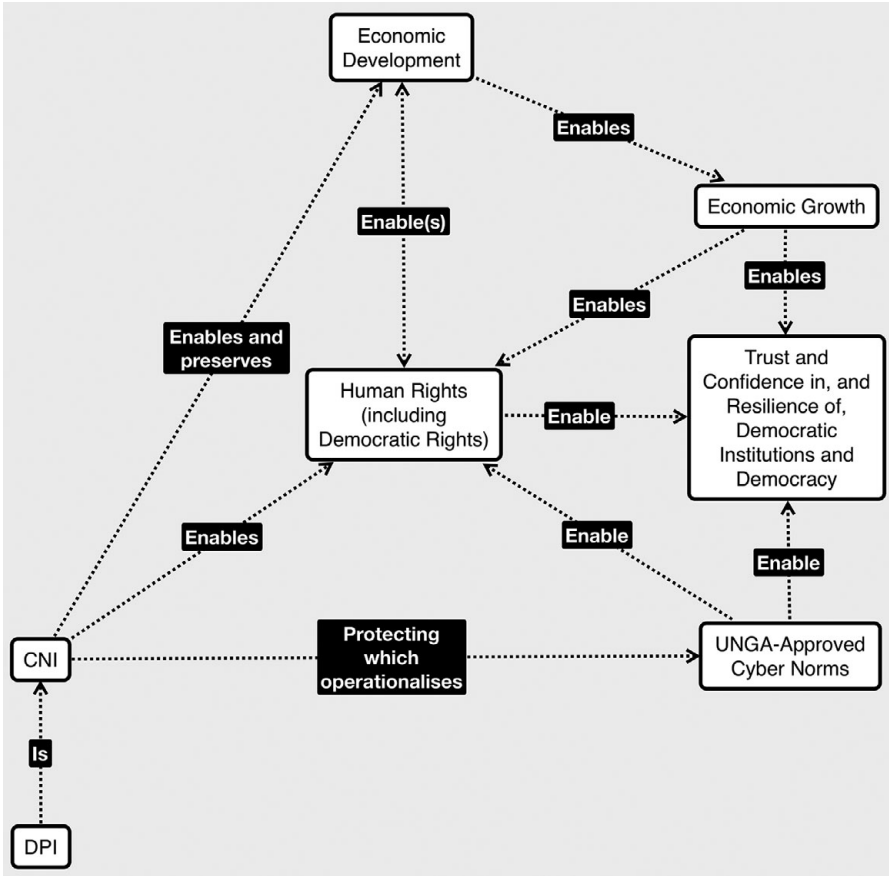


FIGURE 11.1 The relationships between critical national infrastructure (CNI; including digital public infrastructure (DPI)); economic development and growth; human rights; citizens' trust and confidence in democratic institutions and the resilience of those institutions; and United Nations General Assembly (UNGA)-approved norms for responsible state conduct in cyberspace (composed by the author)

risks for India as a democracy. In particular, it calls for India to prosecute systemic cyber risks that its DPI, built with the India Stack, faces via critical software which runs on India's DPI Backbones. This is justified with reference to the sheer complexity of (critical) software supply chains, the greater intent and capability of malicious cyber actors to target software supply chains, and the (recent) history of CNI assets more generally being attacked via vulnerabilities in, or misconfigurations of, critical software. There is also a recommendation that India closely scrutinize cyber risks invited by the use of OSS in building DPI, especially since the India Stack itself uses OSS (Alonso et al., 2023, p. 8). The chapter closes by exploring how India can take the India Stack, as well as its approach to building and deploying DPI more generally, to the world, particularly democracies in the Global South. It calls

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

on India to, as part of sharing its open standards-based approach to DPI, help its democratic Global South partners deploy DPI in a cyber-resilient manner to make it harder for malicious actors to disrupt the provision of essential services and thus undermine their citizens' faith in democratic systems of government as guarantors of economic development and human rights, as well as threaten efforts by these Global South partners to implement the aforementioned UNGA-approved cyber norms, per Figure 11.1.

This chapter defines "critical software" as software, the execution of which, broadly speaking, can seriously impact the cyber resilience of a computer running it, drawing inspiration from the National Institute of Standards and Technology (NIST)'s (2021) definition.

WHAT ARE DIGITAL PUBLIC GOODS AND DIGITAL PUBLIC INFRASTRUCTURE?

Before exploring the India Stack, two foundational concepts must be understood: digital public goods (DPGs) and DPI. DPGs are "types of open-source software, models and standards that countries can use to operationalize their [DPI]" (OECD, 2021, p. 257). DPI comprises "platforms such as identification (ID), payment and data exchange systems that help countries deliver vital services to their people" (OECD, 2021, p. 257). In this manner, DPGs are the building blocks of DPI and thus the essential services that the latter provide in societies and economies. DPGs and DPI are ever more crucial in light of the move of social and economic activity online since the pandemic (OECD, 2022, p. 5). DPGs thus democratize the ability to "participate fully in social, financial, and political life," given that said ability is technologically dependent (Behrends et al., 2021, p. 3). DPGs are, like the DPI they underpin, fundamental to democratic resilience in the societies where they are provided, given the relationships between DPI, CNI, economic development and growth, human rights, as well as the trust and confidence in democratic institutions and democracy as a concept (per Figure 11.1).

DPGs are defined by their open format, adaptable for different populations and contexts (OECD, 2021, p. 257). The underlying code and standards can be audited by the (government) organizations deploying DPGs in DPI, enabling the identification and management of vulnerabilities in the code and other potential shortcomings of the relevant DPGs before they are deployed widely across a population (OECD, 2021, p. 260). This transparency enables more effective and inclusive consultation of relevant stakeholders by (government) organizations deploying DPI, helping drive a better, more inclusive deployment that respects democratic values and helps inspire confidence in the ability of democratic systems of government to deliver economic development via DPGs and DPI.

Indeed, the role of DPGs as enablers of the flourishing of societies and democracies is well recognized. The United Nations Secretary-General (2020, pp. 6–7) pointed to their critical role "in unlocking the full potential of digital technologies and data to attain the Sustainable Development Goals, in particular for low- and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

middle-income countries." In addition to the technical infrastructure on which DPGs are deployed, what are essential to their deployment are common standards that enable open access to datasets that themselves become available as DPGs, as well as "robust human rights and governance frameworks to enhance trust in technology and data use, while ensuring inclusion" (United Nations Secretary-General, 2020, p. 7). These factor into efforts to ensure that DPI itself is developed and deployed in a manner that respects human rights, per the calls of the G20 (G20 Digital Economy Ministers, 2023, paras. 6, 7, Annexure 1, para. 6.j). Therefore, the safely calibrated deployment of DPGs as part of DPI is vital to trust and confidence in democratic institutions running and/or overseeing that deployment and the resilience of the democracies where that deployment occurs.

The nature of DPGs can also be understood by contrasting their reflection of an open approach to the digital delivery of essential services to citizens with the closed approach of private companies. Historically, private companies have often provided these digitally delivered services because of their having the capacity to build and deploy the necessary infrastructure at (population) scale and in an economical manner (Burt, 2018, as cited in OECD, 2021, p. 257; ID4D, 2020, as cited in OECD, 2021, p. 257). Since they own the intellectual property underlying these services and infrastructure – and set the terms and conditions of their use – these companies have substantial influence, if not control, over whether and how these services are delivered, including over their benefits to citizens (Burt, 2018, as cited in OECD, 2021, p. 257; ID4D, 2020, as cited in OECD, 2021, p. 257). These companies are powerful gatekeepers and, given the centrality of these services to the ability of citizens to meaningfully participate in their societies and economies, have great influence over the conduct of affairs in a democracy (Behrends et al., 2021, p. 5). In this manner, the digital delivery of essential services by private companies threatens the digital sovereignty of democracies, that is, their governments' "power and authority . . . to make free decisions affecting citizens and businesses within the digital domain" (Gawen et al., 2021, as cited in OECD, 2021, p. 257). These companies threaten the ability of democratically elected governments to act in the interests of the people who elect them, the very essence of democracy, including by working toward their economic development by achieving the Sustainable Development Goals (OECD, 2021, p. 257). Conversely, this underlines the criticality of DPGs as pillars of the collective ability of the people of a democracy, via the governments that they elect, to act in their interests; and thus, their trust in democracy as a concept.

As with DPGs, DPI operates under an open paradigm governed by frameworks built on transparency and participatory governance (Alonso et al., 2023, p. 8). DPI comprises the "networks, systems or platforms that allow programmatic and secure access to the underlying data and business logic [of DPGs] through [APIs]" (Alonso et al., 2023, p. 8). DPI is "public" if its operator provides equal access to the relevant services to all users, and if its underlying standards and platforms are publicly available, making the subsequent enjoyment of these services by users non-rivalrous (Alonso et al., 2023, p. 8). This is combined with the positive externalities for

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

populations where the DPI is deployed in an open, interoperable manner, which also points to the nature of DPI as providing public goods (Alonso et al., 2023, pp. 8–9). It is the interoperability of DPI (such as payments services with identity verification services) that enables these externalities to be "foundational and cross-cutting" at the public policy and operational levels (Desai et al., 2023, paras. 6–10). Indeed, DPI reaches across sectoral and policy siloes "to create population scale digital ecosystems that promote inclusive development," including the acceleration of progress toward achieving the 2030 Agenda for Sustainable Development and Sustainable Development Goals (European Union & Government of India, 2023, p. 2; see also G20 Digital Economy Ministers, 2023, para. 7). Therefore, just like the DPGs that underpin DPI, it is the "foundational infrastructure" for a democracy and goes to the ability of its people to choose their own destiny (Alonso et al., 2023, p. 8). DPI enables the efficient, convenient, and transparent delivery of a range of essential services and provides all stakeholders with a platform to innovate on top of the DPI itself, facilitating further economic development (Alonso et al, 2023, p. 12). In this vein, the cyber and operational resilience of DPI Backbones are critical to the resilience of the democracy where DPI is deployed. Much like how protecting CNI assets has been termed a "sovereign necessity" in light of the criticality of the essential services these assets provide to the national security and social stability of the jurisdiction where these assets are deployed (Parliamentary Joint Committee on Intelligence and Security, 2022, p. 6), so is protecting DPI Backbones from a range of threats, especially in the cyber domain, vital to the resilience of the democracy where DPI is deployed.

In the same vein, India's DPI, like the India Stack that India's DPI is built with, is the "foundational infrastructure" for Indian democracy, given that the operational resilience of its DPI Backbones enables Indians to participate in their society and economy in the manner in which they collectively see fit (Alonso et al., 2023, p. 8). India's DPI and DPI Backbones go to India's digital sovereignty, the ability of the government elected by the Indian people to make decisions affecting their participation in the burgeoning Indian digital economy, rather than that of (overseas) malicious cyber actors looking to undermine their confidence in their democratic system of government (Gajbhiye et al., 2022; Gawen et al., 2021, as cited in OECD, 2021, p. 257). As per Figure 11.1, if the Indian government takes steps to ensure the cyber resilience of Indian DPI Backbones (CNI assets), it implements the UNGA-approved cyber norms, promotes economic development and growth, Indians' human rights, including their democratic rights, and thus their trust that democracy truly delivers for them.

WHAT ARE THE INDIA STACK AND INDIA'S DPI?

