Digital Public Infrastructure: Concepts, Global Efforts, Benefits, Challenges, and Success Stories

Ozili, Peterson K

2025

Digital Public Infrastructure: Concepts, Global Efforts, Benefits, Challenges, and Success Stories

Peterson K. Ozili

Abstract

Digital public infrastructure (DPI) is an emerging innovation that leverages digital technologies to increase access to public and social services towards improving people's welfare and livelihoods in society. DPI is a set of digital systems that enable members of society to safely and efficiently connect to open-source digital networks to access social services and other economic opportunities that improve their welfare. The study explores the concept of digital public infrastructure, the global trends, opportunities and challenges. The study also highlights some DPI success and failure stories across countries, and it offers some insights into the challenges and risks of digital public infrastructure. It was shown that digital public infrastructure has many components, and it is enabling digital access to public goods and services for many individuals who lack access to essential goods and services. As a result, many individuals and firms are connecting with one another through a public digital networked infrastructure. However, DPI poses some risks or challenges such as difficulty in evaluating impact, cybersecurity risks, lack of interoperability between digital systems, digital exclusion, lack of private and public sector collaboration, lack of accountability mechanisms, ethical dilemmas and geopolitical concerns. The discussion in this article contributes to the digital society literature by showing that digital public infrastructure is an essential part of a digital society and the benefits of DPI to society are enormous if the risks can be mitigated.

Keywords: digital public infrastructure, digital ID, digital payment, data exchange, interoperability, public-private partnerships, cybersecurity, digital society.

April 2025

To cite:

Ozili, P. K. (2025). Digital Public Infrastructure: Concepts, Global Efforts, Benefits, Challenges, and Success Stories. *Digital Society*, *4*(1), 1-22.

1. Introduction

This study explores the concept of digital public infrastructure, the global trends, opportunities and challenges. The term "digital public infrastructure" gained prominence during India's G20 presidency in 2023. It is a term used to describe open-source digital public networked systems that deliver public services to citizens, firms, and governments.

The need for DPI became apparent during the 2020-2022 COVID-19 pandemic. During the pandemic, countries that had robust digital public infrastructure were able to make fast and efficient digital cash transfers to support households during the pandemic (Kumar, 2020). In contrast, countries that did not have a digital public infrastructure were unable to make efficient digital cash transfers to support households during the pandemic (Ozili, 2021). This shows the importance of having a well-functioning digital public infrastructure.

The need for digital public infrastructure also arises from the growing concern that digital inclusion is not happening fast enough in many countries, especially in developing countries that lack adequate financial resources to invest in digital public systems (Webber et al, 2022; Dahlman, et al, 2016). Some developed countries that have abundant financial resources to invest in DPI still have siloed or stand-alone digital systems which are not interoperable with other digital systems. Meanwhile, many African countries have some type of digital systems, but they lack robust digital identity systems which are an integral part of DPI (Dahlman et al, 2016). As a result, many people are left behind and cannot access digital markets and digital services to take advantage of economic opportunities that arise from a well-organized and coordinated digital public infrastructure (Williams et al, 2016; Holmes and Burgess, 2022).

Presently, some countries have siloed digital systems which are owned by private monopolies or large technology firms that charge high fees (McIntosh, 2018). The government in these countries also use these digital systems which are controlled by private monopolies, and the digital systems are often not interoperable. These digital systems may also be exposed to risks such as fraud, cyberattacks, and illicit financial flows if safeguards are not put in place (Cross, 2022; Zukis, 2016; Hodapp and Hanelt, 2022). These risks create inefficiencies and digital exclusion problems that leave many people behind because they cannot access digital markets and digital services that meet their needs and improve their livelihoods (Ozili, 2025). Hence, there is a need to move away from the siloed approach to the development of

innovative digital systems and shift to building a safe and inclusive digital public infrastructure and unlock the full benefits of digital public infrastructure.

Understanding the potential of digital public infrastructure is important for several reasons. One, digital public infrastructure is a shared means to many ends; two, it is a critical enabler of digital transformation in society (Zuckerman, 2020); three, it is the foundation of a modern digital economy; four, it helps to improve public service delivery; five, it can help countries to achieve their national priorities; six, it can help countries to accelerate the attainment of the sustainable development goals (Zuckerman, 2020); and seven, it can streamline government operations and create many economic opportunities in many low- and middle-income countries. Therefore, it is important to explore the concept of digital public infrastructure, the global trends, opportunities and challenges.

This study contributes to the existing literature that examines the role of digital technologies in building good digital societies and resilient digital economies. The present study adds to this literature by showing that digital public infrastructure can play a significant role in building a good digital society and a resilient digital economy. The study also contributes to the literature by introducing the concept of a public digital infrastructure and offering policy-useful insights into its definition, components, benefits, stakeholders, success stories, and the challenges of digital public infrastructure. These insights can guide policymakers and practitioners in developing and implementing DPIs that are less risky and beneficial to society. The study further contributes to the literature by illuminating the global efforts being made to promote and develop a digital public infrastructure in countries as well as the success stories of effective implementation of digital public infrastructure in several countries.

The rest of the study is structured as follows. Section 2 presents the theory and related literature. Section 3 presents the conceptual underpinnings, formative components, stakeholders and DPI initiatives. Section 4 highlights the opportunities of digital public infrastructure. Section 5 highlights some DPI success and failure stories. Section 6 presents some challenges of digital public infrastructure while section 7 presents the conclusion of the study.

2. Theory and Related Literature

2.1. Theory

In terms of theory, the technology acceptance model is widely used in the literature to explain the reasons why people will adopt or use certain digital technologies (Schmidthuber et al, 2020; Rabe and Kostka, 2024), such as digital public infrastructure. The technology acceptance model or theory argues that what determines whether an individual will use a technology is the perceived ease-of-use and the perceived usefulness of the technology to the individual (Davis et al, 1989). In other words, individuals will only accept to use a technology if they perceive it to be 'easy-to-use' and 'useful' to them. The main argument of the theory is that people's perception of what technology can do for them is what drives them to accept or reject the technology (Davis et al, 1989). The implication of the theory for DPI is that the adoption of DPI in society depends on people's perception of the usefulness and the ease of use of DPI.

2.2. Studies showing support for DPI

Other studies examined the prospect of developing a digital infrastructure that can serve society. Goldsmith and Gardner (2022) argue that digital infrastructure can assist in managing public assets, scheduling maintenance, monitoring safety, improving sustainability and accessibility, and prioritizing equity in investment, health, and quality of life. They advocate for investment in digital infrastructure that incorporates hardware, data software, platforms for analysis and collaboration, advanced data capabilities and a smart governance structure to oversee these tools through policy and regulation. Hanna et al (2020) advocate for democratic public ownership of foundational digital infrastructures on the principles of (i) access to all to reduce the digital divide in the population, (ii) empower citizens and workers through participation, transparency, and accountability, (iii) reduce corporate concentration and political power, (iv) link digital infrastructure to ecological sustainability, and (v) ensure that people have control and power over their own data, to develop an ethical data management strategy. Hustad and Olsen (2021) focus on the development of service-oriented sustainable digital infrastructures. They argue that the most important factors to consider when developing service-oriented sustainable digital infrastructures are reuse

capabilities, flexibility, agility, information technology and business alignment, and efficient governance mechanisms.

