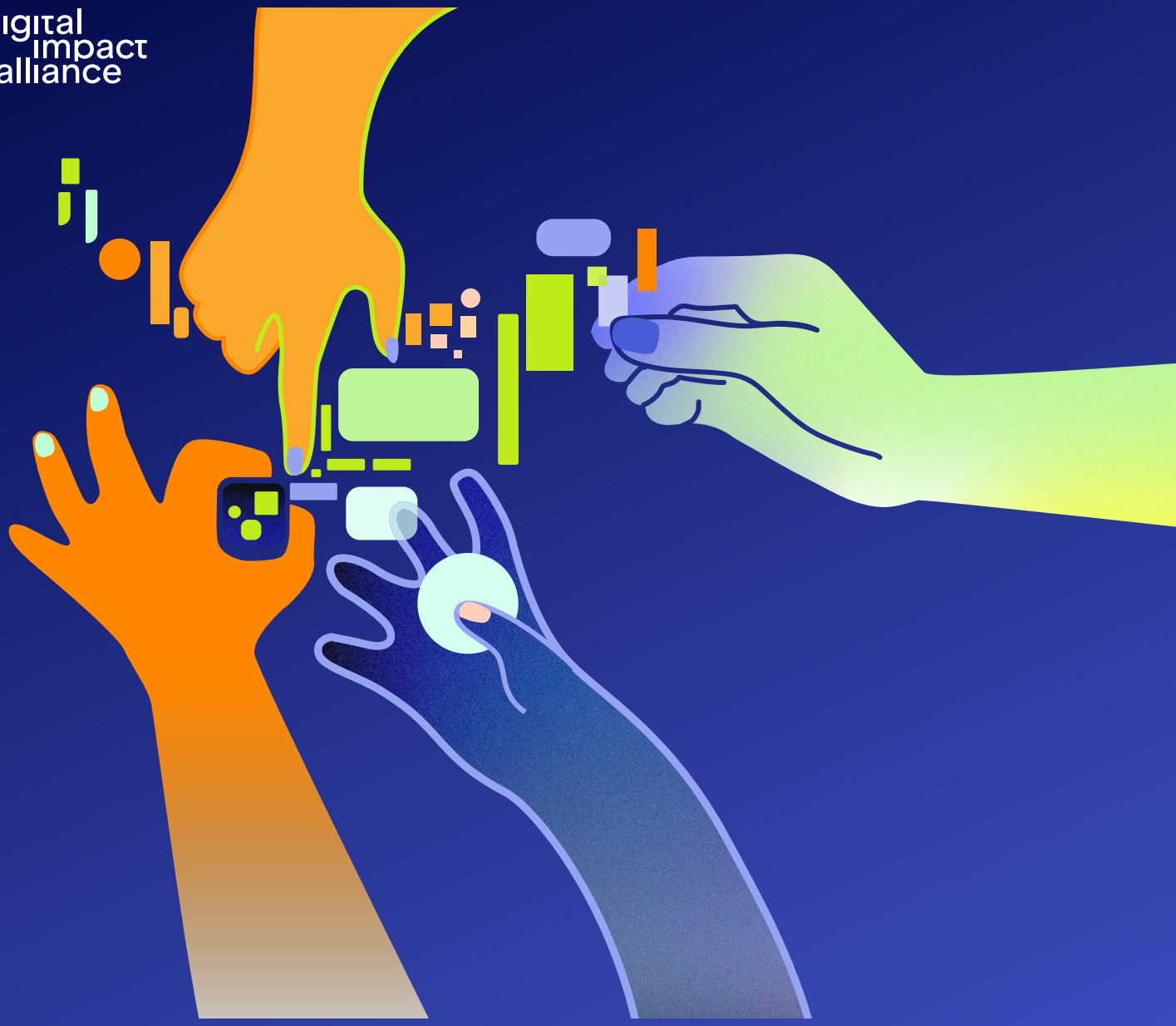
digital impact alliance



Co-Creating Our Digital Future

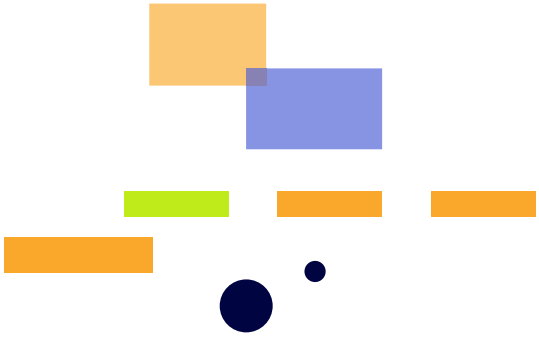
How open-source technology can expand inclusive digital public infrastructure