The India Stack can be defined as follows:

> India Stack is the moniker for a set of open APIs [Application Programming Interfaces] and digital public goods that aim to unlock the economic primitives

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

> of identity, data, and payments at population scale . . . [T]his project was conceptualized and first implemented in India, where its rapid adoption by billions of individuals and businesses has helped promote financial and social inclusion and positioned the country for the Internet Age. (iSPIRT, 2021, para. 1)

Therefore, the India Stack comprises the DPGs that enable the provision of digitally native essential services by India's DPI, the platforms that are built with the India Stack. The India Stack has three layers (Alonso et al., 2023, pp. 3, 10, 20, 22; D'Silva et al., 2019, p. 8):

- identity, which includes Aadhaar (a "12-digital unique identification number that is linked to biometric [identifiers]"), eKYC (Electronic Know Your Customer, that is, identity authentication using Aadhaar), eSign (legally binding digital signatures that are linked with the signatories' respective Aadhaar numbers), GSTN (Goods and Services Tax Network, that is, 15-digit identifiers for businesses registered under the federal goods and services tax regime) and Udyam (a framework for Indian Micro, Small, and Medium Enterprises);
- payments, which include the Unified Payments Interface ('UPI', fast payments rails), Aadhaar-Enabled Payment System (enabling transitions between bank accounts authenticated by the parties' Aadhaar identities), Aadhaar Payment Bridge (digitally transferring government benefits and subsidies to the Aadhaar-linked bank accounts of payees) and Bharat Bill Payment System (a platform through which citizens can pay utility, telephone, and other types of bills); and
- data, which includes DigiLocker (a credential and document management platform for Aadhaar holders) and Account Aggregator (a consent-based data portability framework for Indians' financial information that is handled by federally regulated financial institutions).

This is an extensive catalog of services that are delivered by Indian public sector entities via India's DPI, enabled by the India Stack. The scope of these services speaks to the importance of the India Stack and thus India's DPI to the ability of hundreds of millions of Indians to participate fully in social and economic activities. Some key examples of these services and platforms are Aadhaar (digital identity), the UPI (digital payments), the Account Aggregator Framework (open banking), and DigiLocker (management of government-issued documents and credentials) (Alonso et al., 2023, pp. 10, 20, 22).

One should also note the additional delivery mechanisms for services that India's DPI comprises, including the following:

- Open Network for Digital Commerce (ONDC), a set of open protocols which seeks to democratize e-commerce and replace a "platform-centric" model with a "transaction-centric" one where buyers and sellers can

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

find each other across e-commerce applications that are hosted on the ONDC network and built using those protocols (Gupta, 2022, paras. 28–29; Open Network for Digital Commerce, 2022, pp. 10, 13);

- Direct Benefit Transfer (DBT) mechanism for transferring funds and other benefits under 312 Indian social welfare programs run by fifty-three government departments directly to the bank accounts of beneficiaries (over half of which are linked with their Aadhaar numbers), and which is part of India's Public Financial Management System (PFMS), itself integrated with over 600 banks for verification of bank accounts and with the National Payments Corporation of India (NCPI) for verification of Aadhaar-linked bank accounts (Alonso et al., 2023, p. 8; Government of India, 2023a; Ministry of Finance, 2023, p. 212). The DBT is fundamentally enabled by the "JAM Trinity," that is: the opening of over 530 million bank accounts (as of late August 2024) for formerly unbanked Indians under the "Pradhan Mantri Jan Dhan Yojana" program; Aadhaar, the means by which the identity of most DBT beneficiaries is verified; and the sheer penetration of mobile telephony in India, namely, over 960 million phones that enable phone and/or online banking (Alonso et al., 2023, pp. 15–16; Department of Financial Services, 2023; Ministry of Finance, 2023, pp. 30, 156; MyGovIndia, 2023; Modi, 2024);
- COVID Vaccine Intelligence Network (CoWIN), which was developed as an extension of India's electronic Vaccine Intelligence Network and is a cloud-based solution that ran India's COVID-19 vaccination program (Ministry of Finance, 2023, p. 198). This served all stakeholders, be it vaccine recipients (booking appointments and receiving vaccination certificates), vaccinators, or logistics providers (such as through real-time visibility into the vaccine supply chain at the national, state, and even district levels) (Ministry of Finance, 2023, p. 198).

To understand the sheer scale of India's DPI, the following statistics and developments are instructive:

- India's success with the JAM Trinity in advancing financial inclusion is such that, had the country not used DPI solutions, it was estimated that India would have taken forty-seven years to open bank accounts for over 80 percent of Indian adults; much longer than the nine years taken to lift it to that level from 25 percent in 2008 (World Bank Group, 2023, p. 3, citing D'Silva et al., 2019, p. 4).
- In the case of the UPI:
  - In 2022, India processed the most real-time digital payments in the world, the number growing over 76 percent year-on-year in 2021–2022 and the country representing over 46 percent of all the world's real-time digital payments in 2022 (ACI Worldwide, 2023, pp. 5–6). This

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

has been complemented by the shrinking of the informal economy in India, estimated in 2021 to represent 15–20 percent of India's gross domestic product (GDP), down from 52 percent in the fiscal year 2018 (Ghosh, 2021, pp. 1–2).
    - The number of UPI transactions grew in fiscal year 2023–2024 by a record 57 percent to a record 131 billion (Jacob, 2024, paras. 1–3).
    - As a signal of the value of the UPI as a digital payments paradigm, Google even presented the UPI to the U.S. Treasury Department as an example of how to deploy an open standards-based payments network (Wadhwa, Amla, & Salkever, 2022, paras. 2, 9).
- As of November 2022, there had been over 1.35 billion unique Aadhaar numbers generated; 8.6 billion identity authentications done with Aadhaar; over 1.3 billion eKYC checks done; 754 million bank accounts linked with Aadhaar; and over 1.549 billion transactions done through payment systems simply reliant on counterparties' Aadhaar numbers to identify them (Ministry of Finance, 2023, pp. 155–156).
- Between 2013 and January 2023, the DBT was used to transfer over 3.2 trillion dollars' worth of social security benefits directly to the bank accounts of hundreds of millions of Indians (Ministry of Finance, 2023. pp. 212–213). This was alongside the PFMS transferring COVID relief payments to around 500 million Indians during the pandemic (Alonso et al., 2023, p. 18). Separately, a major benefit of the DBT, enabled by welfare recipients' bank accounts being linked to citizens' Aadhaar numbers, is the substantial reduction in monies being paid to phantom beneficiaries. The Indian government has estimated that it has saved over Rs 2.73 trillion between 2015 and 2022 by plugging these leakages (Choudhary & Singh, 2023, para. 3).
- As at December 31, 2022, twenty-three Indian banks had joined the Account Aggregator framework, enabling Indians, holding 1.1 billion bank accounts collectively, to share their banking data with eligible financial institutions through this open banking framework. Already, 3.3 million Indians have linked their accounts to the framework and 3.28 million of them have shared their data under it (Ministry of Finance, 2023, pp. 308–309). In June 2023, citizens had cumulatively raised 13.46 million consents (representing a monthly growth of over a quarter) while 2.9 million new consents were fulfilled in the same month (World Bank Group, 2023, p. 12).
- The ONDC platform, which went live in September 2022, has expanded to pilot programs in over 180 cities and saw over 5,000 orders daily in the retail category of goods and services (mostly food and beverages) as at April 2023 (Choudhury, 2023, para. 5). This constituted a twenty-five-fold growth in the period March–April 2023 (Choudhury, 2023, para. 1).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

- CoWIN was the backbone of India's COVID-19 vaccination program, the world's largest, and critical to the distribution, administration, and tracking of over 2.2 billion doses of vaccines given to 1.04 billion Indians (847 million of whom were identified by their Aadhaar numbers) between January 2021 and September 2022 (Ministry of Finance, 2023, p. 198; World Health Organization, 2021).

These factors suggest the criticality of DPI, built with the India Stack, to the ability of the citizens of India, the world's largest democracy, to participate fully in their society and economy (Guterres, 2022, para. 10). This is reinforced by the sheer quantum of citizens served by India's DPI and the vitality of the services it provides – from digital identity to payments, data portability, social welfare, and vaccination – to their collective ability to live their lives as they see fit. Given that several of these services are operated by the public sector, India's DPI is vital to the ability of Indian citizens to shape their collective destiny via the government they elect – the very essence of democracy – and have faith in that system of government as a means of driving their economic development, growth, and promotion of their human rights, including their democratic rights, as flagged in the opening paragraphs of this chapter and in Figure 11.1.

The importance of India's DPI and the India Stack to India's ability to drive the economic development of its people, and thus their confidence in its democratic institutions as enablers of this development (given in Figure 11.1), is also underlined by the praise these have received from senior officials in governments and international organizations. The President of the UNGA referred to India as "leading in the field of digital public infrastructure" with the world having "much to learn from [India]" (Ministry of External Affairs, 2022a). The Secretary-General of the United Nations labeled India's DPI as "world-class" and implementing a "whole-of-society approach to development [which] combines old-fashioned community outreach with cutting-edge technology" (Observer Research Foundation, 2022). The German Ambassador to New Delhi referred to India's journey as a growing digital economy, including through the digital delivery of services, as an example for Germany to learn from (ANI, 2022c). The United States' then-Deputy National Security Advisor for Cyber and Emerging Technology praised Aadhaar as an enabler of "critical services" for Indian citizens – "often to sets of a population who were illiterate so that they could get their rations, they could get their access" – and for its "thoughtful" approach to preserving the privacy of citizens through data minimization (Inglis & Neuberger, 2021, pp. 16–17). The Deputy Director of the International Monetary Fund's Fiscal Affairs Department, termed the DBT as a "logistical marvel, seeking to help people at low-income levels, reaching hundreds of millions of people" (ANI, 2022b).

Industry and civil society actors have also praised India's DPI, enabled by the India Stack, as an example for the world. The Chief Technology Officer and a

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Senior Vice-President of PayPal at the time, Sri Shivananda, spoke of the uniqueness of India's achievement:

> There is no technical stack in the world with a country's name as a prefix. What the Indian government and regulators have done together with the common national identity through a digital system and a common national API for payments, is nothing but brilliant. India is one of the first countries that has a platform first approach, with the platform being secure, robust and reliable. It is a role model for many other countries to follow. (Via & Sanghi, 2021, para. 104)

Philanthropist and technology luminary, Bill Gates, was similarly effusive in his remarks:

> No country has built [a] more comprehensive platform than India ... Because of the pioneering investment including creating the basic Aadhaar identity, India was in the lead in getting out (relief) payments ... during the pandemic ... We would like to see all countries, particularly developing countries, adopt these things. (PTI, 2023, paras. 3, 5, 10)

These words of praise for India's DPI, built atop the India Stack, underline the criticality of both to the ability of India's people to independently run their affairs through the government they elected to further their digital sovereignty. It also reinforces the nature of India's DPI as a guarantor of their economic development and thus, ultimately, their trust and confidence in the democratic system of government to advance their interests through tools such as DPI and the India Stack, given in Figure 11.1. Therefore, (praise for) the substantial track record of DPI stresses its importance as a pillar of the resilience of India's increasingly digital democracy (explored earlier).

This makes India's prosecution of systemic cyber risks that its DPI, especially its DPI Backbones, face via critical software all the more important, which the chapter now explores.

PROSECUTING SYSTEMIC CYBER RISKS FROM CRITICAL SOFTWARE

Given that India's DPI, like the India Stack itself, is digitally native, the security of the software that is deployed on DPI Backbones is paramount for its operational resilience. The weaponization of vulnerabilities in that software by malicious cyber actors – be they criminals, hacktivists, or state(-affiliated) actors – ultimately weaponizes the "digital dependence" of over a billion Indians on these CNI assets to verify their identity, as well as make and receive digital payments, among other things (OECD Council, 2022, Preamble para. 6). These are systemic cyber risks for India as the world's largest democracy (Guterres, 2022, para. 10).

Governments generally recognize the need to prosecute such risks. Under India's presidency, the G20 Leaders (2023, para. 57) recognized the increasing importance of a "secure digital economy" for all stakeholders. The G20 Digital Economy

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Ministers (2023) repeatedly used the word "secure" to describe the digital economy and technologies, including DPI, that their governments seek to foster. The Ministers "reaffirm[ed] the importance of security in the digital economy as a key enabling factor" (G20 Digital Economy Ministers, 2023, para. 5). Given the vitality of secure digital technologies to how citizens of democracies conduct their lives, as flagged above, software security goes directly to how they collectively shape their destinies and, flowing from that, their confidence in democratic institutions as protectors of their democratic rights such as freedom, assembly, expression, privacy, and association in the increasingly digital societies they inhabit.