Liu et al (2024) examine the potential of digital infrastructure to improve people's health in China. They examine the construction of digital infrastructure which is the result of the Broadband China policy introduced between 2014 and 2016. They examine whether the digital infrastructure scheme can improve people's health. They use health data from China from 2010 to 2020 to determine the causal relationship between digital infrastructure and people's health. They find that the construction of digital infrastructure improved the health of people. It also improved the use of medical services, it increased people's investment in their health and it helped residents to develop healthy lifestyles. Zhou (2022) examines the relationship between economic growth and digital infrastructure construction in China and find that digital infrastructure can build a digital economy which reduces labour cost and reduce inflation. However, Zhou (2022) points out a major challenge which is the oligarchs that dominate and monopolise the internet-based digital enterprise in China. These oligarchs are an obstacle to effective economic growth.

Meanwhile, Tang and Yang (2023) show that the construction of digital infrastructure can significantly increase total carbon emissions and conserve energy by inducing per capita energy consumption. They recommend the introduction of carbon emission trading scheme to mitigate the impact of digital infrastructure in China cities. Tang and Zhao (2023) examine the role of digital infrastructure in improving total factor productivity for sustainable economic development. They examine 30 regions in China from 2006 to 2017 and find that new digital infrastructure can improve regional total factor productivity, and the positive effect is more pronounced in regions with high economic development levels, high research and development levels, and high traditional infrastructure development levels. Guo et al (2024) also examine the correlation between digital infrastructure and the enterprise green transformation in China. They show that the digital infrastructure in China called the "Broadband China" strategy improves enterprise green transformation, and the mechanism through which the digital infrastructure improves enterprise green transformation is through green technology innovation and alleviating financing constraints. Clarke (2020) considered digital government units as a type of digital public infrastructure which uses digital data and technology to create, optimize and transform digital government services. They pointed out

that many DGUs adopt a common orthodoxy, and they mostly use agile, user-centric design, pluralistic procurement, data-driven decision making, horizontal 'platform' based solutions and a 'delivery-first' ethos.

In an African study, Ayodele (2024) predicts that digital public infrastructure holds the key for African continental integration, and it can help Africa to achieve its developmental ambitions alongside other soft and hard infrastructures which are critical for Africa's development such as postal services, financial services, health services, roads, railways, ports, and electricity and broadband connections. Finger and Montero (2022) examine whether digital platforms which are intermediating with physical public services could be considered public services as they have public service features. They argue that such digital platforms are not purely public services, however, they can be public services if they are regulated to ensure they have the features of public service and reflect public interests. Webber et al (2022) examine the variation in the attitudes of stakeholders towards investments in the digital economy using semi-structured interviews of participants in New Zealand. They find that some stakeholders consider the internet to be an important digital infrastructure in the digital economy, but they raised concern that some people and some places would be left behind if access to the internet is uneven and non-uninform across New Zealand. Other stakeholders had concerns about who will prosper from using the internet, who will be left behind, and who should pay for training on how to use the internet, among others.

2.3. Studies with critical perspectives on DPI

The critical literature show that digital systems or infrastructure are not always beneficial due to the risks associated with technology and people. For instance, Bentley et al (2024) point out that digital technologies, including digital infrastructure systems, have been subject to criticism due to their weak privacy protection and their tendency to increase digital exclusion and worsen the digital divide in society. Lythreatis et al (2022) warn that a widening digital divide in society will erode the expected gains from adopting a public digital infrastructure system because digital illiterate people who do not have access to digital technologies will not benefit from such digital systems. Eaves et al (2024) acknowledge that transparency and accountability are critical for the effective deployment and implementation of DPI. However, they urge for caution and warn that, as smaller digital systems are integrated to build a big

DPI, there is a high possibility that transparency and accountability may be sacrificed in a bid to build a big DPI. Nagar and Eaves (2024) examine the intersection between DPI and artificial intelligence systems. They argue that any attempt to use DPI as a foundation for AI development will give rise to an immediate problem which is that DPI has to be implemented first and its adoption must be widespread, but this is not possible because members of marginalized communities, who may face systemic disparities that limit their ability to use these digital tools, may refuse or may be hesitant to use a government-led DPI due to legacies of marginalization (Nagar and Eaves, 2024). In a study on **Singapore**, Zhuang et al (2025) also argue that although digital systems can create a more resilient, efficient, and competitive society, they widen the digital divide and the people most affected are historically marginalised communities such as people with visual disabilities who are at risk of being left behind. Hardy (2024) further points out that even in digital societies that have adopted a form of DPI, such as the X-road in **Estonia**, many people still face insecurities due to the growing realisation that they cannot live life without being online or being on some sort of digital platform, and arguing that it would be difficult for people to cope and survive if a nationwide or global digital disruption occurs.

2.4. Gap in the literature

While these studies in the literature mostly examine the prospect of digital infrastructure, very little research has been done on the global trend, opportunities and challenges of digital public infrastructure. Therefore, the present study contributes to the literature by introducing the concept of a public digital infrastructure, particularly the definition, components, benefits, stakeholders, success stories, and the challenges of digital public infrastructure. It also explores the global trend, opportunities and challenges of DPI.

3. Conceptual underpinnings, formative components, stakeholders and DPI initiatives

This section presents some conceptual underpinnings of digital public infrastructure such as an analogy, the definition and importance of digital public infrastructure.

3.1. A perfect analogy to understand digital public infrastructure

Digital public infrastructure is similar to roads built by the government which form a physical transportation network that is essential for people to connect with each other. Similarly, digital public infrastructure can be viewed as a digital networked system created by governments to enable people connect digitally with each other to access a wide range of information, goods and services. Just as roads and railways spread across the entire country, the economy, connecting people, and money; in the same way, digital public infrastructure spread across the entire digital economy, connecting people, data, and money. Just as roads and railways are popularly known as the infrastructure of the physical world, digital public infrastructure is also known as the infrastructure of the digital world.

3.2. Definition of digital public infrastructure

Digital public infrastructure is an emerging concept which means that its meaning might change from time to time. Presently, a digital public infrastructure is a set of digital systems that enable countries to provide economic opportunities and deliver social services to the population safely and efficiently (Eaves et al, 2024). The G20 New Delhi Leaders' Declaration defined DPI as a "set of shared digital systems that are secure and interoperable, built on open technologies, to deliver equitable access to public and/or private services at a societal scale".[1] DPI can also be defined as a government-led open-source digital networked system which is built to allow private innovators to build innovations around it to serve public interest (Zuckerman, 2020). In this sense, Digital public infrastructure can be viewed as a combination of two broad elements: (i) networked open technology systems which are built for public interest, and (ii) a community of private sector innovators who are working to drive innovation for public interest.