Chrissy Meier and Heath Arensen

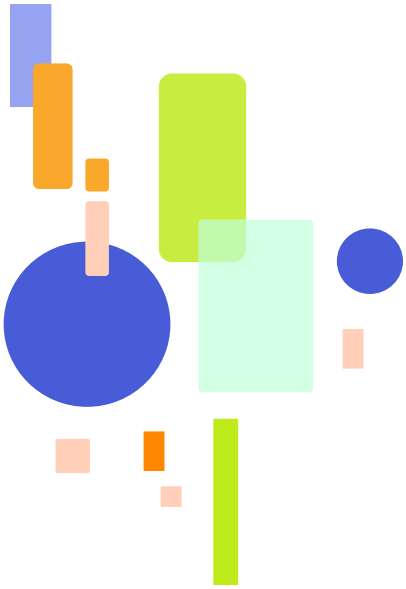
April 2023

SECTION 1

Introduction



After years of working on digital transformation to advance the Sustainable Development Goals (SDGs), the Digital Impact Alliance (DIAL) recognizes that the next seven years (2023 to 2030) present a unique window of opportunity for expanding safe, inclusive, and trusted foundational digital public infrastructure (DPI). This moment arises from the growing political consensus regarding the need for DPI, as demonstrated by the UN Secretary-General's High-Level Expert Panel on Digital Cooperation convened in 2018, the launch of the Digital Public Goods Alliance (DPGA) in 2019, the Charter for Digital Public Goods **(DPG Charter)** drafted in 2022, India's focus on DPI during its G20 presidency in 2023, and the forthcoming Global Digital Compact, to be agreed upon in September 2024.



This paper seeks to help the global community take advantage of this window of opportunity by presenting insights from DIAL's years of working with governments and partners on digital transformation. From this experience, we offer three overarching insights:

1. It is necessary to focus on *foundational* digital public infrastructure in order to effectively drive individual empowerment and private-sector innovation.

2. Digital public goods (DPGs) can help overcome many of the current challenges associated with developing foundational digital public infrastructure.

3. The conditions required for digital public goods to be a viable, long-term option for digital public infrastructure will not emerge organically.

We do not expect that all countries will implement DPGs in all cases. However, we do see a number of benefits of DPGs that are leading governments to choose these open-source products (see Section III). To support this decision and maximize the benefits of DPGs, we present five outcomes that, when accomplished through coordinated efforts, will create an ecosystem (see Image 1) that offers a full suite of sustainable digital public goods that supports countries and regions as they design, deploy, and maintain their own unique, safe, and inclusive digital systems (see Section IV). We conclude with recommendations that provide a way forward from the current state of play (see Section V).

This analysis is based on desk research, DIAL's experience with the Open Source Center (OSC), and consultations with various partners to inform the DPG Charter.