Given that most of the services provided by India's DPI are provided by the public sector (Alonso et al., 2023, p. 10; D'Silva et al., 2019, p. 8), the weaponization of vulnerabilities affecting the underlying DPI Backbones has the very real potential to undermine Indians' confidence in their democratically elected government to protect their collective ability to shape their own destiny, and thus their confidence in democracy itself. This echoes the implications of the cyber-enabled disruption of the functioning of physical CNI assets for social and economic stability that were flagged in the earlier sections of this chapter, and thus the relationships visualized by Figure 11.1 between CNI (including DPI) cyber resilience, economic development, growth, as well as the trust and confidence of citizens generally in democratic institutions, and the implementation of the UNGA-approved cyber norms.

India's G20 Sherpa, Amitabh Kant, pointed to how "Cybersecurity is paramount and will be the key to the future," including in managing "the whole DPI framework" (Digital India, 2023, para. 7). In particular, India needs to be mindful of the systemic cyber risks to its DPI and the India Stack via critical software running on its DPI Backbones. This is because critical software is identified in terms of performing functions critical to the cyber resilience of the computer that the software is running on (National Institute of Standards and Technology, 2021, p. 10). NIST (2021, pp. 1–3) defines critical software:

> as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:
> - is designed to run with elevated privilege or manage privileges;
> - has direct or privileged access to networking or computing resources;
> - is designed to control access to data or operational technology;
> - performs a function critical to trust [that is, the cyber resilience of the device running the software]; or,
> - operates outside of normal trust boundaries with privileged access.

NIST specifies categories of such software, including access management, device security, operating systems, web browsers, remote access and scanning, and operational and network monitoring (National Institute of Standards and Technology, 2021, pp. 3–8). Given these factors, critical software represents an attractive attack vector for malicious cyber actors to leverage in targeting DPI Backbones.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

In this context, India must take steps to appropriately incentivize the vendors of critical software running on DPI Backbones to invest in the security of their software development life cycles (SDLCs), that is, the "formal or informal methodology for designing, creating, and maintaining software" (Souppaya, Scarfone, & Dodson, 2022, p. 1).

Each SDLC can be viewed as being vulnerable to eight categories of threat vector that malicious cyber actors can exploit in order to, for instance, insert malware and thus compromise the, in this case, critical software produced by that SDLC (SLSA, 2023). These threat vectors in each SDLC are multiplied across each developer and vendor populating the software supply chain(s) for that critical software product. In general, a software supply chain comprises the "entire sequence of events that impacts software from the point of origin where it is designed and developed, to the point of end-use," and each event can be a means of ultimately targeting the end-user of a piece of software (U.S. Department of Commerce & U.S. Department of Homeland Security, 2022, p. 34). If successful, that targeting is defined as a software supply chain attack, that is, the "compromise of software code … at any phase of the supply chain to infect an unsuspecting [end-user]" (Clancy et al., 2021, p. 1; NTIA Multistakeholder Process on Software Component Transparency Framing Working Group, 2021, p. 24).

Given that critical software can be weaponized to directly compromise the cyber resilience of the computer running it, it becomes all the more crucial for India to take steps to incentivize the vendors of critical software deployed on DPI Backbones – not just ensure the security of their own SDLCs but also manage risks from their software supply chains. If they do not do so, they open up India's DPI Backbones to software supply chain attacks and thus make the delivery of a range of essential services to hundreds of millions of Indians by Indian DPI ever more prone to disruption.

The imperative for India to drive critical software vendors to perform software supply chain risk management (SCRM) in particular is enlivened by the increasingly hostile threat environment for software supply chains. Herr et al. (2020, p. 8), for example, have compiled a list of eighty-two software supply chain attacks, involving different elements of software supply chains, from 2010 to 2020. Similarly, Australian agencies have warned that threat actors are "increasingly looking to compromise multiple victims across a range of sectors via a single entry point" and targeting "products commonly found in ICT supply chains" (Australian Cyber Security Centre, 2022, p. 65; Australian Signals Directorate, 2023, p. 53). The Cybersecurity and Infrastructure Security Agency (2021b, p. 5) similarly pointed to the threat to software supply chains from highly sophisticated threat actors. The Agence Nationale de la Sécurité des Systèmes d'Information (2023, p. 30) referred to the targeting of software supply chains as "[continuing] to pose a systemic risk." The Quad, a diplomatic grouping of four democracies (Japan, Australia, India and the United States), signed joint principles for software security in May 2023 that began

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

with an explicit recognition of "the security risks posed by lack of adequate controls to prevent tampering with the software supply chain by adversarial and non-adversarial threats" (Commonwealth of Australia et al., 2023, p. 2). Indeed, the severity of the threat landscape for software supply chains is underlined by, apart from the relative recency of these warnings from governments, the frankness of tone in these quotes (Nayyar, 2023, p. 19).

The impetus for India to act with respect to combating critical software risk to its DPI Backbones, including the risk via the software supply chains of critical software vendors, is bolstered by the past few decades of instances where CNI assets around the world have been successfully targeted via critical software running on their systems. The United States and Israel exploited vulnerabilities in software controlling Iranian uranium centrifuges (in the Iranian defense industrial base) to sabotage them (Perlroth, 2021, pp. 122–130). The Russian state manipulated supervisory control and data acquisition (SCADA) software used by three Ukrainian electricity utilities to open circuit breakers remotely, taking dozens of substations offline and causing blackouts that affected hundreds of thousands of citizens in 2015 (Cybersecurity & Infrastructure Security Agency, 2021a, paras. 2, 8–9; Zetter, 2016, pp. 2–3, 8, 19). Additionally, the Russian state gained access to the KA-SAT satellite internet network via, in part, a misconfigured virtual private network appliance to disrupt it at the start of the war in Ukraine (Blinken, 2022, para. 2; Viasat, Inc., 2022, para. 10). The NotPetya and WannaCry attacks both exploited vulnerabilities in the Windows operating system to cripple the Ukrainian government's ability to function and the country's CNI, and European and British CNI assets, respectively (Greenberg, 2018, paras. 28, 34; 2019, p. 1; Perlroth, 2021, pp. 389, 402; Romine, 2017, p. 3; Smart, 2018, pp. 8, 10; Trautman and Ormerod, 2019, p. 528). Such attacks are possible with respect to India's DPI Backbones, part of India's CNI, given that they are entirely dependent on software to function. These attacks would also occur within the context of India being the second-most targeted of all countries by malicious cyber actors in 2021 and 2022, with attacks reported to have increased by 24.3 percent in 2022 (CloudSEK, 2023, pp. 8–9).

India has made some progress on the world stage in tackling software security risks, which includes tackling critical software security risks. As G20 President, it forged consensus among the world's largest economies on the need to uplift software security. The *G20 High-Level Principles to Support Businesses in Building Safety, Security, Resilience, and Trust in the Digital Economy* (*G20 High-Level Principles*), endorsed by the G20 Leaders, include principles regarding "Security and Trust" (G20 Digital Economy Ministers, 2023, Annexure 2, para. 1; G20 Leaders, 2023, para. 57.i). As part of "develop[ing] a human-centric culture of security and trust in the digital economy," these principles seek to promote a "security by design" approach in relation to digital technologies (G20 Digital Economy Ministers, 2023, Annexure 2, para. 1.c). Specifically for DPI, developed under India's presidency and endorsed by the G20 Leaders, the G20 Framework for Systems of Digital

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Public Infrastructure (G20 DPI Framework) calls for stakeholders to incorporate "security features within the core design" (G20 Digital Economy Ministers, 2023, Annexure 1, para. 6.e; G20 Leaders, 2023, para. 56.i). Though these are political commitments with respect to building security into the digital economy and DPI, they are welcome. Fulfilling them would require the G20 countries – including the world's largest software markets, and developer and innovation centers (see, e.g., U.S. Department of Commerce & U.S. Department of Homeland Security, 2022, p. 35) – to incentivize software developers and vendors in their jurisdictions to harden their SDLCs and perform robust software SCRM, having positive externalities for cyber resilience generally, not just that of India's DPI Backbones. Given the relationships between DPI, human rights promotion, trust, and confidence in democratic institutions described by Figure 11.1, these positive externalities ultimately reinforce the resilience of democratic institutions and drive the implementation of UNGA-approved cyber norms.

Alongside work to incentivize the vendors of critical software running on DPI Backbones to invest in the security of their SDLCs, including to perform robust software SCRM, India must closely scrutinize cyber risk invited by the use of OSS. In general, this is because of the sheer pervasiveness of OSS in modern computing (European Commission, 2020, p. 2). It has been estimated that OSS comprises dependencies for 97 percent of all software (Scott et al., 2023, p. 2). The India Stack itself uses OSS (Alonso et al., 2023, p. 8). If one looks at critical software, per a 2020 assessment by the U.S. Department of Commerce of 389 American technology companies that produce "security-related products," OSS was "frequently" incorporated in software running tools such as firewalls, logging programs, network management devices and (62 percent of) SCADA systems (National Institute of Standards and Technology, 2021, pp. 5–7; U.S. Department of Commerce & U.S. Department of Homeland Security, 2022, pp. 36–37). Furthermore, attack surfaces are multiplied by the sheer number of dependencies of commercial software's OSS dependencies themselves; meaning that vendors using OSS in their products are inheriting risks transmitted through multiple tiers of OSS developers and maintainers, (potentially) resulting in those OSS dependencies being "deeply buried" within their products (Scott et al., 2023, pp. 10–11). The sheer size of the resultant attack surface for critical software vendors that incorporate OSS into their products, therefore, should give urgency to scrutiny by India of OSS-borne risk to critical software and thus DPI Backbones.

Indeed, that attack surface is evident in the huge number of vulnerabilities in the OSS ecosystem and, therefore, in the dependencies of commercial software. Synopsys (2023, p. 7) found that 84 percent of 1,730 commercial codebases that it analyzed "contained at least one known open-source vulnerability" in 2022, a 4 percent increase on the equivalent figure yielded from analysis of over 2,409 codebases in 2021. Malicious cyber actors have seized on this, with Sonatype (2023, p. 4) finding that software supply chain attacks increased 633 percent

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

year-on-year in 2022, marking a 742 percent average annual increase over the three years to 2023. An egregious example of malicious cyber actors seeking to exploit vulnerabilities in OSS is the exploitation of a critical vulnerability in the Log4j package, which was first seen in December 2021 (Silvers et al., 2022, p. 3). Merely five days after the vulnerability was disclosed, threat actors were observed trying to exploit it 400 times per second (Prince, 2021, as cited in Silvers et al., 2022, p. 4). Such was the severity of the vulnerability, including because of its being a(n enigmatic) transitive dependency for an innumerable amount of OSS and commercial software, that it triggered a multinational response by public and private sectors alike, scrambling to "identify and mitigate hundreds of millions of potentially affected devices" (Silvers et al., 2022, pp. 5–9, 11). The Director of the Cybersecurity and Infrastructure Security Agency (CISA) went as far as terming the vulnerability as "one of the most serious I've seen in my entire career, if not the most serious" (Starks, 2021, para. 1).

Therefore, the immense number of vulnerabilities in OSS ecosystems that are inherited by commercial software products, including critical software products that are deployed on DPI Backbones, as well as the greater intent of malicious cyber actors to exploit those vulnerabilities as part of software supply chain attacks makes it all the more vital for India to pay greater attention to the OSS risk to its DPI and the India Stack. While India should thus be applauded for the G20, under its presidency, recognizing "the importance of promoting open-source software" to enable (cross-border) DPI interoperability, India must not lose sight of the need to drive work to uplift the security of OSS, in line with the G20 calling for security to be built into the digital economy and DPI, as flagged earlier (G20 Digital Economy Ministers, 2023, para. 9). Its resilience as a democracy, the world's largest, is at stake, given the criticality of its DPI generally (as CNI) to Indians' trust in democratic institutions and the democratic mode of government as the ideal means to advance their economic development, growth and human rights, including their democratic rights, per Figure 11.1 (Guterres, 2022, para. 10). Similarly, critical software- and OSS-borne risks to India's DPI Backbones threaten its efforts to implement the UNGA-approved cyber norms outlined in the opening paragraphs of this chapter.