[1] https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf

3.3. Components of digital public infrastructure

Several components or elements are needed for the successful development and deployment of a digital public infrastructure (see figure 1).

- **Digital identity system**: It enables the creation, management, and authentication of unique identities for use in many digital scenarios (Singh, et al, 2019; Giannopoulou, 2023).

- **Digital payment system**: It enables the exchange of money and near-money instruments between governments, businesses, and individuals (Singh et al, 2019). A digital payment system enables people and corporations to instantly send and receive money.

- **Data exchange and integration system**: It facilitates the sharing of information between individuals, the private sector and the public sector (Rukanova et al, 2023). It ensures that the digital public infrastructure is interoperable with other stand-alone digital systems to enable connectivity with many independent digital systems in a seamless manner to promote inclusive participation and ensure a more open and competitive digital ecosystem.

- **Consent networks**: It is the privacy-based system or mechanism that allows users to authorize access and approve the exchange and usage of their personal digital information (Eaves et al, 2024). In the absence of consent networks, people's right to privacy might be breached.

- **Credentials**: It enables the safe sharing of government-issued and privately issued credentials, such as certificates, invoices, driver's licenses, and passports, on digital spaces and platforms (Hobson et al, 2023).

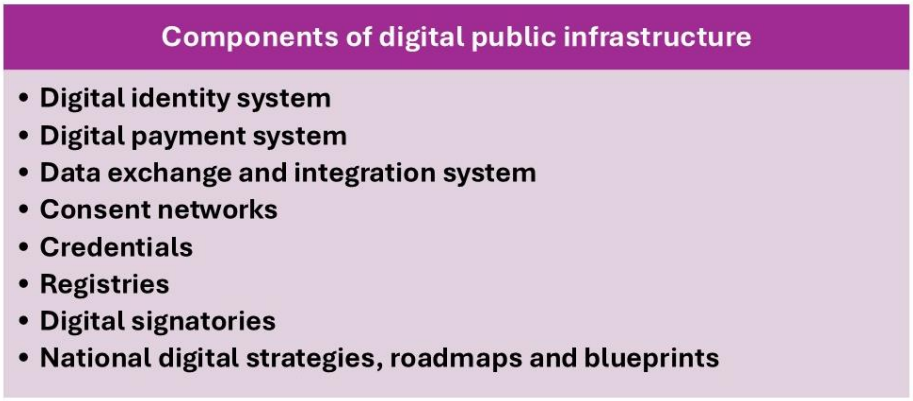
- **Registries**: It is a system that verify claims of ownership of digital assets, digital credentials, or digital information. Digital public infrastructure will function effectively

when there are registries that keep verifiable records of what people own or are entitled to.

- **Digital signatures**: Digital public infrastructure should also have embedded mechanisms that enable digital signatures to be created, verified, and managed to ensure the legal validity of digital documents and digital transactions (Brands, 2000).

- **National digital strategies, roadmaps and blueprints:** Many countries will need to develop wholistic national plans, strategies, roadmaps and blueprints for a robust digital public infrastructure. Many countries may need assistance in developing their digital public infrastructure and in identifying additional elements that might be needed for national digital integration.

Figure 1. Components of digital public infrastructure



Source: Author

3.4. Stakeholders driving digital public infrastructure

Several stakeholders are taking action to create digital public infrastructure in countries (see figure 2). The stakeholders include public sector agents, private sector agents, academia, civil society, and international organisations (Selim and ElGohary, 2020).

- **The private sector:** The role of the private sector in developing digital public infrastructure is to (i) use existing technologies to create innovative solutions for digital public infrastructure, (ii) provide crucial financial resources for digital public infrastructure development in partnership with governments, (iii) provide private

sector expertise in managing complex projects and implementing technology that lead to more sustainable digital public infrastructure systems, and (iv) contribute to training, skill-development initiatives and building local capacities to manage and maintain digital public infrastructure systems (Selim and ElGohary, 2020). Examples of private sector stakeholders include private companies, business associations, lobby groups, etc.

- **The public sector:** The role of the public sector in developing digital public infrastructure is to (i) provide regulatory frameworks for digital public infrastructure, (ii) ensure that the technologies used for DPI solutions are used securely, ethically, responsibly and effectively, (iii) encourage policies and initiatives that foster innovation in the private sector, (iv) provide the initial government funding for digital public infrastructure to encourage and stimulate private sector to also contribute their own financial resources to digital public infrastructure initiatives (Selim and ElGohary, 2020). Examples of public sector stakeholders include government departments, agencies and ministries.

- **Academia**: The role of academia in developing digital public infrastructure is to develop conceptual frameworks that aid the understanding of digital public infrastructure, (ii) develop global digital public infrastructure taxomony to promote uniform shared meaning of digital public infrastructure concepts and terminologies, (iii) organize knowledge sharing forums or conferences with private and public sector experts to promote dialogue that support decision making at the highest levels, (iv) produce high quality research outputs that inform and influence policymaker's decision on the most effective and efficient way to deploy digital public infrastructure. Examples of academic stakeholders include academic research staff, university departments, centers of knowledge, research institutes, etc.

- **Civil society organizations**: The role of civil society organizations in developing digital public infrastructure is to (i) raise awareness about the need for a country to have its own digital public infrastructure, (ii) advocate for stronger national or regulatory policies and business practices that promote digital public infrastructure, and (iii)

provide valuable insights and expertise on digital public infrastructure issues. Examples of these stakeholders include non-governmental organizations (NGOs), thinktanks, philanthropic organizations, etc.

- **International development organizations**: The role of international development organizations in developing digital public infrastructure is to (i) provide technical assistance to countries in developing appropriate digital public infrastructure regulations and safeguards, and (ii) provide external funding, grant and loans to scale carefully selected digital public infrastructure projects. Examples of these stakeholders include the World Bank, the United Nations Development Programme and the Gates Foundation, among others.

Figure 2. Stakeholders driving digital public infrastructure

Source: Selim and ElGohary (2020)

3.5. Public-Private Partnerships in Financing DPI

Typically, the government funds majority of the digital public infrastructure projects in high-income countries such as government's funding of national digital identity systems in Netherland, Finland, Norway, US, and Germany. The government of high-income countries

often fund digital public infrastructure projects because they have sustainable practices, robust economic structures, adequate financial resources, and advanced technologies which allows them to accelerate the development of digital public infrastructure projects. In contrast, low-income and middle-income countries do not have adequate funding to invest in the development of digital public infrastructure projects (Webber et al, 2022). They may rely on assistance from domestic sources, multilateral organizations, and philanthropic funders. Due to differences in funding capability, the most appropriate funding model for financing digital public infrastructure in low-income and middle-income countries is public-private partnership (Ma et al, 2023). This is the appropriate funding model because DPI requires significant financial resources, and the government alone cannot fund it due to the many components and systems that need to be brought together to develop a robust digital public infrastructure. Funding such digital public infrastructure will require pooling together both public sector and private sector financial resources. Public sector financial resources that can be allocated to DPI include tax revenue and budgetary allocation to digital public infrastructure projects. Private sector financial resources that can be allocated to DPI include funds from local private investors, loans from domestic financial institutions, donations from philanthropists, grants, and loans from private international financial institutions.