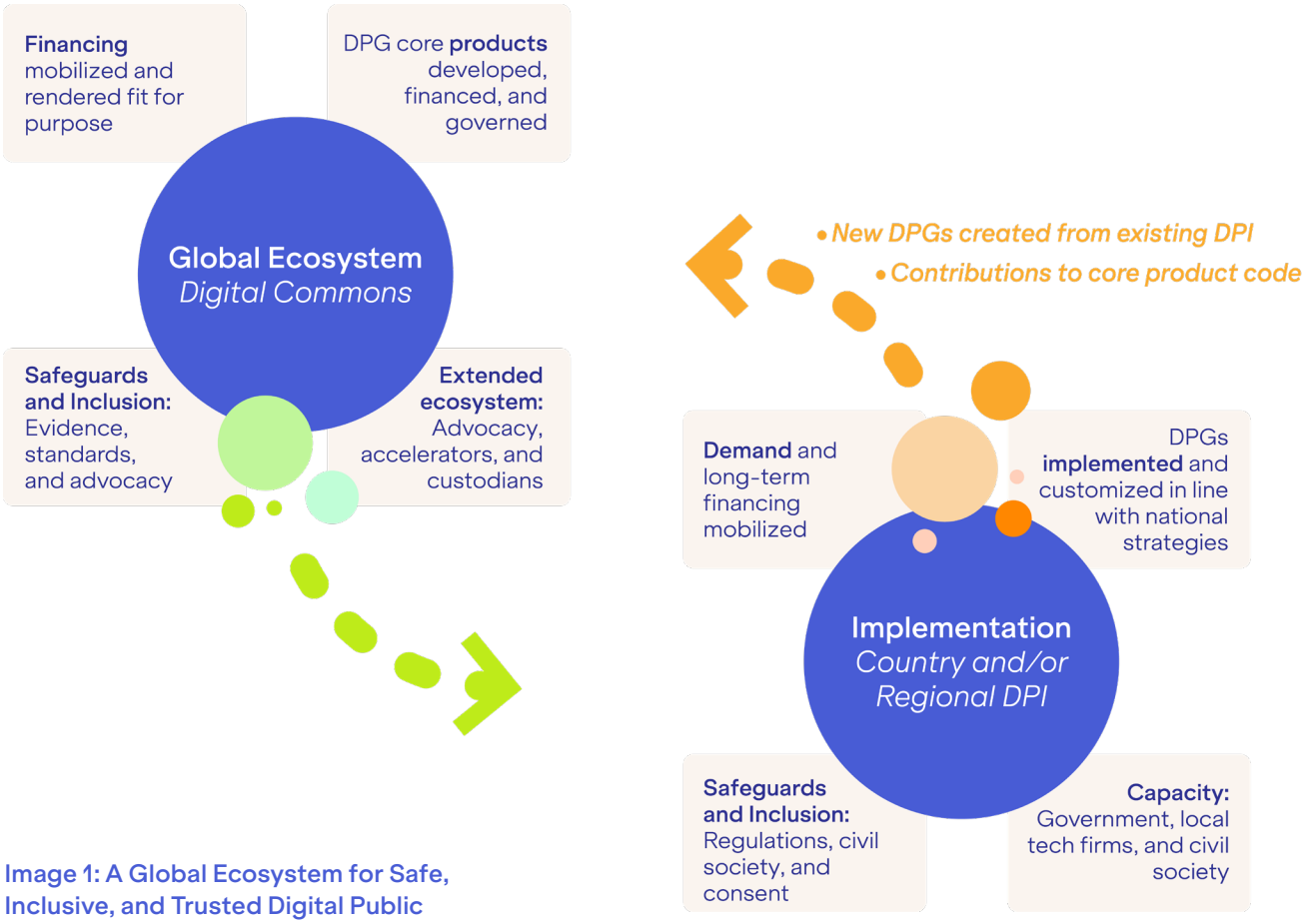
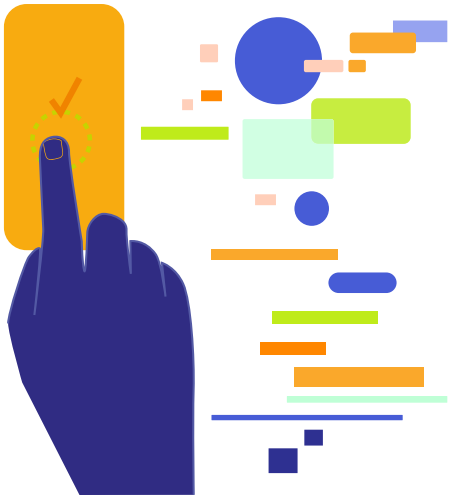


Image 1: A Global Ecosystem for Safe, Inclusive, and Trusted Digital Public Infrastructure Supported by Digital Public Goods. Source: Authors' interpretation based on existing available research