These are the sort of issues that India must especially be mindful when it looks to share its open standards-based approach to DPI through the India Stack, particularly with democratic partners in the Global South. It is imperative that India helps fellow democracies deploy DPI in a cyber-resilient manner that makes it harder for malicious actors to weaponize their technological dependencies and undermine citizens' trust and confidence in their democratic modes of government, as detailed in the next section.

TAKING INDIA'S APPROACH TO DPI AND THE INDIA STACK TO THE WORLD

Given the success of India's DPI in advancing India's economic development (as detailed in the introduction to the India Stack and Indian DPI), India's exporting its

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

approach can enable other countries, especially democracies in the Global South, to benefit like it has. These benefits include the strengthening of the trust and confidence of their citizens in democracy as a system of government to drive economic development and growth, per the relationships described in Figure 11.1. This will be reinforced by advice from India on how to deploy DPI in a cyber-resilient manner, informed by the G20 *High-Level Principles* and *G20 DPI Framework* enacted under India's G20 presidency, and especially if India implements the recommendations in the immediately preceding section of this chapter ("Recommendations") on prosecuting systemic cyber risks from critical software. India, the world's largest democracy, can thus enable its fellow democracies, especially among developing countries, to implement the UNGA-approved cyber norms, per Figure 11.1, and better ensure their national (cyber) resilience amid a deteriorating threat landscape detailed in the previous section of this chapter (Guterres, 2022, para. 10).

India's experience as G20 President holds it in good stead. DPI was among its core priorities, including the facilitation of more sharing of expertise on DPI (Ministry of External Affairs, 2022c, paras. 35–37). India followed this up by forging "groundbreaking" international consensus on DPI (Gates, 2023). It successfully pushed for the creation of the *G20 DPI Framework*, endorsed by the G20 Leaders (as mentioned in the previous section of this chapter) who also "recognize[d] that safe, secure, trusted, accountable and inclusive digital public infrastructure, respectful of human rights, personal data, privacy and intellectual property rights can foster resilience, and enable service delivery and innovation" (G20 Leaders, 2023, para. 56). Indeed, the Indian G20 presidency produced the first "multilaterally agreed language and detail on DPI" (Chaudhuri, 2023, para. 14). With governments and donors around the world seeking to invest in DPI deployment (versus little prior multilateral work on DPI), the championing of DPI by the G20 in 2023 was pathbreaking, a "centerpiece of India's G20 presidency," and has helped forge India's "digital revolution" as a source of soft power (Chaudhuri, 2023, paras. 11, 16; Mehta, 2023, para. 2). India is indeed poised to share its approach, particularly with democratic developing countries for them to, as the Indian prime minister put it, "unlock the power of inclusive growth" (Modi, 2023, para. 21), which would enable them to better promote their democratic resilience, given in Figure 11.1.

Indeed, Indian efforts will be aided by New Delhi's general reputation as a trusted development partner, particularly for the Global South (Banerji, 2023).

Firstly, its G20 presidency was and wider foreign policy is animated by "Vasudhaiva Kutumbakam," a Sanskrit phrase from the *ślokas* [VI.71–73] of the ancient Hindu text, the *Maha Upanishad*, which roughly translates to "the world is one family" (Ministry of External Affairs, 2022b, para. 21; Vivekananda International Foundation, 2019, p. 7). One of the priorities of its G20 presidency was "accelerated, inclusive and resilient growth" (Ministry of External Affairs, 2022b, para. 32).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Secondly, as part of its prioritization of inclusive growth and development, India devoted special attention to uplifting that of the Global South and its role in international governance. India hosted two virtual "Voice of the Global South Summits" where countries from the Global South provided their views on matters such as economic development and DPGs, matters that go directly to the promotion of human rights and democratic resilience, given in Figure 11.1 (Government of India, 2023b; Ministry of External Affairs, 2023a, paras. 1–2, 9–17). As G20 President, India placed the "Global South squarely at the center of the global governance agenda," having successfully proposed the permanent G20 membership of the African Union, which it considers "the most satisfying outcome" of its Presidency (Jaishankar, 2023a, para. 5; Pant, 2023, paras. 1–2). As the Indian External Affairs Minister put it, India pushed for solutions to global challenges from the Global South itself as G20 President (Jaishankar, 2023a, para. 4). This is combined with the Indian prime minister "firmly" believing that "that the success of our G20 presidency is the success of the Global South" (Jaishankar, 2023b, para. 6).

Thirdly, India has an excellent reputation for public goods delivery, for instance, as a trusted health care partner. Under its COVID-19 vaccine diplomacy initiative, "Vaccine Maitri," it gifted over 14.85 million doses of locally manufactured COVID-19 vaccines to fifty countries and provided close to 51.52 million doses to forty-eight countries in the Global South under the COVAX facility until November 30, 2022 (Ministry of External Affairs, 2023b, p. 309). Jamaica actually received its first batch of COVID-19 vaccines from India, with the Jamaican Foreign Minister saying that, "From the very onset, India was a reliable partner whose assistance was critical to our pandemic response" (ANI, 2022a, paras. 2–3). Similarly, India co-led with South Africa the international push for a waiver of intellectual property rights for COVID-19 vaccines and is now working to extend the waiver to drugs used to treat the disease (Kumar, 2021, para. 1; The Pharma Letter, 2023).

These factors add to the attractiveness of India's offering in terms of DPI and the India Stack, especially for fellow democracies in the Global South. The goodwill India thus enjoys will be reinforced by how it is not looking to weaponize the India Stack. Rather, India seeks to empower other countries to use an open standards-based approach to the digital delivery of essential services, which prioritizes cyber resilience, per the *G20 High-Level Principles* and *G20 DPI Framework* enacted under India's G20 presidency and if India implements the Recommendations. As seen with CoWIN (Sansad TV, 2023), recipient countries are free to customize and build with the India Stack and India's approach as they see fit, "no strings attached," to quote the head and co-founder of the Digital India Foundation (Sansad TV, 2023). With the international community confident in DPI being "a critical accelerator" of the achievement of the Sustainable Development Goals (Gates, 2023), the Indian approach to DPI will enable recipient democracies, especially in the Global South, to promote their citizens' faith in democracy itself as a means of driving their economic development, growth, and thus preservation of

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

their human rights, combined with implementing UNGA-approved cyber norms, as per Figure 11.1.

This is in stark contrast with China's Belt and Road Initiative and Digital Silk Road that constitute the blatant weaponization of Chinese technology vendors to influence and/or interfere in the affairs of recipient countries (Lewis, 2023, p. 7). Instead, India, the world's largest democracy, seeks to help these countries build their digital sovereignty and strengthen their overall democratic resilience through robust, cyber-resilient DPI and DPI Backbones in line with their needs, rather than "weaponise their interdependence" with the India Stack (Guterres, 2022, para. 10; Narlikar, 2021, pp. 289–290). This echoes how India characterizes its development cooperation with the Global South as "demand driven, outcome oriented, transparent and sustainable" (Jaishankar, 2023b, para. 9).

Further differentiating India's efforts from China's on digital economy diplomacy is its bilateral cooperation with leading democratic partners on DPI projects (in the Global South), such as the European Union, United States, France, Germany and Japan (Choudhury, 2023, paras. 20, 28; European Union & Government of India, 2023, p. 2; Government of India & Government of France, 2023, para. I.6.1.7; Ministry of External Affairs, 2023c, para. 3; The White House & Government of India, 2023; The White House & Government of India, 2024 para. 39, para. 37; Government of India & Republic of Germany, 2024, para. 32). India and the United States have incorporated DPI into their bilateral Initiative on Critical and Emerging Technologies (Government of India, 2023c, para. 5). Both countries also cooperate on DPI with the Republic of Korea through a "trilateral technology dialogue," looking to "expand cooperation on . . . [among other things,] delivering technology solutions for the broader Indo-Pacific region" (U.S. Mission Korea, 2024, paras. 1–2). Furthermore, the world's largest democracy and France's championing of DPI as an enabler for "open, free, democratic and inclusive digital economies and digital societies" (Government of India & Government of France, 2023, para. I.6.1.7; Guterres, 2022, para. 10) will help project India as a trusted, democratic technology partner for fellow developing country democracies that look to bolster their citizens' faith in democracy and democratic institutions as drivers of economic development and uphold UNGA-approved cyber norms by developing and deploying robust, cyber-resilient DPI, per Figure 11.1. India's reputation as such is key to the success of its work to share its DPI expertise because "trust and transparency" are valuable commodities in foreign policy, especially in digital economy diplomacy, as defined by the Indian External Affairs Minister (Ministry of External Affairs, 2022b).

Indeed, amid technological contestation and balkanization, those very commodities will underwrite India's efforts to lead "an international architecture of collaboration" on DPI (Carnegie India, 2022; Ministry of External Affairs, 2022b). India has established the Global Digital Public Infrastructure Repository (GDPIR, welcomed by the G20 Leaders), a virtual library for DPI that countries and organizations have deployed at scale (at the time of writing, the GDPIR features over fifty projects from

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

sixteen countries) (G20 Leaders, 2023, para. 56.ii; Ministry of Electronics and Information Technology, 2023, para. 3; https://dpi.global). India has created the One Future Alliance (OFA), a voluntary capacity building initiative for DPI targeted at low- and middle-income countries (LMICs) (G20 Leaders, 2023, para. 56.iii). India's credibility is also enhanced by its forming a Social Impact Fund (SIF), having pledged 25 million dollars to this government-led, multistakeholder capacity-building and financing initiative for DPI deployment in the Global South (Ministry of Electronics and Information Technology, 2023, para. 4).

The GDPIR, OFA, and SIF can underpin an India-anchored international architecture for DPI. The GDPIR provides a knowledge base for DPI. The OFA can structure DPI internationalization (Choudhury, 2023, para. 26), financially backed by the Global South-focused SIF. In potentially leading the OFA and SIF and already hosting the GDPIR, India can build on its credentials as a trusted hub for DPI expertise while working with its democratic partners, as mentioned earlier, and other stakeholders such as industry and academia to streamline DPI capacity-building efforts around the world and thus, at least indirectly, streamline the promotion of democracy as a sustainable means of driving economic development (Choudhury, 2023, para. 27; see Figure 11.1). India can also include the Global South in its DPI diplomacy by linking the OFA, GDPIR, and SIF with the DAKSHIN "global centre of excellence dedicated to [the Global South]," which the Indian prime minister launched in November 2023 (DD News, 2023, paras. 1–2). Such efforts would most likely implement the vision of the G20 Digital Economy Ministers (2023, para. 10) under the Indian presidency, which called for coordinated capacity building, technical assistance as well as "global multistakeholder approaches … for implementing robust, inclusive, human-centric, and sustainable DPI in LMICs."