3.6. Global Initiatives Supporting Digital Public Infrastructure

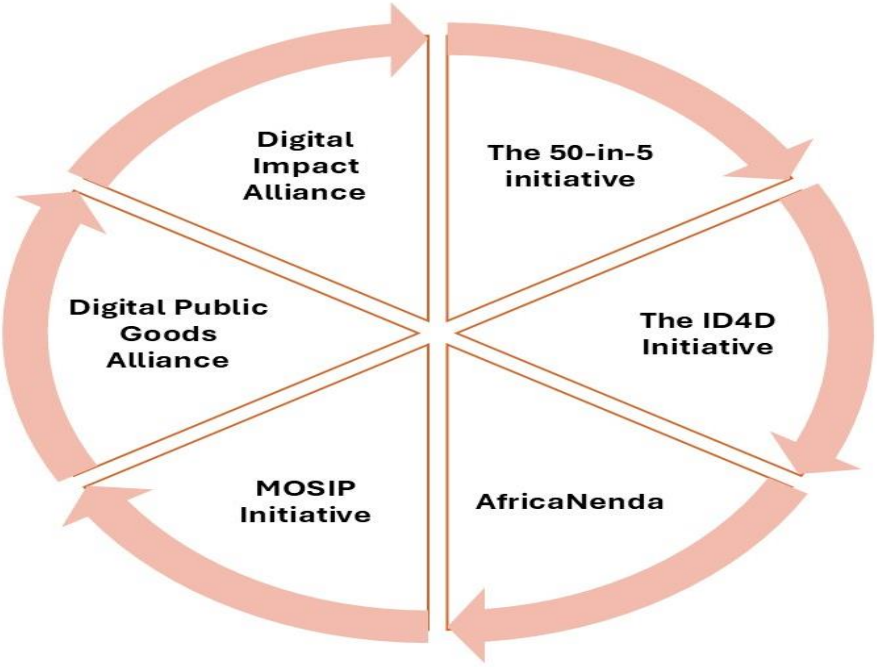
Several initiatives exist to support the creation and development of digital public infrastructure in countries around the world (see figure 3). Many of these initiatives are supported by the World Bank and the Gates Foundation. These initiatives are highlighted below.

- **The 50-in-5 initiative**: The 50-in-5 initiative is a country-led advocacy campaign which aims to implement digital public infrastructure safely and inclusively by 2028 (Duliev, 2023). It aims to help 50 countries to design, launch, and scale components of their digital public infrastructure. The 50-in-5 initiative also aims to bring countries together to share learnings, best practices, and technologies that reduce costs, build local capacity, maximize impact, and accelerate the implementation of digital public infrastructure.
- **The ID4D Initiative**: The ID4D Initiative is an initiative led by the World Bank (Musoni et al, 2023). The ID4D initiative was created to advocate for the development of

identification (ID) systems that are based on a robust set of principles, including privacy by design, security, user control, safeguarding data privacy, and protecting user rights through a comprehensive legal and regulatory framework (Musoni et al, 2023).

- **AfricaNenda**: The AfricaNenda program is a program that provides pre-project technical support and greater institutional capacity to expand and scale-up fundable, instant and inclusive payment system projects in African countries with the aim to achieve universal financial inclusion on the African continent by 2030 (Domingo et al, 2023).
- **MOSIP Initiative**: The Modular Open Source Identity Platform (MOSIP) is a university-incubated not-for-profit foundation which is supported by the Gates Foundation (Martin, 2021). MOSIP helps governments to conceive, develop, and implement effective foundational ID systems in their countries. MOSIP offers countries modular and open-source technology to build and own their national identity systems. It offers a robust, scalable, and inclusive platform on which national foundational IDs are built and configured in an efficient and cost-effective way (Martin, 2021).
- **Digital Public Goods Alliance**: The Digital Public Goods Alliance (DPGA) is a multi-stakeholder initiative that is endorsed by the United Nations. DPGA aims to accelerate the attainment of the sustainable development goals in low- and middle-income countries by facilitating the discovery, development, investment, and usage of digital public goods. DPGA facilitates the discovery and deployment of digital public goods towards a more equitable world.
- **Digital Impact Alliance**: The Digital Impact Alliance (DIA) is an initiative which aims to connect governments, funders, and development actors with the essential insights, knowledge, and tools needed to advance positive, sustainable and inclusive digital transformation. Its core objective is to connect people with evidence to build the digital tools that work for society.

Figure 3. Global Initiatives Supporting Digital Public Infrastructure



Source: Public information

4. Opportunities of digital public infrastructure

Digital public infrastructure has several benefits.

- Digital public infrastructure can facilitate the development of a vibrant and competitive economy.
- It can foster trust between governments and citizens by enabling the delivery of essential services to citizens.
- It creates economic opportunities in many industries including ICT, education, health, travel, finance, skills, and agriculture.
- **SDG benefit** – It accelerates progress toward the sustainable development goals and delivers shared prosperity for everyone especially women and people with low income (Choudhuri et al, 2021).

- **Financial inclusion benefit** – Digital public infrastructure can increase financial inclusion by enabling the private and public sector to efficiently deliver solutions to expand banking, credit, and payment services to individuals who have traditionally been left behind (D'Silva et al, 2019). For example, India uses the Aadhaar digital IDs and unified payment interface (UPI) instant payments to achieve financial inclusion.
- **Healthcare benefit** – Digital public infrastructure can increase access to healthcare and improve healthcare outcomes (Choudhuri et al, 2021). Digital public infrastructure can also unlock many services and opportunities that improve public health in rural communities.
- **Climate risk mitigation benefit** – Digital public infrastructure can enable seamless climate data sharing to identify climate risks, enable communities to proactively plan for adverse weather events, allow for faster climate change response when disaster occurs, and mitigate climate change risks.
- **Competition and innovation benefit** – Digital public infrastructure can enable private firms to innovate faster, drive competition, deliver new services to markets, and create jobs to expand economic opportunity and economic growth (Zuckerman, 2020).
- **Access to a wide range of services**: Digital public infrastructure has the potential to make it easier for individuals to receive wages, pay bills, receive government cash transfers, access essential services provided by the government, and conduct transactions safely and cheaply irrespective of income level (Zuckerman, 2020).
- **Business and entrepreneurial benefits** – Digital public infrastructure also stimulates markets by giving digital service providers equal opportunity to compete and reach new customers and markets. It allows entrepreneurs to use digital public infrastructure to innovate and launch new businesses that create jobs (Zuckerman, 2020; Henry et al, 2025).

5. DPI success and failure stories: some country cases

Few countries have witnessed some success and failure in deploying a digital public infrastructure. We discuss some success and failure stories in this section and present a summary of why some countries succeeded and why others failed in Tables 1 and 2.