SECTION 2

Focus on *Foundational* Digital Public Infrastructure

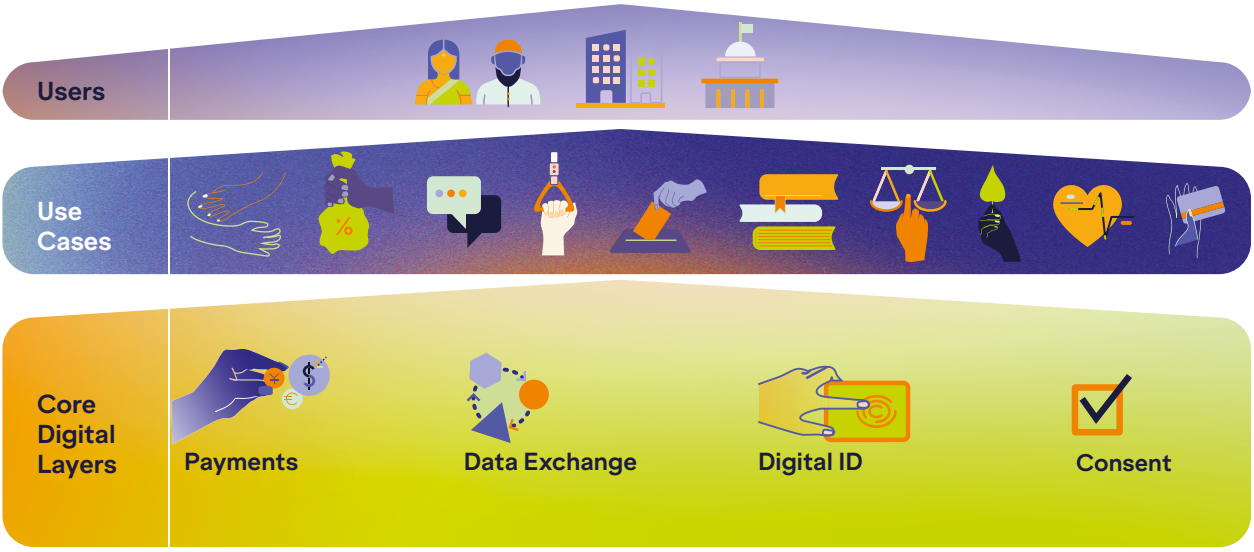


Digital public infrastructure refers to platforms such as identification (ID), payment, and data exchange systems that help countries deliver vital services to their people.[1] At its best, this infrastructure not only improves the delivery of government services, it enables civic participation, powers private-sector innovation, and enables more effective regional cooperation, increasing the potential positive impact on individuals and communities.

Some governments have invested heavily in digitization over the past decade, motivated in large part by the desire to lower the cost-of-service delivery. We are now seeing concrete results in terms of time and cost savings, both for governments and people.[2]

These initial results demonstrated that digitization has the potential to drive impact beyond time and cost savings, including building pathways to financial inclusion, women's economic empowerment, private-sector innovation, food security, and more.

Image x: Digital Public Infrastructure (Core Digital Layers) Provides the Foundations of a Digital Stack That Can Empower People, Businesses, and Communities. *Digital Impact Alliance (2022)*



What is the difference between digitization for the sake of efficiency and digital public infrastructure that drives long-term, positive, whole-of-society impact? We argue that the difference comes from taking a *foundational* approach to digital public infrastructure. This starts with digital systems that are whole-of-society, interoperable, and designed for the public good.

- **When digital public infrastructure is whole-of-society** various government ministries, private sector companies, civil society and community groups departments can leverage it. Upfront investment in this type of approach is expensive and requires extensive change management. Over the long term, however, costs are lowered as a larger number of operational units are able to take advantage of the initial investment.

- **When digital public infrastructure is *interoperable*,** there are agreed upon standards in place to enable government systems to communicate with each other through real-time data sharing. This allows a government to benefit from any number of **building blocks**—interoperable software code, platforms, and applications—that can be reused and adapted depending on needs. Both open-source and proprietary systems are able to support this level of interoperability. Interoperability is a key ingredient for countries, companies, and individuals to realize the benefits of the data economy.

- **When digital public infrastructure is designed for the *public good*,** there are safeguards in place to promote accountability, prevent misuse by either government or business, and deliver value to all individuals and communities, including women and other historically marginalized groups. Without proper safeguards in place, any investment in digital public infrastructure risks doing more harm than good.

Yet, despite the clear benefits, few countries have managed to put in place truly foundational digital public infrastructure. Why? We see three key, although not exhaustive, explanations.

1. **Legacy and proprietary digital government systems are not easily adapted to a *foundational* approach:** Many software systems that are currently used for digital public infrastructure are quite expensive and limited in their flexibility to adapt to change over time. A foundational approach requires working across ministries and departments to design and implement a whole-of-government approach; allowing for the procurement of interoperable technology from both open-source and proprietary vendors; and overcoming vendor lock-in that keeps governments tied to existing, often outdated, technology.