India can weave its aforementioned bilateral cooperation with democratic partners on DPI – including through a U.S.–India Global Digital Development Partnership suggested by both countries in June 2023 – as well as its aforementioned trilateral cooperation with the United States and Republic of Korea into its multilateral DPI diplomacy via the OFA and SIF so that the latter initiatives receive further credibility from the backing of major democracies (The White House & Government of India, 2023, para. 39). An example of such crossover from bilateral or trilateral cooperation to multilateral cooperation is how, in January 2024, France "expressed its support to join [OFA]" in order to "further synergize global efforts on building DPI capacities" (Government of India & Government of France, 2024, para. 24). In terms of concrete multilateral cooperation, India itself has pledged $10 million to the World Health Organization's Global Initiative on Digital Health, which includes capacity building for countries in the Indo-Pacific region seeking to adopt India's approach to DPI to aid cancer diagnosis and treatment (Commonwealth of Australia, Government of India, Government of Japan, & United States Government, 2024a, para. 9).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Indeed, such cooperation would be aided by increased momentum for DPI cooperation at the multilateral (and multistakeholder) level more broadly since India's G20 presidency. The following are key examples of this momentum in 2024 alone:

- In September, the UNGA approved the *Global Digital Compact* (United Nations, General Assembly, 2024, Annex I), which recognized: DPGs and "Resilient, safe, inclusive and interoperable" DPI as "key drivers of inclusive digital transformation and innovation"; and the necessity for greater investment in their deployment (United Nations, General Assembly, 2024, Annex I, paras. 14–16). The UNGA even committed to, among other things, establish safeguards "for inclusive, responsible, safe, secure and user-centred [DPI]," and grow finance for DPGs and DPI development (particularly in developing countries) by 2030 (United Nations, General Assembly, 2024, Annex I, paras. 17(c), (e)).
- In October, the "Global DPI Summit 2024" featured representatives across stakeholder groups from over 100 countries (Global DPI Summit 2024, 2024, para. 1). In addition to highlighting "the extraordinary progress" in the rollout of DPI around the world, attendees called for greater collaboration in areas like ecosystem-building, "safeguards to ensure that DPI is people-centric, transparent, accountable, and fair of all users"; ensuring adequate "support for the widespread implementation of DPI"; and driving adoption of robust technical standards to drive better interoperability and security of DPI (Backbones) (Global DPI Summit 2024, 2024, paras. 2, 5–8, 11–12, 15–18).
- In November, India cosponsored the *Declaration on Digital Public Infrastructure, AI and Data for Governance* with Brazil (G20 President for 2024) and South Africa (G20 President for 2025), which was endorsed by several G20 governments (Government of India, Government of Brazil, & Government of South Africa, 2024).

Such momentum certainly helps India's cause as it seeks to lead international efforts to develop and adopt DPI. That world leaders, particularly through the UN, endorsed the value of DPGs and DPI as instruments of economic and digital development, and called for greater investment in their development and deployment is highly consequential. After all, consensus at the UN level not merely validates but also significantly builds upon the pioneering multilateral consensus engineered by New Delhi on DPI and DPGs as G20 President in 2023.

Furthermore, India's being a trusted DPI partner and its leadership in DPI development and deployment will be aided by its work through the Quad. In September 2024, the Quad released the *Quad Principles for Development and Deployment of Digital Public Infrastructure*, including inclusivity, security (such as by incorporating "security features into the core design to ensure . . . resilience") and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

"Governance for Public Benefit, Trust, and Transparency" (Commonwealth of Australia, Government of India, Government of Japan, & United States Government, 2024b, paras. 3.i, v, vii).

This is combined with the work of the Quad on uplifting software security, particularly through the *Joint Principles for Software Security* that it released in May 2023 and that seek to "promote and strengthen a culture where software security is by design and default" (Quad Senior Cyber Group, 2023, p. 2). These joint principles lay down "high-level secure software development practices" that echo the recommendations of NIST (Quad Senior Cyber Group, 2023, p. 2; Souppaya, Scarfone & Dodson, 2022, p. 4). Apart from committing to acquire software from vendors meeting these practices (thereby pledging to use their collective purchasing power to uplift software security), the Quad countries aim to "where necessary ... build policy frameworks" that "encourage" software developers and suppliers to follow said software development practices (Quad Senior Cyber Group, 2023, p. 2).

Given the fundamental dependence of any DPI and DPGs on secure software (as mentioned earlier), work by the Quad to uplift software security under these joint principles underpins the ability of India to implement the Recommendations at home and help build and deploy cyber-resilient DPI in other (Global South) democracies; thereby helping the latter boost the confidence of their citizens in democratic institutions as effective vehicles for their economic development, per Figure 11.1. This is particularly significant in light of the deteriorating threat landscape for software supply chains, as per the previous section of this chapter on prosecuting systemic cyber risks. Given that DPI Backbones are CNI assets (see the opening paragraphs of this chapter), India's work to uplift software security through the Quad would also help fellow democracies implement the UNGA-approved cyber norms, as well as deliver public goods for their people such as national cyber resilience and national security (Nayyar, 2023, pp. 28–30).

One should note that India has already taken several concrete steps to export its approach to DPI.

For example, it cooperates with a number of countries when it comes to internationalizing the UPI.

- As part of its engagement with over thirty countries, including Japan, Australia, and Saudi Arabia, the NPCI has connected the UPI with France's Lyra Network, as well as the Bhutanese, Mauritian, Singaporean, and Sri Lankan payments networks (Ministry of Commerce & Industry, 2022, para. 6; Rudra, 2023, para. 1; Sibal, 2022, 2023, paras. 1–3; Wadhwa, Amla, & Salkever, 2022, para. 2; Prime Minister's Office, 2023; Ministry of External Affairs, 2024a, para. 1; PIB India, 2024).
- The Reserve Bank of India cofounded Project Nexus, a multilateral program to link the national 'Fast Payments Systems' of India with

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Malaysia, Philippines, Singapore, and Thailand, in June 2024, and it is expected to be launched by 2026 (Pancholy, 2024, paras. 1–4).

- The Indian and Emirati governments have signed agreements on "cooperation in digital infrastructure projects" and on linking the UPI with the United Arab Emirates' (UAE's) AANI payments network, while UPI payments can already be made through the PhonePe payments app at Mashreq's NEOPAY Terminals in the UAE (Ministry of External Affairs, 2024b, para. 3; HT News Desk, 2024).
- Just in October 2024, the Maldivian president decided to establish "a consortium to introduce [the] UPI in the Maldives" (The President's Office, 2024, para. 3).

India's economic statecraft with respect to exporting the UPI also features the work of the NPCI International (the "international arm" of the NPCI) with a growing number of overseas partners.

- The body signed a memorandum of understanding (MoU) with Google Pay India to expand the acceptance of UPI payments outside India; export the approach to digital payments that the UPI represents; and "[ease] the process of remittances between countries" through use of the UPI's infrastructure (NPCI International, 2024a, paras. 2, 8).
- It signed an MoU with the major Greek bank, Eurobank, to create a "strategic alliance" for upgrading India–Greece payments flows and "streamlining remittances from Greece to India" using UPI technology (NPCI International, 2024b, paras. 1, 3).
- It partnered with the Bank of Namibia and Central Reserve Bank of Peru to help their respective countries develop and deploy UPI analogues (NPCI International, 2024c; NPCI International, 2024d).

If one moves from payments to health care, CoWIN's success as a component of India's DPI to fight the pandemic attracted so much international interest that India's virtual "CoWIN Global Conclave" was attended by representatives from 142 countries (Chandna, 2021; Ministry of Health and Family Welfare, 2021). By early February 2023, India had open-sourced CoWIN and shared it with over twenty-seven countries, enabling them to customize the platform as per their needs (Sansad TV, 2023).

When it comes to digital identity, the Philippines and Morocco became the first countries to adopt an Aadhaar-based digital identity system in March 2023 (Lele, 2023).

In terms of sharing India's approach to DPI more generally, there have been a number of such initiatives in train in the past few years alone.

- India signed MoUs with Armenia, Sierra Leone, Suriname, and Antigua and Barbuda on building DPI based on the India Stack (Kant & Sudke, 2023, para. 9).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

- Sri Lanka plans to tailor India's DPI approach to enable the "effective and efficient delivery of citizen-centric services" (Government of India & Government of Sri Lanka, 2023, para. 4.IV.e). This is in addition to both countries agreeing to establish a Joint Working Group on implementing DPI, including by adapting India's DigiLocker and Aadhaar for Sri Lanka (Government of India & Government of Sri Lanka, 2024, paras. 15. iii, v).
- Google India and the EkStep Foundation launched "DPI in a Box," an initiative providing countries with "a readily deployable model" of India's DPI, including Aadhaar (Google India Team, 2024, paras. 13–18).
- In September 2024, the Secretary of Papua New Guinea's (PNG's) Department of Information Communication Technology observed that PNG's bilateral cooperation with India informed the former's own projects on digital identity, payments, and building DPI ecosystems (ASPICanberra, 2024). The Secretary stressed the need for development partners more generally to see the value in (financing) DPI projects (ASPICanberra, 2024).
- India and the Maldives agreed to cooperate on DPI, including by enabling the Maldives to adopt an Aadhaar analogue (Government of India & Republic of Maldives, 2024, para. 4.IV.ii).

In light of factors such as India's expertise and experience in DPI development and deployment, its growing cooperation with international partners in a variety of contexts, and the strengthening multilateral and multistakeholder consensus on the need for greater investment in DPI around the world, the world looks to India to lead. Indeed, India is well-positioned to lead the way on DPI, particularly in advising fellow democracies (in the Global South) on how to develop and deploy cyber-resilient DPI solutions and thus implement the UNGA-approved cyber norms (see Figure 11.1). In doing so, India will not only help fellow democracies better assure their national (cyber) resilience amid a worsening risk landscape but also help them strengthen the faith of their own polities in democracy as a force multiplier for their own development, much like DPI itself.

CONCLUSION

This chapter began by defining democracy, including with reference to international law, as the right of a people to shape their collective destiny, as well as including specific human rights such as peaceful assembly, expression, and association. It pointed to the relationship between economic development, economic growth, and the promotion of human rights, including democratic rights. Threats to the ability of democratic institutions such as elected governments to drive their citizens' economic development and thus promote their human rights are threats to

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

their democracies themselves, given that the manifestation of these threats can undermine their citizens' confidence in democracy as a system of government under which they can flourish. In this context, the cyber resilience of CNI assets, which enable and preserve economic development, was argued to be a pillar of their democracies and indeed their governments' ability to implement UNGA-approved cyber norms with respect to human rights and CNI protection. The example of DPI Backbones as CNI assets provided the lens for this chapter on defending democracy in a digital age featuring a worsening cyber threat landscape, with India's approach to DPI and the India Stack serving as a case study.

After introducing DPI and DPGs (the essential ingredients for DPI) as enablers for the delivery of digitally native essential services at scale via open standards-based paradigms unconstrained by the closed paradigms of private technology companies, this chapter explored the DPI of the world's largest democracy and the India Stack. It highlighted the sheer quantum of service delivery by India's DPI, built on the three layers of the India Stack: identify, payments, and data. India's DPI has accelerated financial inclusion, empowered citizens through reliable digital public services, greatly reduced leakages of social security expenditures, and made its COVID-19 vaccination program quite efficient and transparent. In this respect, India's DPI, built atop the India Stack, is crucial to the world's largest democracy driving the economic development of its people and thus their confidence in their democratic system of government as the ideal means of advancing their interests, attracting the praise of world leaders and international organizations alike.

Given that DPI and DPGs are digitally native, and Indians are extremely dependent on the latter for a number of digitally native essential services, the chapter then called for India to prosecute systemic cyber risks to its DPI Backbones that stem from the critical software running on them. With India's G20 presidency forging multilateral consensus on the foundational importance of security to the digital economy, there is a need for India to incentivize the vendors of critical software to invest in the security of their SDLCs, perform robust software SCRM, and manage OSS risks appropriately. India has made progress in doing so, including as G20 President. The *G20 DPI Framework* and *G20 High-Level Principles*, endorsed by the G20 Leaders in 2023 and calling for security to be built into all software and DPI alike, are a testament to India's efforts.

The chapter concluded with a discussion of how India, the world's largest democracy, can export its approach to DPI and the India Stack, especially to fellow democracies in the Global South. Given India's success in advancing its citizens' economic development through DPI and the India Stack, other democracies stand to gain from what it has learned, including by strengthening the trust and confidence of their citizens in democracy as a system of government to drive their development and growth, as well as implementing the UNGA-approved cyber norms. This will be reinforced by advice from India on how to deploy DPI in a cyber-resilient manner, informed by the G20 *High-Level Principles* and G20 *DPI*

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Framework and if India implements the Recommendations, all the more important amid a deteriorating cyber threat landscape.