- **Brazil – In 2020, the Central Bank of Brazil launched the Pix payment platform which is a type of DPI in Brazil (Sampaio and Ornelas, 2024). Pix is a new instantaneous bank-to-bank transfer payment system, and it cost only US$ 4 million to develop it while it generated a cost savings of US$ 5.7 billion in 2021 alone (Sampaio and Ornelas, 2024). Pix became very popular in Brazil. It had 149 million users and 15 million firms were using it as of December 2023 (Sampaio and Ornelas, 2024).**

- **Peru – The Yape digital payment system was launched in February 2017 by Banco de Crédito del Perú (BCP) which is the country's largest bank (Aurazo and Gasmi, 2024). Initially, Yape only allowed BCP customers to transfer funds to each other using mobile phone numbers or QR code scans. Later, Yape integrated other financial institutions to enable transactions between customers of different financial institutions. In 2023, Yape had 12 million users which represented 35% of the population of Peru and it grew to become the first "super app" in Peru. It is widely accepted as a means of payment in stores, restaurants, fast food outlets and gas stations (Aurazo and Gasmi, 2024).**

- **Singapore** – Singapore developed the Singpass which is a robust digital public infrastructure in the country (**Hoe, 2018**). The Singpass is a national digital identity ecosystem which serves as a digital infrastructure for the public and private sectors to build trusted digital services and provide opportunities for digitalisation and co-creation (Hoe, 2018). Singpass also enables individuals and businesses to access their data through a federated network of authoritative datasets (Hoe, 2018). It allows personal and corporate data to be shared after receiving explicit consent. Singpass removes the need for multiple online identities, passwords, and physical tokens, and replaces it with stronger security, authenticity mechanisms, confidentiality, and integrity for both offline and online transactions (Hoe, 2018).

- **India** – India is a trailblazer in deploying digital public infrastructure domestically. India has already developed some key elements of a digital public infrastructure. India developed the Aadhaar which is India's foundational digital identity system (Maheshwari, 2023). The Aadhaar digital identity system enables the government of India to effectively digitize government-to-person (G2P) payments (Maheshwari, 2023). As of today, Aadhaar has more than 1.365 billion users enrolled[2], which is more than 90 percent of India's population. The Aadhaar digital identity system captures each user's information in a unique 12-digit ID number. The user information in the unique number is shared using data exchange with service providers to enable services, such as bank account opening. The Aadhaar-enabled bank accounts then interoperate with the Aadhaar-enabled Payment System to authenticate the beneficiaries who are due to receive direct benefit transfers from the government before the direct benefit transfers are paid into the beneficiaries' accounts[3]. India also has another payment system known as the Aadhaar Payment Bridge system[4], which uses the Aadhaar number as a central key to send social benefits to the intended beneficiaries (Maheshwari, 2023). India also built the Unified Payment Interface (UPI) which is the payment system in India (Maheshwari, 2023). The UPI executes eight billion transactions monthly and transacts a value of USD 180 billion monthly amounting to 65 percent of India's annual GDP.

- **Kenya** – A success story from East Africa is Kenya's National Safety Net Program, commonly known as Inua Jamii. The Inua Jamii is a system that enables digitized G2P payments through DPI's three pillars (McKay et al, 2020). It is a government program that use selected payment service providers to transfer social protection benefits to beneficiaries (McKay et al, 2020). Before beneficiaries receive the payments, the payment service providers use digital identity to authenticate beneficiaries via biometric data and national ID cards. This authentication uses data exchanged

[2] https://www.microsave.net/2023/05/19/how-can-digital-public-infrastructure-improve-government-to-person-payments/
[3] https://www.dpi.global/globaldpi/aadhar
[4] https://www.npci.org.in/what-we-do/nach/faqs/banks

between Kenya's Single Registry, which unites beneficiary information from all Inua Jamii's programs and its Integrated Population Registration System (IPRS). Additionally, the registry collects beneficiaries' data during the programs, such as registration, enrolment, payments, and grievance management records (McKay et al, 2020). It serves as an intermediary between these programs and the IPRS. This system has helped the Kenyan government to disburse KES 8.54 billion (USD 62.94 million) to 1.07 million beneficiaries in January 2022.

- **Zambia** – Zambia's digital public infrastructure is exemplified in the government digitized cash-based interventions for refugees in the Meheba Refugee settlement camp in collaboration with UNHCR, UNCDF, and MSC (Abdelgawad et al, 2023). The initiative registers eligible beneficiaries with SIM cards and provide them with digital wallets and PINs (Abdelgawad et al, 2023). Their mobile numbers and digital wallets are updated in a government refugee database, called ProGres, which authenticates them before they receive payments through the digital wallets. 52 percent of the cash-based intervention payments occurred using digital wallets and the distribution time was reduced from 13 days to 2 days after the digitized CBI was implemented.

- **Estonia**[5] – The Estonian government built a compulsory national digital ID and a data sharing infrastructure called "X-Road" in its effort to develop a digital public infrastructure (Himma-Kadakas and Kõuts-Klemm, 2023). The X-Road was released in December 2001. The X-Road was first used to build the country's population registry. Afterwards, government institutions and private institutions in Estonia began to connect their information systems and registries into the X-Road infrastructure (Himma-Kadakas and Kõuts-Klemm, 2023). X-Road connects different information systems, transmit large data sets, and perform searches across several information systems simultaneously. As of today, the X-Road infrastructure connects more than 900 public and private organisations, and it provides more than 3,000 services and with more than 11 billion requests made to date. Estonia's X-Road digital

[5] https://www.orfonline.org/expert-speak/development-and-promotion-of-digital-public-infrastructures

infrastructure has enabled the government to provide 99 percent of public services online.

- **Ethiopia** – Ethiopia uses the Fayda system as its National Digital ID System (Musoni et al, 2023). The Fayda system is a digital public infrastructure that digitally record the identity of every Ethiopian resident (Musoni et al, 2023). Every resident in Ethiopia is required to have a Fayda number before they can obtain a taxpayer identification number so that each new taxpayer identification number (TIN) created is connected to a Fayda number (Musoni et al, 2023).

	Table 1. Some DPI Success Stories				
Region	**Country**	**Type of DPI**	**Intended purpose**	**Operationalised by who?**	**Why it was a success**
Latin America	Brazil	Pix payment platform – centralized digital payment system	Pix was created in 2020 to be an instant payment system in Brazil. It allows users to send and receive money between bank accounts.	Central Bank of Brazil (BCB)	1) High acceptance rate among most businesses in Brazil; 2) enables transactions to occur in less than 10 seconds, 24 hours a day, 7 days a week; 3) reduces reliance on credit, 4) eliminates the need for cash; 5) enables unbanked individuals to participate in the digital economy, ensuring financial inclusion; 6) it has robust security features with two-factor authentication and encryption to protect user data.
Asia	Singapore	Singpass – a national digital identity ecosystem	Singapore developed the Singpass in 2003. It allows public and private sector innovators to build trusted digital services around Singpass and provide opportunities for digitalisation and co-creation.	The Government Technology Agency of Singapore	It allows personal and corporate data to be shared after receiving explicit consent. Singpass removes the need for multiple online identities, and replaces it with a stronger security and authenticity mechanisms.
Africa	Ethiopia	Fayda system – a National Digital ID System.	The Fayda system, developed in 2023, is a digital identity public infrastructure that digitally record the identity of every Ethiopian	The National ID Program (NIDP) is the agency that issues the Fayda digital ID system in Ethiopia.	1) It is widely accepted and used as a valid proof of legal identity in Ethiopia; 2) having a Fayda number is a requirement to have a taxpayer identification number which, in turn, gives Ethiopians access to shared public and private services.
Europe	Estonia	X-Road – a compulsory data-exchange or data-sharing infrastructure	X-road was founded in 2000. It was designed to facilitate secure sharing of data	Estonia's Information System Authority	It is the pillar of Estonia's digital society because it provides a wide range of e-government services, such as online tax filing, e-voting, and digital ID. Many Estonian residents,