2. **The upfront costs associated with this approach are high, and there is insufficient funding available:** Despite the growing consensus that cross-cutting approaches to digital infrastructure are the most effective, donor and government funds are still largely tied to sectors such as health, education, and agriculture. This is due to a variety of factors, including domestic politics and the slow nature of bureaucratic change. It's worth noting that over time, costs should be lower with an interoperable, foundational system in place, since it is easier and less expensive to replace or add new building blocks as needs change.

3. **Governments may be motivated to invest in and use digital systems for reasons *counter* to the public good:** Digital systems can be used to empower, but they can also be used to suppress. Government, nonstate, and foreign actors can all use digital technology to accelerate their use of the five tactics of digital repression: mass surveillance, targeted persecution, internet shutdowns, censorship, and disinformation.[3] Thus, efforts to build foundational digital public infrastructure for the public good are challenged to find ways to mitigate these risks, which look different in each country depending on complex political, social, and economic factors.

SECTION 2

Leverage DPGs Where Appropriate to Overcome Current Obstacles to Developing Foundational Digital Public Infrastructure

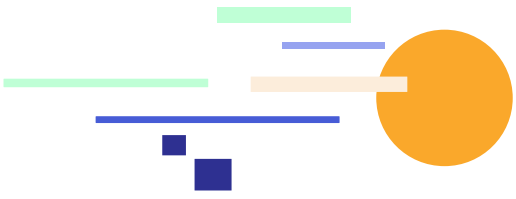
From its start in 2015, DIAL saw an opportunity to reduce duplication and increase the impact of digital development funding by improving the market for open-source technology. In 2018, DIAL set up the Open Source Center, which provides technical assistance consulting for open-source projects to strengthen their community governance and long-term financial viability. Through this hands-on work with open-source clients, DIAL gathered nuanced and critical understanding of how to invest in and govern shared technology in the international development context, and more broadly at a societal level.[4]

This shared technology—referred to in this context as digital public goods—can make it easier to implement foundational digital public infrastructure. Why?

1. **Digital public goods can be designed as reusable shared building blocks, which facilitates a foundational approach.** Due to their open licensing, digital public goods eliminate the cost of duplicating basic infrastructure in each country. These benefits are not always clear in the short run, since a well-funded government will benefit similarly from a technology regardless of the licensing. However, these benefits become quite clear in the long run and when countries with less resources look to develop their own digital public infrastructure. As a recent academic paper described this,

"Imagine a technology company developing a system that helps a city optimize traffic control in order to reduce greenhouse gas emissions. The city benefits from the improved mobility management by reducing air pollution. However, governments in low- and middle-income countries might be unable to purchase licenses of this smart software and, therefore, cannot combat inefficient traffic. Thus, the positive effect of this smart but proprietary digital technology on the green transition is limited. Important public sector institutions are excluded to benefit from digital transformation due to intellectual property laws."[5]

Furthermore, a building block approach, such as that championed by the GovStack initiative, helps overcome obstacles to a whole-of-society approach by building digital public infrastructure using reusable software components that form the foundation of a multitude of e-government services.[6] For example, when Ukraine implemented its Platform of Registries using a building block approach, it lowered the cost for one ministry to create a new registry by 90%.[7]



2. **Digital public goods can drive cost savings by promoting reuse and lowering the risk of vendor lock-in.** Governments spend $151.8 billion in software and $203.9 billion annually in information technology services, thus making the potential cost savings quite relevant for cash-strapped countries.[8] These costs are simply impossible for many countries to sustain, and thus are leading countries to look to open-source technology and protocols to drive both procuring and sustaining digital public infrastructure.