India is poised to share its approach to DPI and the India Stack for a number of reasons, particularly that: its G20 presidency forged the first multilateral consensus on DPI policy; India is known for being a trusted development partner (for the Global South), which continues to be enhanced by how it is not seeking to weaponize its DPI expertise and the India Stack against smaller democracies (in the Global South); and India is increasingly cooperating on DPI (in the Global South) with leading democracies, which lends its own efforts more credibility. This is backed by the building of momentum at the multilateral and multistakeholder levels since India's G20 presidency on the value of DPI as an instrument of economic and digital development, and the need for greater investment in the development and deployment of DPI around the world.

These factors hold the world's largest democracy in good stead also in its plans to lead "an international architecture of collaboration" on DPI (Carnegie India, 2022) through initiatives such as the OFA, SIF, and GDPIR, potentially integrated with the DAKSHIN global center of excellence for the Global South. Its leadership and partnership with other countries will be aided by its work through the Quad on DPI and on uplifting software security in general, given that DPI and DPGs are digitally native, and this work will help *all countries* implement the UNGA-approved cyber norms, as well as deliver public goods for their people such as national cyber resilience and national security. This is complemented by India's strides in exporting its approach to DPI, including through the linkage of the UPI with overseas payments networks, the sharing of an open-sourced version of CoWIN with a few dozen countries for their vaccination programs, as well as its agreeing to work bilaterally with a range of Global South countries on their development and deploying DPI.

Whether it is deploying DPI at home in a cyber-resilient manner or capacity-building fellow democracies on how to do so in order to bolster their polities' confidence in democracy itself, the world looks to India to lead.

And the world is indeed India's oyster.

REFERENCES

ACI Worldwide. (2023). *It's prime time for real-time 2023*. GlobalData. https://go.aciworldwide.com/rs/030-ROK-804/images/2023-Prime-Time-for-Real-Time-Report.pdf

Agence Nationale de la Sécurité des Systèmes d'Information. (2023, January 15). *Cyber threat overview 2022*. French Government. https://cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf

Alonso, C., Bhojwani, T., Hanedar, E., Prihardini, D., Uña, G., & Zhabska, K. (2023). *Stacking up the benefits: Lessons from India's digital journey* (Working Paper No. 2023/078). International Monetary Fund. https://imf.org/en/Publications/WP/Issues/2023/03/31/Stacking-up-the-Benefits-Lessons-from-Indias-Digital-Journey-531692

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

ANI. (2022a, September 25). *"India is a reliable partner", says Jamaican Foreign Minister in New York*. ThePrint. https://theprint.in/world/india-is-a-reliable-partner-says-jamaican-foreign-minister-in-new-york/1142442/

ANI [@ANI]. (2022b, October 13). *#WATCH | Paolo Mauro, Deputy Director of International Monetary Fund speaks on India's digital cash transfer scheme* [Video attached] [Tweet]. Twitter. https://twitter.com/ANI/status/1580366069780615168

ANI [@ANI]. (2022c, December 1). *We will look very closely and intensely at how India has done in order to promote digitisation. I think India…* [Post]. X. https://twitter.com/ANI/status/1597977439451635712

ASPICanberra. (2024, September 19). *Digital public infrastructure in the Indo-Pacific: security, privacy and accessibility* [Video]. YouTube. https://youtu.be/8A3xloF-SuM

Australian Cyber Security Centre. (2022, November 4). *Annual cyber threat report: July 2021 to June 2022*. Australian Government. https://cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf

Australian Signals Directorate. (2023, November 14). *ASD annual cyber threat report: 2022–2023*. Australian Government. https://cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

Banerji, E. (2023, January 26). *Opinion | India: The voice of the global south*. News18. https://news18.com/news/opinion/opinion-india-the-voice-of-the-global-south-6917011.html

Behrends, J., Simons, J., Troy, K., & Gupta, H. (2021). *Digital public goods: Guidance for development, governance, and stewardship*. Harvard University. https://ethics.harvard.edu/publications/digital-public-goods-guidance-development-governance-and-stewardship

Blinken, A. J. (2022, May 10). *Attribution of Russia's malicious cyber activity against Ukraine* [Press release]. U.S. Department of State. https://state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine

Burt, C. (2018, June 13). *Vendor lock-in hindering African identity projects*. Biometric Update. https://biometricupdate.com/201806/vendor-lock-in-hindering-african-identity-projects

Carnegie India. [Carnegie India]. (2022, November 30). *Panel: The Next Decade of India Stack* [Video]. YouTube. https://youtu.be/sfInBUOgIcQ

Chandna, H. (2021, November 15). *CoWIN set to go global as over 12 countries in talks with govt to borrow technology*. News18.com. https://news18.com/news/india/cowin-set-to-go-global-as-over-12-countries-in-talks-with-govt-to-borrow-technology-4443131.html

Chaudhuri, R. (2023, September 1). *Decoding the G20 consensus on digital public infrastructure: A key outcome of India's presidency*. Carnegie India. https://carnegieindia.org/2023/09/01/decoding-g20-consensus-on-digital-public-infrastructure-key-outcome-of-india-s-presidency-pub-90467

Choudhary, S., & Singh, N. (2023, August 27). *9 years on, Jan-Dhan helps govt seal leaks and purge bogus accounts: About 6.26 PMJDY account holders receives DBT*. Business Standard. https://business-standard.com/india-news/jan-dhan-helps-centre-tackling-corruption-in-direct-benefits-transfers-123082700732_1.html

Choudhury, D. (2023, April 26). *ONDC grows 25 times in 2 months to cross 5,000 food, grocery orders a day*. moneycontrol. https://moneycontrol.com/news/business/startup/ondc-grows-25-times-in-2-months-to-cross-5000-food-grocery-orders-a-day-10478711.html

Clancy, C., Ferraro, J., Martin, R., Pennington, A., Sledjeski, C., & Wiener, C. (2021, January). *Deliver uncompromised: Securing critical software supply chains: Proposal to establish an end-to-end framework for software supply chain integrity*. The MITRE Corporation. https://mitre.org/sites/default/files/2021-11/prs-21-0278-deliver-uncompromised-securing-critical-software-supply-chain.pdf

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

CloudSEK TRIAD Team. (2023, February 8). *Global threat landscape report 2021–2022*. CloudSEK. https://cloudsek.com/whitepapers-reports/global-threat-landscape-report-2021-2022

Commonwealth of Australia, Government of India, Government of Japan, & United States Government. (2023, May 20). *Quad Cybersecurity Partnership: Joint principles for secure software*. PMC.gov.au. https://pmc.gov.au/sites/default/files/resource/download/quad-joint-principles-secure-software.pdf

Commonwealth of Australia, Government of India, Government of Japan, & United States Government. (2024a, September 21). *The Wilmington Declaration Joint Statement from the Leaders of Australia, India, Japan, and the United States* [Joint statement]. https://whitehouse.gov/briefing-room/statements-releases/2024/09/21/the-wilmington-declaration-joint-statement-from-the-leaders-of-australia-india-japan-and-the-united-states/

Commonwealth of Australia, Government of India, Government of Japan, & United States Government. (2024b, September 22). *Quad Principles for Development and Deployment of Digital Public Infrastructure* [Media Note]. https://state.gov/quad-principles-for-development-and-deployment-of-digital-public-infrastructure/

Cybersecurity & Infrastructure Security Agency. (2021a, April). *Defending against software supply chain attacks*. United States Government. https://cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

Cybersecurity & Infrastructure Security Agency. (2021b, July 20). *Cyber-attack against Ukrainian critical infrastructure* (ICS Alert No IR-ALERT-H-16-056-01). United States Government. https://cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

D'Silva, D., Filková, Z., Packer, F., & Tiwari, S. (2019, December). *The design of digital financial infrastructure: Lessons from India* (BIS Paper No. 106). Bank for International Settlements. https://bis.org/publ/bppdf/bispap106.pdf

Dahl, R. A., & Shapiro, I. (2024, December 18). Democracy. In The Editors of Encyclopaedia Britannica (Eds.), *Encyclopaedia Britannica*. Encyclopaedia Britannica. https://britannica.com/topic/democracy

DD News. (2023, November 17). *PM Modi unveils DAKSHIN at Global South Summit*. DD News. https://ddnews.gov.in/international/pm-modi-unveils-dakshin-global-south-summit

Department of Financial Services. (2023, May). *Pradhan Mantri Jan Dhan Yojana (PMJDY)*. Mission Office, Department of Financial Services, Ministry of Finance, Government of India. https://pmjdy.gov.in/

Desai, V. T., Markskell, J., Marin, G., & Varghese, M. (2023, March 15). *How digital public infrastructure supports empowerment, inclusion, and resilience*. World Bank Blogs. https://blogs.worldbank.org/digital-development/how-digital-public-infrastructure-supports-empowerment-inclusion-and-resilience

Digital India [@_DigitalIndia]. (2023, November 5). *#KeyHighlights Address by G20 Sherpa Shri Amitabh Kant (@amitabhk87) at the Workshop on Transformative Technology – Promoting Development, Growth and Innovation…* [Post]. X. https://x.com/_DigitalIndia/status/1721099269413683237

Economic development. (2023). *Cambridge Dictionary*. Cambridge University Press.

European Commission. (2020, October 21). *Communication to the Commission: Open Source Software Strategy 2020–2023* (Communication No C(2020) 7149). European Union. https://commission.europa.eu/system/files/2023-02/en_ec_open_source_strategy_2020-2023.pdf

European Union & Government of India. (2023, May 16). *EU–India Joint Statement 1st meeting of the Trade and Technology Council* [Joint statement]. European Commission. https://digital-strategy.ec.europa.eu/en/library/eu-india-ttc-joint-statement

Feldman, M., Hadjimichael, T., Lanahan, L., & Kemeny, T. (2016). The logic of economic development: A definition and model for investment. *Environment and Planning C: Government and Policy*, *34*(1), 5–21. https://doi.org/10.1177/0263774X156 14653

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

G7 Digital and Tech Ministers. (2023). *Ministerial Declaration: The G7 Digital and Tech Ministers' Meeting* [Ministerial Declaration]. University of Toronto. https://g7.utoronto.ca/ict/2023-declaration.html

G20 Digital Economy Ministers. (2023). *Digital Economy Ministers Meeting: Outcome document & chair's summary*. G20. https://g7g20-documents.org/database/document/2023-g20-india-sherpa-track-digital-economy-ministers-ministers-language-g20-digital-economy-ministers-meeting-outcome-document-and-chair-summary

G20 Leaders. (2023). *G20 New Delhi Leaders' Declaration*. G20. https://g20.in/content/dam/gtwenty/gtwenty_new/document/G20-New-Delhi-Leaders-Declaration.pdf

Gajbhiye, D., Arora, R., Arham, N., Yangdol, R., & Thakur, I. (2022). *Measuring India's digital economy*. Reserve Bank of India. https://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/05ART201220221265B8E871824B98970F03E87228C0FE.PDF

Gates, B. [@BillGates]. (2023, September 12). *The #G20 reached a groundbreaking consensus on the role of digital public infrastructure as a critical accelerator of the Sustainable* [Post]. X. https://twitter.com/BillGates/status/1701318146878218667

Gawen, E., Hirschfeld, A., Kenny, A., Stewart, J., & Middleton, E. (2021). *Open source in government: Creating the conditions for success*. Public Digital. https://assets.public.digital/Open_Source_Exec_Summary.pdf