			among government agencies so that citizens will not need to create new identities to access different types of public services.		businesses and public institutions use it to access services seamlessly
Australia & Oceania	Australia	The New Payments Platform (NNP) – a robust digital payments infrastructure	The New Payments Platform is Australia's national fast payments infrastructure. It was launched in 2018 to facilitate data-rich, real-time payments.	The NPP was developed via industry collaboration	1). It offers customers benefits in terms of greater convenience, more visibility and control over payment arrangements and the ability to more easily move bank accounts between providers. 2) It initiates payments in a safe and secure manner with appropriate controls to ensure ongoing protection of consumers and effective risk management.

-

Table 2. DPI Failure Stories

Country	Type of DPI	Intended purpose	Operationalized by who?	Why it failed
United Kingdom	Gov.UK Verify – an identity assurance system	Verify was an identity assurance system. It was operational between 2016 and 2023. It provided a secure way to prove one's identity online in the UK. Once an individual's identity has been proved, the individual could use the same identity to access other public services. The verify system was designed to provide a single trusted login across all British government digital services. It could verify a user's identity in 15 minutes.	UK government in partnership with private companies which the government had approved to verify identities.	1) The success rate in verifying individuals was 47% as of October 2018. 2) Verify does not meet all the identity requirements of government departments, such as identifying intermediaries or businesses. 3) The UK government was reluctant to continue funding the Verify project after it had already spent up to £130 million in developing GOV.UK Verify as of October 2018. 4) Government departments began to discontinue using Verify. 5) Verify was discontinued.
Kenya	Huduma Namba – a Kenyan government digital identity program	Huduma Namba was launched in 2019 to be the National Integrated Identity Management System (NIIMS) in Kenya. Under the program, a unique personal identification number is assigned to	Kenyan government	It failed because (i) the government did not conduct proper public sensitization; (ii) the political atmosphere at the time of the launch was hostile and it created room for suspicions, therefore, legislators did not urge their constituents to accept it; (iii) it became

		every citizen at birth or upon registration / enrollment. A card bearing a person's digital identity is issued to every citizen. The card will enable individuals to access various government services, and it acts as a travel document within the East African region.		unpopular due to lack of political support for the program.

6. Challenges of digital public infrastructure

In the previous section (table 2 precisely), it was shown that DPIs that are developed and implemented with good intentions can fail due to political factors, financial constraints and other reasons. This points to the challenges associated with DPI. The challenges associated with digital public infrastructure are diverse. Some of the challenges are highlighted and discussed below.

- **Difficulty in evaluating impact**: A major challenge of digital public infrastructure is not its design or adoption. The major challenge of digital public infrastructure is how to measure its real impact (Choudhuri et al, 2021). Presently, there is no universal way to rigorously evaluate the impact of digital public infrastructure. There are no standardized metrics to determine: (i) user adoption rates, (ii) the efficiency of service delivery, (iii) the adequate number of safeguards to introduce in a digital public infrastructure, and (iv) the economic impact of digital public infrastructure initiatives on individuals, firms, governments, and international development organizations.
- **Cybersecurity Risks**: Another challenge is cybersecurity risks. Digital public infrastructure, just like new technologies, may have deficient safeguards that increase users' vulnerability to data privacy violation and other breaches (Choudhuri et al, 2021; Eke and Stahl, 2024).
- **Lack of interoperability between digital systems**: Different government departments and agencies use digital systems that are not interoperable with existing digital systems (Campmas et al, 2022). Continuous efforts should be made to ensure

seamless integration of existing systems with one another to provide a seamless experience for users.

- **Digital exclusion, illiteracy and lack of trust in digital systems**: Another challenge of DPI is the low level of digital inclusion, low level of digital literacy, low level of digital financial inclusion and low level of trust in digital systems in many jurisdictions (Coyle et al, 2023). People who lack trust in digital systems, and people who lack digital identification cannot use digital public infrastructure to improve their welfare (Bodó and Janssen, 2022).
- **Lack of private and public sector collaboration:** Another challenge is difficulty in collaboration. Collaborating with the private and public sectors is not straightforward (Charalabidis et al, 2011). There may be resistance to collaboration among government entities due to differences in statutory mandates. There may also be resistance to collaboration among private firms who are rivals.
- **Lack of accountability mechanisms:** Accountability framework for digital public infrastructure does not exist in some countries. In countries where it exists, the existing accountability framework may be too weak to ensure proper investigation, remediation, and corrective measures to mitigate harm caused by unethical and irresponsible use of digital public infrastructure (Saldanha et al, 2022).
- **Algorithmic biases** – The algorithm used to operationalize DPIs may contain systematic and repeatable errors that create unfair and discriminatory outcomes, such as granting a group of people greater access to certain services over others.
- **Ethical dilemmas –** As DPI becomes ubiquitous in digital societies, there will be underlying tensions between granting people access to public goods and services and using their unconsented data for DPI surveillance and monitoring purposes. Operators of DPI will constantly find ways to navigate the tightrope between digital access for customers and obtaining access to customer data to gain insights that can be used to improve the DPI system.
- **Geopolitical concerns –** As countries compete to develop and deploy DPI systems, they will also need to navigate possible geopolitical bottlenecks in the DPI value chain that constrain access to cross border talent, data, and infrastructure that are needed to maintain DPI systems. Geopolitical conflicts such as export control, tariffs and

sanctions, can slowdown or prevent the movement of DPI-related cross border talent, data, and infrastructure from advanced countries to developing countries.

7. Conclusion

This study explored the concept of digital public infrastructure, the global trends, opportunities and challenges. The study contributes to existing literature that examines the role of digital technologies in building good digital societies and resilient digital economies by showing that digital public infrastructure can play a significant role in building a good digital society and a resilient digital economy.

The study showed that digital public infrastructure is gaining momentum globally as a transformative force in developing a resilient digital economy and a good digital society. It was shown that a digital public infrastructure is the foundation upon which robust digital societies are built. Once the core elements of a digital public infrastructure are put in place – which are digital identity systems, digital payment systems, data exchange and integration systems, consent networks, credentials, registries, digital signatures, and national digital strategies – it will be possible to build a digital public infrastructure that (i) enable public, private, and civil society innovation, (ii) create a platform to connect people to access digital services, and (iii) deliver digital services that benefit everyone and put people at the centre. As more people globally connect to existing digital public infrastructures, governments, communities, and private sector organizations will have the opportunity to harness the power of digital connectivity to improve people's quality of life. It can improve access to education, access to healthcare, uplift people out of poverty, stimulate innovation, encourage competition in physical and digital markets, and increase digital and financial inclusion.