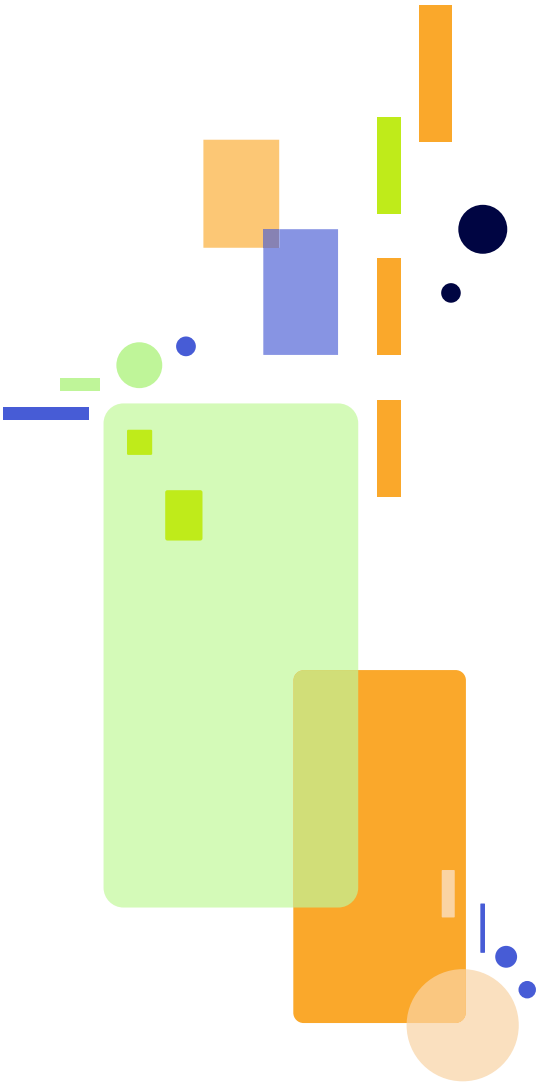
   Open-source technology is already delivering on this promise for some countries. For example, many municipalities in Brazil switched to open-source software in the early 2000s because "estimates at the time concluded that across the country, nearly USD 200 million per year was spent on licensing fees to Microsoft alone and, by switching, USD 120 million could be saved."[9] In India, switching primary and secondary schools' digital solutions to open-source software reduced costs by USD 1.3 billion.[10]

   The high ongoing costs associated with proprietary software has led to vendor lock-in, a situation in which a user is forced to pay high prices and stick with a technology that does not meet their needs due to contracts and the lack of data portability. According to a survey by ID4Africa in 2018, vendor lock-in is the largest concern among national identity authorities in Africa.[11] While open-source technology does not inherently overcome vendor lock-in, it has the potential to do so when properly financed and supported by a competitive market of vendors.[12]

   By making source code freely available to customize and use, digital public goods allow governments to ensure that software meets local needs. Furthermore, local private-sector companies have the chance to become *systems integrators*—the technical services providers that implement and maintain technology systems. As a result, governments can align digital government efforts with efforts to invest in the local digital workforce.

   "Digital public goods provide an opportunity for Sierra Leone and our peers to move from being buyers to creators," says Bineta Diop, Directorate of Science, Technology and Innovation, Sierra Leone.

3. **Digital public goods help empower, rather than suppress, through a commitment to *do no harm* by design.** While technology alone will never be able to prevent government overreach and repression, DPGs do offer a number of advantages in preventing harm. Per the standard, DPGs adhere to privacy and other applicable laws, follow global standards and best practices such as the **Principles for Digital Development,** and provide safeguards against misuse or leakages of personal data. A number of other technical and nontechnical safeguards are still needed (see Section IV).



SECTION 3

Invest in Coordinated, Intentional Efforts to Create the Conditions Required for DPGs to Be a Viable, Long-Term Option for Digital Public Infrastructure

Despite emerging consensus on the benefits of digital public goods, it is rare today to find a digital public good that is implemented at the government infrastructure level. There are a number of reasons for this, many of which stem from perceived and actual problems with the sustainability of open-source technology.

Overcoming these challenges, thereby moving closer to creating the ecosystem depicted in Image x, requires coordinated and intentional effort toward achieving five interrelated, non-exhaustive outcomes (Image 2). These outcomes are informed by analysis completed by SEEK Consulting in 2020 and were refined during DPG Charter consultations in 2022. The current challenges facing each outcome are outlined below, while specific recommendations for overcoming these challenges are discussed in Section VII.