Ghosh, S. K. (2021). *Share of informal economy may have shrunk to no more than 20% from 52% in FY18* (Ecowrap Issue No. 43, FY22). State Bank of India. https://sbi.co.in/documents/13958/10990811/01112021_Ecowrap_20211101.pdf/a4a69fed-e227-6da0-d217-a8474a5ae982?t=1635764900143

Global DPI Summit 2024. (2024). *Global DPI Summit Outcome Statement* [Outcome statement]. https://globaldpisummit.org/page/4280934/outcome-statement

Google India Team. (2024, October 3). *Driving large-scale impact for businesses and individuals through Gemini and Google Cloud* [Blog post]. Google. https://blog.google/intl/en-in/company-news/outreach-initiatives/driving-large-scale-impact-for-businesses-and-individuals-through-gemini-and-google-cloud/

Government of India. (2023a). *Direct benefit transfer*. Direct Benefit Transfer Mission, Government of India. https://dbtbharat.gov.in/

(2023b, November 15). *2nd voice of Global South Summit* [Press release]. Ministry of External Affairs, Government of India. https://mea.gov.in/press-releases.htm?dtl/37261/2nd_Voice_of_Global_South_Summit

(2023c, December 4). *Visit of US Principal Deputy National Security Adviser to India (December 04, 2023)* [Press release]. Ministry of External Affairs, Government of India. https://mea.gov.in/press-releases.htm?dtl/37333/Visit_of_US_Principal_Deputy_National_Security_Adviser_to_India_December_04_2023

Government of India, Government of Brazil, & Government of South Africa. (2024, November 20). *Declaration on Digital Public Infrastructure, AI and Data for Governance* [Declaration]. Ministry of External Affairs, Government of India. https://mea.gov.in/bilateral-documents.htm?dtl/38551/Declaration+on+Digital+Public+Infrastructure+AI+and+Data+for+Governance++Joint+Communiqu233+by+the+G20+Troika+India+Brazil+and+South+Africa+endorsed+by+several+G20+countries+guest+countries+and+international+organizations

Government of India, & Government of France. (2024, January 26). *India – France Joint Statement on the State Visit of H.E. Mr. Emmanuel Macron, President of French Republic, to India (25–26 January 2024)* [Joint statement]. https://mea.gov.in/bilateral-documents.htm?dtl/37534/India__France_Joint_Statement_on_the_State_Visit_of_HE_Mr_Emmanuel_Macron_President_of_French_Republic_to_India_25__26_January_2024

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

(2023, July 14). *Horizon 2047: 25th Anniversary of the India-France Strategic Partnership, Towards A Century of India-France Relations* [Joint statement]. https://mea.gov.in/bilateral-documents.htm?dtl/36806/Horizon_2047_25th_Anniversary_of_the_IndiaFrance_Strategic_Partnership_Towards_A_Century_of_IndiaFrance_Relations

Government of India, & Republic of Germany. (2024, October 25). *Joint Statement: 7th India-Germany Inter-Governmental Consultations (IGC)* [Joint statement]. Ministry of External Affairs, Government of India. https://mea.gov.in/bilateral-documents.htm?dtl/38467/Joint_Statement_7th_IndiaGermany_InterGovernmental_Consultations_IGC

Government of India, & Republic of Maldives. (2024, October 7). *India and Maldives: A Vision for Comprehensive Economic and Maritime Security Partnership* [Joint statement]. Ministry of External Affairs, Government of India. https://mea.gov.in/bilateral-documents.htm?dtl/38384/India_and_Maldives_A_Vision_for_Comprehensive_Economic_and_Maritime_Security_Partnership

Government of India, & Government of Sri Lanka. (2023, July 21). *Promoting connectivity, catalysing prosperity: India-Sri Lanka Economic Partnership Vision* [Joint statement]. Ministry of External Affairs, Government of India. https://mea.gov.in/bilateral-documents.htm?dtl/36864/Promoting_Connectivity_Catalysing_Prosperity_IndiaSri_Lanka_Economic_Partnership_Vision

(2024, December 16). *India – Sri Lanka Joint Statement: Fostering Partnerships for a Shared Future* [Joint statement]. Ministry of External Affairs, Government of India. https://mea.gov.in/press-releases.htm?dtl/38797/India__Sri_Lanka_Joint_Statement__Fostering_Partnerships_for_a_Shared_Future

Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history: Crippled ports. Paralyzed Corporations. *Wired*. https://wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

(2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Gupta, T. (2022, May 11). Explained: How the ONDC Is all set to democratise e-commerce in India. *Swarajya*. https://swarajyamag.com/technology/explained-how-the-ondc-is-all-set-to-democratise-e-commerce-in-india

Guterres, A. (Speaker). (2022, October 19). *Secretary-General's remarks on the partnership between India and the United Nations on India's 75th anniversary* [Speech Transcript]. United Nations. https://un.org/sg/en/content/sg/speeches/2022-10-19/secretary-generals-remarks-the-partnership-between-india-and-the-united-nations-india%E2%80%99s-75th-anniversary

Herr, T., Lee, J., Loomis, W., & Scott, S. (2020, July). *Breaking trust: Shades of crisis across an insecure software supply chain*. Atlantic Council. https://atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf

HT News Desk. (2024, March 29). *PhonePe users can now make UPI payments in UAE: All you need to know*. Hindustan Times. https://hindustantimes.com/business/phonepe-users-can-now-make-upi-payments-in-uae-all-you-need-to-know-101711681533321.html

ID4D. (2020). *Open source for global public goods*. World Bank Group. https://documents1.worldbank.org/curated/en/672901582561140400/pdf/Open-Source-for-Global-Public-Goods.pdf

Inglis, C., & Neuberger, A. (2021, October 28). *A conversation with Chris Inglis and Anne Neuberger (J. A. Lewis, interviewer)* [Interview transcript]. Centre for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211028_Lewis_Inglis_Neuberger.pdf

International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

iSPIRT. (2021, December 15). *IndiaStack*. IndiaStack. https://indiastack.org

Jacob, S. (2024, 1 April). *In a first, yearly transactions through UPI cross 100 billion in FY24*. Business Standard. https://business-standard.com/finance/news/upi-transactions-cross-100-billion-mark-in-fy24-clock-131-billion-124040100655_1.html

Jaishankar, Dr. S. [@DrSJaishankar]. (2023a, November 17). *Addressed the first Foreign Ministers' session of the Voice of Global South Summit. Made the following points: India walked the…* [Post]. X. https://twitter.com/DrSJaishankar/status/1725457015051608130

(2023b, November 17). *Addressed the second Foreign Ministers' session of the Voice of Global South Summit. Made the following points: India took over…* [Post]. X. https://twitter.com/DrSJaishankar/status/1725489700381893077

Kant, A., & Sudke, A. (2023, November 22). *Lessons for Africa, from India: Africa can achieve quick and inclusive growth by Replicating India's DPI model*. Financial Express. https://financialexpress.com/opinion/lessons-for-africa-from-india/3313459/lite/

Kumar, M. (2021, November 26). *India to push for patent waiver for COVID-19 vaccines at WTO*. Reuters. https://reuters.com/world/india/india-push-patent-waiver-covid-19-vaccines-wto-2021-11-26

Lele, S. (2023, March 23). *Philippines and Morocco start the adoption of Aadhaar architecture*. Business Standard. https://business-standard.com/article/international/philippines-and-morocco-start-the-adoption-of-aadhaar-architecture-123032201100_1.html

Lewis, J. (2023, April 10). *An overview of global cloud competition*. Centre for Strategic & International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230410_Lewis_Overview_Cloud_1.pdf

Marslev, K., & and Sano, H.-O. (2016). *The Economy of Human Rights: Exploring potential linkages between human rights and economic development* (Human Rights Research Paper No 2016/2, 2016). The Danish Institute for Human Rights. https://humanrights.dk/sites/humanrights.dk/files/media/migrated/the_economics_of_human_rights_2016.pdf

Mehta, N. (2023, September 9). G20: India's new soft power is digital public infrastructure. *The Times of India*. https://timesofindia.indiatimes.com/blogs/academic-interest/g20-indias-new-soft-power-is-digital-public-infrastructure/

Ministry of Commerce & Industry. (2022, September 19). *Shri Piyush Goyal concludes fruitful visit to Saudi Arabia* [Press release]. Ministry of Commerce & Industry. https://pib.gov.in/PressReleasePage.aspx?PRID=1860633

Ministry of Electronics and Information Technology. (2023, November 23). *Prime Minister announces completion of Global Digital Public Infrastructure Repository and creation of a Social Impact Fund to advance Digital Public Infrastructure in Global South* [Press release]. https://pib.gov.in/PressReleasePage.aspx?PRID=1979113

Ministry of External Affairs. [Ministry of External Affairs, India]. (2022a, September 24). *India@75: Showcasing India UN Partnership in Action (Sep 24, 2022)* [Video]. YouTube. https://youtube.com/live/8fvQ1X1g-eU

(2022b, November 29). *EAM: Global Technology Summit 2022* [Video]. YouTube. https://youtube.com/live/MR-ebRUHMCU

(2022c, December 9). *G-20 and India's Presidency* [Press release]. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882356

(2023a, January 13). *Summary of Deliberations: Voice of Global South Summit 2023 (January 12–13, 2023)* [Statement]. Government of India. https://mea.gov.in/bilateral-documents.htm?dtl/36119/Summary_of_Deliberations_Voice_of_Global_South_Summit_2023_January_1213_2023

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

(2023b, February 23). *Annual Report 2022*. Government of India. https://mea.gov.in/Uploads/PublicationDocs/36286_MEA_Annual_Report_2022_English_web.pdf

(2023c, July 27). *15th India-Japan Foreign Ministers' Strategic Dialogue* [Press release]. Government India. https://mea.gov.in/press-releases.htm?dtl/36913/15th+India Japan +Foreign+Ministers+Strategic+Dialogue

(2024a, February 12). *Prime Minister jointly inaugurates UPI services with Mauritius Prime Minister & Sri Lankan President* [Press release]. https://mea.gov.in/press-releases.htm?dtl/37616/Prime_Minister_jointly_inaugurates_UPI_services_with_Mauritius_Prime_Minister_amp_Sri_Lankan_President

(2024b, February 13). *Prime Minister's meeting with the President of the UAE* [Press release]. https://mea.gov.in/press-releases.htm?dtl/37620/Prime_Ministers_meeting_with_the_President_of_the_UAE

Ministry of Finance. (2023, January). *Economic Survey 2022–23*. Government of India. https://indiabudget.gov.in/economicsurvey/

Ministry of Health and Family Welfare. (2021, July 5). *Prime Minister Shri Narendra Modi inaugurates the Co-WIN Global Conclave* [Press release]. https://pib.gov.in/PressReleaseIframePage.aspx?PRID = 1732897

Modi, N. (2023, September 6). Narendra Modi: India's G20 is a chance for the world to unite. *The Times*. https://thetimes.co.uk/article/narendra-modi-indias-g20-is-a-chance-for-the-world-to-unite-gpp6jgfjn

[@narendramodi]. (2024, August 28). *Today, we mark a momentous occasion—#10YearsOfJanDhan. Congratulations to all the beneficiaries and compliments to all those who worked to* [Post]. X. https://x.com/narendramodi/status/1828640493737054688

MyGovIndia [@mygovindia]. (2023, August 28). *Banking for all paves the way for a brighter tomorrow. With a rising number of Jan Dhan Accounts, we're forging...* [Image attached] [Tweet]. X. https://x.com/mygovindia/status/1696003775012413487

Narlikar, A. (2021). Must the weak suffer what they must? In D. W. Dresser, H. Farrell, & A. L. Newman (Eds.), *The uses and abuses of weaponized interdependence* (pp. 289–304). Brookings Institution Press.