The implication of the findings is that, as the advocacy for creating a digital public infrastructure increase, countries will have to decide whether they want to build a digital public infrastructure from scratch and how to build it, or whether they want to leverage on the existing siloed digital technology infrastructure that are used locally to deliver proven public goods. Even if countries were to build a digital public infrastructure from scratch, there is no set way to build a digital public infrastructure.

It is recommended that policymakers should lay out a comprehensive strategy on how to build interoperable identity, payment, and data exchange systems that will be successful. Furthermore, policymakers need to decide on who should build the digital public infrastructure. Should the government build it alone? Or should the government and the private sector build it together? While the answer is not straightforward, it would seem more likely that government entities and private sector firms may need to work together to develop the foundational layers for a digital public infrastructure. After developing the foundational layers, the private sector should be allowed to build a stack of innovative solutions around the foundational digital public infrastructure that has been created.

For the built digital public infrastructure to succeed, policymakers should ensure that certain safeguards are in place to prevent bad actors from using digital public infrastructures to steal identities and commit fraud. Technical safeguards should be introduced to prevent non-state actors from gaining unauthorized access to digital public infrastructure systems to steal personal data. Also, strong cybersecurity laws, policies and regulations should be developed to protect the privacy rights of individuals. Efforts should also be made to build accountability frameworks that provide checks and balances to ensure that digital public infrastructure continues to serve the public good.

Regarding the future of DPI, the future of digital public infrastructure remains bright because emerging technological advancements such as AI, the internet of things, and blockchain advancements can accelerate the development of digital public infrastructure by increasing the efficiency, reach, and impact of public services and public initiatives on people (Verdecchia et al, 2022; Janssen et al, 2009). These emerging technological advancements can lead us to a future where digital public infrastructure will be a cornerstone to foster digital inclusion, financial inclusion, economic growth, poverty reduction, job creation, quality digital education and improved healthcare (Henry et al, 2025). In the future, digital public infrastructure will immensely improve public governance and enhance public service delivery (Eaves et al, 2024).

Finally, the discussion in this article provide several avenues for future research. Future research can provide insight into the regulation of digital public infrastructure and offer deep insight into how regulation would affect access and freedom to innovate for entrepreneurs. Future research can also examine the technological and institutional capacity to build a fully

operational digital public infrastructure in developing countries given their limited economic, financial, and technological resources.

Reference

Abdelgawad, A. A., Khan, A., & Baharmand, H. (2023). Exploring gaps in using digital delivery mechanisms for cash-based assistance in refugee crises. *International Journal of Disaster Risk Reduction*, 96, 103907.

Aurazo, J., & Gasmi, F. (2024). Digital payment systems in emerging economies: Lessons from Kenya, India, Brazil, and Peru. *Information Economics and Policy*, *69*, 101113.

Ayodele, O. Digital infrastructure: creating the backbone for development. In The Quest for Unity (pp. 403-426). Routledge.

Bentley, S. V., Naughtin, C. K., McGrath, M. J., Irons, J. L., & Cooper, P. S. (2024). The digital divide in action: how experiences of digital technology shape future relationships with artificial intelligence. *AI and Ethics*, *4*(4), 901-915.

Brands, S. (2000). *Rethinking public key infrastructures and digital certificates: building in privacy*. MIT Press, Cambridge, Massachusetts.

Bodó, B., & Janssen, H. (2022). Maintaining trust in a technologized public sector. *Policy and Society*, *41*(3), 414-429.

Campmas, A., Iacob, N., & Simonelli, F. (2022). How can interoperability stimulate the use of digital public services? An analysis of national interoperability frameworks and e-Government in the European Union. *Data & Policy*, *4*, 19, 1-24.

Charalabidis, Y., Koussouris, S., & Ramfos, A. (2011, November). A cloud infrastructure for collaborative digital public services. In *2011 IEEE Third International Conference on Cloud Computing Technology and Science* (pp. 340-347). IEEE.

Choudhuri, B., Srivastava, P. R., Gupta, S., Kumar, A., & Bag, S. (2021). Determinants of smart digital infrastructure diffusion for urban public services. *Journal of Global Information Management (JGIM)*, *29*(6), 1-27.

Clarke, A. (2020). Digital government units: what are they, and what do they mean for digital era public management renewal?. *International Public Management Journal*, 23(3), 358-379.

Coyle, D., Diepeveen, S., & Deshmukh, S. (2023). Digital Public Infrastructure: Mitigating New Forms of Exclusion to Enable Tech for All. *T20 Policy Briefs.*

Cross, C. (2022). Meeting the challenges of fraud in a digital world. In *The handbook of security* (pp. 217-238). Springer International Publishing, Cham.

Dahlman, C., Mealy, S., & Wermelinger, M. (2016). Harnessing the digital economy for developing countries. *OECD Development Centre Working Paper No. 334*

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). Technology acceptance model. J Manag Sci, 35(8), 982-1003.

Domingo, E., Arnold, S., & Apiko, P. (2023). Interoperability of digital payment systems: Lessons from the East African Community. *ECDPM Discussion Paper No. 357.*

D'Silva, D., Filková, Z., Packer, F., & Tiwari, S. (2019). The design of digital financial infrastructure: lessons from India. *BIS Paper*, 106.

Duliev, A. (2023). World Bank's Digital public infrastructure (DPI) initiative.

Eaves, D., Mazzucato, M., & Vasconcellos, B. (2024). Digital public infrastructure and public value: What is 'public'about DPI. *UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024-05). London: UCL Institute for Innovation and Public Purpose. Retrieved March*, *28*, 2024.

Eke, D., & Stahl, B. (2024). Ethics in the governance of data and digital technology: An analysis of European data regulations and policies. *Digital Society*, *3*(1), 11.

Finger, M., & Montero, J. (2022). The digitalisation of infrastructure and infrastructure-based (public) services: what are the problems?. *Network Industries Quarterly*, 24, 1.

Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society*, *2*(2), 18.

Goldsmith, S., & Gardner, E. (2022). Implementing Digital Infrastructure Responses to Equity, Sustainability, and Safety. *Data-Smart City Solutions Papers*.

Guo, B., Hu, P., & Lin, J. (2024). The effect of digital infrastructure development on enterprise green transformation. *International Review of Financial Analysis*, 92, 103085.

Hanna, T. M., Lawrence, M., Buller, A., & Brett, M. (2020). Democratic digital infrastructure. Building a 21st Century network in the UK and US. Accesible en: https://www. common-wealth. co. uk/reports/democratic-digitalinfrastructure (consultado el 20 de julio de 2020).

Hardy, A. (2024). Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance. *Internet Policy Review*, *13*(3), 1-31.