National Institute of Standards and Technology. (2021, October 13). *Definition of Critical Software Under Executive Order (EO) 14028*. United States Government. https://nist.gov/system/files/documents/2021/10/13/EO Critical FINAL.pdf

Nayyar, R. (2023). *The quad: Carved in code: Collaborating to deliver the greatest public good*. German Institute for Global and Area Studies. https://giga-hamburg.de/assets/tracked/pure/48834609/GIGA_DigitalDiplomacyStatecraft_WP_01_Nayyar_update2307.pdf

Newbill, C. M. (2019). Defining critical infrastructure for a global application. *Indiana Journal of Global Legal Studies, 26*(2), 761–779. https://repository.law.indiana.edu/ijgls/vol26/iss2/11

NPCI International. (2024a, January 17). *Google Pay India signs MoU with NPCI International for Global Expansion of UPI* [Press release]. https://npci.org.in/PDF/npci/press-releases/2024/NPCI-Press-Release-Google-Pay-India-signs-MoU-with-NPCI-International-for-Global-Expansion-of-UPI.pdf

(2024b, February 29). *NPCI International and Eurobank Sign MoU in View of Forming a Strategic Alliance on Foreign Inward Remittances* [Press release]. https://npci.org.in/PDF/npci/press-releases/2024/NIPL-Press-Release-NPCI-International-and-Eurobank-Sign-MoU-in-View-of-Forming-a-Strategic-Alliance-on-Foreign-Inward-Remittances.pdf

(2024c, May 2). *NPCI International Partners with Bank of Namibia for Deploying India's UPI Stack in Namibia* [Press release]. https://npci.org.in/PDF/npci/press-releases/2024/NPCI-International-Partners-with-Bank-of-Namibia-for-Deploying-India's-UPI-Stack-in-Namibia.pdf

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

(2024d, June 5). *NPCI International and the Central Reserve Bank of Peru Partner to Develop UPI-Like Real-Time Payments System in Peru* [Press release]. https://npci.org.in/PDF/npci/press-releases/2024/NIPL-Press-Release-NPCI-International-and-the-Central-Reserve-Bank-of-Peru-Partner-to-Develop-UPI-Like-Real-Time-Payments-System-in-Peru.pdf

NTIA Multistakeholder Process on Software Component Transparency Framing Working Group. (2021, October 21). *Framing Software component transparency: Establishing a common software bill of materials (SBOM)*. United States Government. https://ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

Observer Research Foundation. [ORF]. (2022, October 19). *India @ 75 || India-UN Partnership: Strengthening South-South Cooperation* || [Video]. YouTube. https://youtube.com/live/bItbHTPBE_4

OECD. (2021). *Development Co-operation Report 2021: Shaping a just digital transformation*. OECD Publishing. https://doi.org/10.1787/ce08832f-en

(2022). *OECD policy framework on digital security*. OECD Publishing. https://doi.org/10.1787/a69df866-en

OECD Council. (2022, September 26). *Recommendation of the Council on National Digital Security Strategies* [OECD Legal Instrument No OECD/LEGAL/0480]. OECD. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480

Open Network for Digital Commerce. (2022, January). *Open network for digital commerce: Democratizing digital commerce in India*. https://ondc-static-web-bucket.s3.ap-south-1.amazonaws.com/res/daea2fs3n/image/upload/ondc-website/files/ONDCStrategyPaper_ucvfjm/1659889490.pdf

Pant, H. V. (2023, September 14). *Rediscovering the centrality of the Global South*. Observer Research Foundation. https://policycommons.net/artifacts/4825715/rediscovering-the-centrality-of-the-global-south/5662432/

Parliamentary Joint Committee on Intelligence and Security. (2022). *Advisory report on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*. Parliament of Australia. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024898/toc_pdf/AdvisoryreportontheSecurityLegislationAmendment(CriticalInfrastructureProtection)Bill2022.pdf;fileType = application/pdf

Perlroth, N. (2021). *This is how they tell me the world ends*. Bloomsbury Publishing.

PIB India. [@PIB_India]. (2024, December 14). *Driving the #DigitalPayment revolution, #UPI achieved 15,547 crore transactions worth Rs. 223 lakh crore from January to November, 2024, showcasing* [Post]. X. https://x.com/PIB_India/status/1867834028487020946

Prime Minister's Office. (2023, February 21). *PM Narendra Modi and Prime Minister of Singapore Lee Hsien Loong participate in the Virtual Launch of UPI-PayNow Linkage between India and Singapore* [Press release]. https://pib.gov.in/PressReleseDetail.aspx?PRID = 1900976

Pancholy, P. (2024, July 1). *Reserve Bank of India and ASEAN Countries to Create a Platform to Facilitate Instantaneous Cross-Border Retail Payments* [Press release]. https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid = 58197

Prince, M. [@eastdakota] (2021, December 14). *Correction: Seeing >1000 per second instances of ${, of those 400 per second are confirmed attempts at exploit* [Tweet]. Twitter. https://twitter.com/eastdakota/status/1470819030155993089

PTI. (2023, March 1). *Bill Gates praises India's digital public networks, payment systems; says this will be cheapest 5g market*. Outlook. https://business.outlookindia.com/news/bill-gates-praises-india-s-digital-public-networks-payment-systems-says-this-will-be-cheapest-5g-market-news-266464

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

Quad Senior Cyber Group. (2023, May 20). *Quad cybersecurity partnership: Joint principles for secure software*. Department of the Prime Minister and Cabinet. https://pmc.gov.au/sites/default/files/resource/download/quad-joint-principles-secure-software.pdf

Romine, C. H. (2017, June 15). *Testimony of Charles H. Romine, Ph.D.* U.S. Department of Commerce. https://ogc.commerce.gov/sites/default/files/media/files/2017/20170615_house_science_-_romine.pdf

Rudra, T. (2023, July 14). *UPI enters France following NPCI's MoU agreement with Lyra Network last year*. Inc42. https://inc42.com/buzz/upi-enters-france-following-npcis-mou-agreement-with-lyra-network-last-year/

Sansad TV. [Sansad TV]. (2023, February 4). *Diplomatic Dispatch: India's Leadership in Digital Public Goods | 03 February, 2023* [Video]. YouTube. https://youtu.be/HZNOT2tq4vo

Scott, S., Brackett, S. A., Herr, T., & Hamin, M. (2023, February). *Avoiding the success trap: Toward policy for open-source software as infrastructure*. Atlantic Council. https://atlanticcouncil.org/wp-content/uploads/2023/02/Avoiding-the-success-trap-Toward-policy-for-open-source-software-as-infrastructure.pdf

Security of Critical Infrastructure Act 2018 (Cth).

Sen, A. (2001). *Development as freedom*. Oxford University Press.

Sibal, S. [@sidhant] (2022, July 29). *Statement in Parliament* [Image attached] [Tweet]. Twitter. https://twitter.com/sidhant/status/1552962784224153600/photo/1

(2023, May 19). *Exclusive | Japan considering joining India's UPI payment system, says Japanese Minister Kono Taro*. WION. https://wionews.com/world/exclusive-japan-considering-joining-indias-upi-payment-system-says-japanese-minister-kono-taro-593773

Silvers, R., Adkins, H., Alperovitch, D., Carlin, J., DeRusha, C., Inglis, C., et al. (2022, July 11). *Review of the December 2021 Log4j Event*. United States Government. https://cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf

SLSA. (2023). *Introduction*. https://slsa.dev/spec/v0.1/#supply-chain-threats.

Smart, W. (2018). *Lessons learned review of the WannaCry ransomware attack*. Department of Health & Social Care. https://england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

Sonatype. (2023). *8th Annual State of the Software Supply Chain*. Sonatype. https://sonatype.com/hubfs/8th%20Annual%20SSCR%20-%202023.pdf

Souppaya, M., Scarfone, K., & Dodson, D. (2022, February). *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* (NIST Special Publication No 800-218). United States Government. https://doi.org/10.6028/NIST.SP.800-218

Starks, T. (2021, December 13). *CISA warns 'most serious' Log4j Vulnerability likely to affect hundreds of millions of devices*. CyberScoop. https://cyberscoop.com/log4j-cisa-easterly-most-serious

Synopsys. (2023, February 22). *2023 Open source security and risk analysis report*. Synopsys. https://synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2023.pdf

The Pharma Letter. (2023, March 22). *India and South Africa renew push for extending TRIPS waiver beyond Covid vaccines*. https://thepharmaletter.com/article/india-and-south-africa-renew-push-for-extending-trips-waiver-beyond-covid-vaccines

The President's Office. (2024, October 20). *President decides to introduce India's Unified Payment Interface in Maldives, paving the way for improved financial transactions* [Press Release]. Republic of Maldives. https://presidency.gov.mv/Press/Article/31921

The White House. (2023, March). *National cybersecurity strategy*. The United States Government. https://whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013

The White House & Government of India. (2023, June 22). *Joint statement from the United States and India* [Joint statement]. The White House. https://whitehouse.gov/briefing-room/statements-releases/2023/06/22/joint-statement-from-the-united-states-and-india/

(2024, September 21). *Joint Fact Sheet: The United States and India Continue to Expand Comprehensive and Global Strategic Partnership* [Joint Fact Sheet]. The White House. https://whitehouse.gov/briefing-room/statements-releases/2024/09/21/joint-fact-sheet-the-united-states-and-india-continue-to-expand-comprehensive-and-global-strategic-partnership/

Trautman, L. J., & Ormerod, P. C. (2019). WannaCry, ransomware, and the emerging threat to corporations. *Tennessee Law Review*, *86*(2), 503–556. https://ir.law.utk.edu/cgi/viewcontent.cgi?article = 1080&context = tennesseelawreview

United Nations. (2019, November 26). *Democracy*. United Nations. https://un.org/en/global-issues/democracy

(2020). *Road map for digital cooperation: Implementation of the recommendations of the high-level panel on digital cooperation: Report of the Secretary-General*. United Nations. https://un.org/en/content/digital-cooperation-roadmap/

United Nations, General Assembly, *The Pact for the Future*, A/79/L.2 (20 September 2024), available from https://docs.un.org/A/79/L.2.

United Nations, General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135 (14 July 2021), available from https://docs.un.org/A/76/135.

Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

U.S. Department of Commerce & U.S. Department of Homeland Security. (2022, February 23). *Assessment of the critical supply chains supporting the U.S. information and communications technology industry*. United States Government. https://dhs.gov/sites/default/files/2022-02/ICTSupplyChainReport_0.pdf

U.S. Mission Korea. (2024, March 13). *Readout of the United States–India–Republic of Korea Trilateral Technology Dialogue* [Press release]. U.S. Embassy & Consulate in the Republic of Korea. https://kr.usembassy.gov/031324-readout-of-the-united-states-india-republic-of-korea-trilateral-technology-dialogue/

Viasat, Inc. (2022, March 30). *KA-SAT Network cyberattack overview*. Viasat. https://viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

Vir, A. & Sanghi, R. (2021, January 15). The internet country: How India created a digital blueprint for the economies of the future. *Tigerfeathers*. https://tigerfeathers.substack.com/p/the-internet-country

Vivekananda International Foundation. (2019, March 25). *Vasudhaiva Kutumbakam: Relevance of India's ancient thinking to contemporary strategic reality*. https://vifindia.org/sites/default/files/Vasudhaiva-Kutumbakam-Conference-Proceedings.pdf

Wadhwa, V., Amla, I., & Salkever, A. (2022, June 30). *As Silicon Valley fantasizes about Web3, India leaps ahead on payments*. Fortune. https://fortune.com/2022/06/30/blockchain-india-upi-payments-global-reach/

World Bank Group. (2023). *G20 policy recommendations for advancing financial inclusion and productivity gains through digital public infrastructure*. World Bank Group. https://openknowledge.worldbank.org/entities/publication/b8d6b107-3e97-41be-886d-1c46ee906042

World Health Organization. (2021, January 16). *India rolls out the world's largest COVID-19 vaccination drive* [Press release]. World Health Organization. https://who.int/india/news/feature-stories/detail/india-rolls-out-the-world-s-largest-covid-19-vaccination-drive.

Zetter, K. (2016, May 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. https://wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:21:38, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.013