Henry, G., Benson, O. G., Kazemi, F., & Palova, K. (2025). Digital Information Platforms and Support for Immigrant Professionals' Employment and Settlement: An Integrative Review. *Digital Society*, *4*(1), 14.

Himma-Kadakas, M., & Kõuts-Klemm, R. (2023). Developing an Advanced Digital Society: An Estonian Case Study. In *Internet in the Post-Soviet Area: Technological, Economic and Political Aspects* (pp. 109-133). Springer International Publishing, Cham.

Hobson, T., France, L., Greenbury, S., Hare, L., & Wochner, P. (2023). Trustchain–trustworthy decentralised public key infrastructure for digital credentials. eprint arXiv:2305.08533.

Hodapp, D., & Hanelt, A. (2022). Interoperability in the era of digital innovation: An information systems research agenda. *Journal of Information Technology*, *37*(4), 407-427.

Hoe, S. L. (2018). Building a smart nation: Singapore's digital journey. *Asian Research Policy*, *9*(1), 86-95.

Holmes, H., & Burgess, G. (2022). Digital exclusion and poverty in the UK: How structural inequality shapes experiences of getting online. *Digital Geography and Society*, *3*, 100041.

Hustad, E., & Olsen, D. H. (2021). Creating a sustainable digital infrastructure: The role of service-oriented architecture. *Procedia Computer Science*, 181, 597-604.

Janssen, M., Chun, S. A., & Gil-Garcia, J. R. (2009). Building the next generation of digital government infrastructures. *Government Information Quarterly*, *26*(2), 233-237.

Kumar, P. (2020). Cash transfers during COVID-19 pandemic and roadmap to universal basic income. *Journal of Governance & Public Policy*, *10*(2), 81-101.

Liu, Y., Liu, K., Zhang, X., & Guo, Q. (2024). Does digital infrastructure improve public Health? A quasi-natural experiment based on China's Broadband policy. *Social Science & Medicine*, 344, 116624.

Lythreatis, S., Singh, S. K., & El-Kassar, A. N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, *175*, 121359.

Ma, L., Christensen, T., & Zheng, Y. (2023). Government technological capacity and public–private partnerships regarding digital service delivery: Evidence from Chinese cities. *International Review of Administrative Sciences*, *89*(1), 95-111.

Maheshwari, A. (2023). Digital Public Infrastructure in India. *Global Media Journal*, *21*(63), 1-3.

Martin, A. (2021). Aadhaar in a box? Legitimizing digital identity in times of crisis. *Surveillance & Society*, *19*(1), 104-108.

McIntosh, D. (2018). We need to talk about data: How digital monopolies arise and why they have power and influence. *J. Tech. L. & Pol'y*, *23*, 185.

McKay, C., Mdluli, G., Chebii, M., & Malu, V. (2020). The future of government-to-person (G2P) payments: Innovating for customer choice in Kenya. *CGAP and FSD Kenya*.

Musoni, M., Domingo, E., & Ogah, E. (2023). Digital ID systems in Africa: Challenges, risks and opportunities. *ECDPM Discussion Paper No. 360.*

Nagar, S., & Eaves, D. (2024). Interactions Between Artificial Intelligence and Digital Public Infrastructure: Concepts, Benefits, and Challenges. *arXiv preprint arXiv:2412.05761*.

Ozili, P. K. (2021). Covid-19 pandemic and economic crisis: The Nigerian experience and structural causes. *Journal of Economic and Administrative Sciences*, *37*(4), 401-418.

Ozili, P. (2025). Digital markets: formative components, regulation, challenges and insights from the European Union Digital Markets Act. *Digital Policy, Regulation and Governance*.

Rabe, W., & Kostka, G. (2024). Perceptions of social credit systems in Southeast Asia: An external technology acceptance model. *Global Policy*, 15, 314–328.

Rukanova, B., Van Engelenburg, S., Ubacht, J., Tan, Y. H., Geurts, M., Sies, M., ... & Van Dijk, D. (2023). Public value creation through voluntary business to government information sharing enabled by digital infrastructure innovations: a framework for analysis. *Government Information Quarterly*, *40*(2), 101786.

Saldanha, D. M. F., Dias, C. N., & Guillaumon, S. (2022). Transparency and accountability in digital public services: Learning from the Brazilian cases. *Government Information Quarterly*, *39*(2), 101680.

Sampaio, M. C., & Ornelas, J. R. H. (2024). Payment Technology Complementarities and their Consequences in the Banking Sector: evidence from Brazil's Pix. *Faster digital payments: global and regional perspectives*, 17.

Schmidthuber, L., Maresch, D., & Ginner, M. (2020). Disruptive technologies and abundance in the service sector-toward a refined technology acceptance model. *Technological Forecasting and Social Change*, 155, 119328.

Selim, A. M., & ElGohary, A. S. (2020). Public–private partnerships (PPPs) in smart infrastructure projects: the role of stakeholders. *HBRC journal*, *16*(1), 317-333.

Singh, N. K., Sahu, G. P., Rana, N. P., Patil, P. P., & Gupta, B. (2019). Critical success factors of the digital payment infrastructure for developing economies. In *Smart Working, Living and Organising: IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2018, Portsmouth, UK, June 25, 2018, Proceedings* (pp. 113-125). Springer International Publishing.

Tang, K., & Yang, G. (2023). Does digital infrastructure cut carbon emissions in Chinese cities?. *Sustainable Production and Consumption*, 35, 431-443.

Tang, J., & Zhao, X. (2023). Does the new digital infrastructure improve total factor productivity?. *Bulletin of Economic Research*, 75(4), 895-916.

Verdecchia, R., Lago, P., & De Vries, C. (2022). The future of sustainable digital infrastructures: A landscape of solutions, adoption factors, impediments, open problems, and scenarios. *Sustainable Computing: Informatics and Systems*, *35*, 100767.

Webber, D., Hughes, E., Pacheco, G., & Parry, G. (2022). Investment in digital infrastructure: Why and for whom?. *Region*, *9*(1), 147-163.

Williams, F., Philip, L., Farrington, J., & Fairhurst, G. (2016). 'Digital by Default'and the 'hard to reach': Exploring solutions to digital exclusion in remote rural areas. *Local Economy*, *31*(7), 757-777.

Zhuang, K. V., Choo, B., Gerard, G., Lee, C. S., Tan, F., & Llamzon, R. (2025). Towards Inclusive Digital Transactions: Disability and The Case of Singapore's Singpass App. ICIS 2024 Proceedings. 20.

Zhou, A. (2022). Digital infrastructure and economic growth—Evidence for China. *Journal of Infrastructure, Policy and Development*, 6(1), 1-13.

Zuckerman, E. (2020). What is digital public infrastructure?. The Center for Journalism and Liberty. A Part of the Open Markets Institute. November.

Zukis, B. (2016). Information technology and cybersecurity governance in a digital world. *The Handbook of Board Governance: A Comprehensive Guide for Public, Private and Not-for-Profit Board Members*, 555-573.