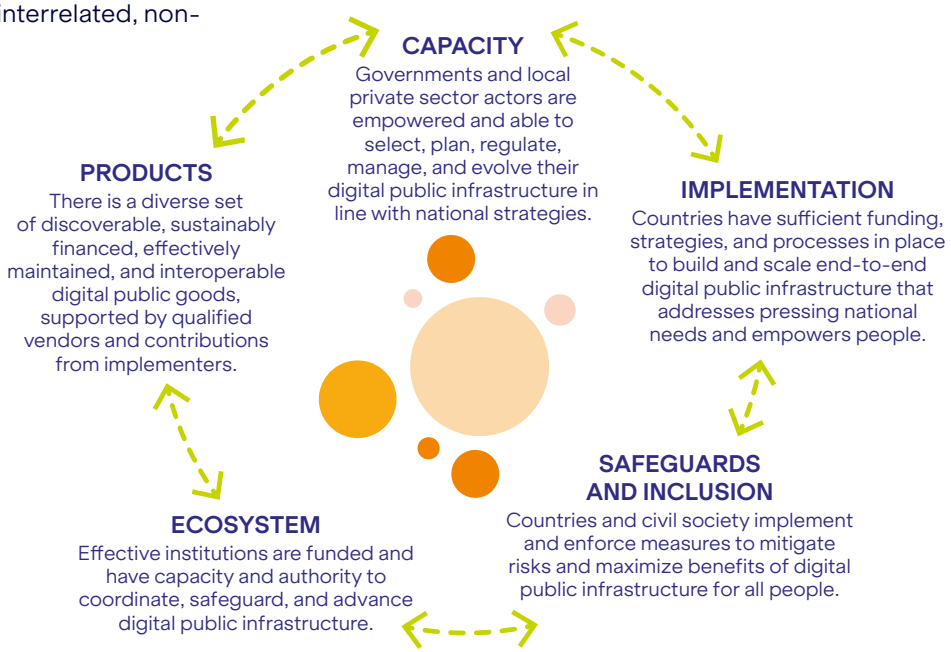


Image 2: Five Outcomes to Move Toward a More Effective Global Ecosystem for Digital Public Infrastructure

1. Products

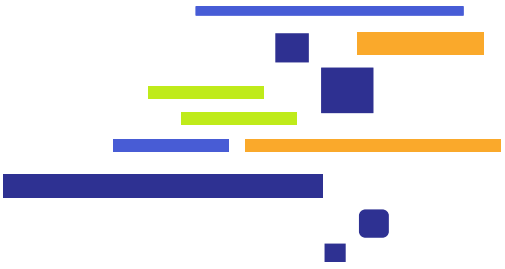
In order for digital public goods to deliver the benefits described above, they must be discoverable, sustainably financed, effectively maintained, and supported by qualified vendors and contributions from users and volunteers. There are three key challenges hindering this outcome: sourcing, financing, and governing.

Sourcing

Sourcing refers to the availability and discoverability of digital public goods. A larger supply of digital public goods designed specifically for key components of digital public infrastructure would provide governments with more options and increase competition, thereby spurring innovation. One potential new source of digital public goods is existing software developed internally by governments (or in fewer cases, international organizations and private companies) that could be extracted and refined to become shareable. There are clear signs that governments are increasingly interested in sharing existing systems, such as Ukraine's willingness to share its **Platform of Registries** and Togo's intention to share their **Novissi** platform.[13] But preparing these types of platforms to be sharable will require funding and technical support from outside entities, as well as solving the financing and governance challenges described below.

Financing

Without the right set of factors in place, many digital public goods risk falling into the "valley of death" (see Image 3). This valley of death, or **pioneer gap,** is a common challenge for start-ups that struggle to obtain the financing necessary to move from the innovation/idea phase to maturity/scale, and is particularly acute for social impact start-ups that initially rely on grant funding.



Any open-source technology will need to cover the following costs, either through financing from grant or generated revenue or, alternatively, community contributions.

- **Development costs:** Product owners *require* a team of qualified technical people working consistently with a developer community for a digital public good to be deployment ready.
- **Nondevelopment costs:** This includes funding to cover expenses related to administration, documentation, education and awareness building, and travel.
- **Operational costs:** This includes funding for human resources, logistics, hosting, and other recurring costs, as well as technical staff and community resources for maintenance and improvements to the codes.

Many existing digital public goods rely on donor grant funding to cover some or all of these costs. However, open-source products that are started with grant funding often struggle to replace this type of funding with other revenue streams, particularly if donors fail to work with partners to ensure low operational costs and strong governance models from the beginning. A key finding from our work with the Open Source Center is that a primary challenge for many core products is that their host organization. may be either a non-profit or for-profit which respectively favor either grants or revenue, not both. In reality, successful open-source products are designed for a mix of revenue sources, including grants, membership fees, revenue from paid services, and, in some cases, investor financing. We conclude that when donors act as funder of last resort, they can de-risk DPGs which increases market confidence and uptake to reach the scale where the mix of revenue sources covers operational overheads.

Governance

Digital public goods need governance models that support ongoing sustainability and maintain their open nature and commitment to the public good. Thus, digital public goods call for new governance models that move beyond existing models for either for-profit technology or open-source technology that is not committed to the public good.

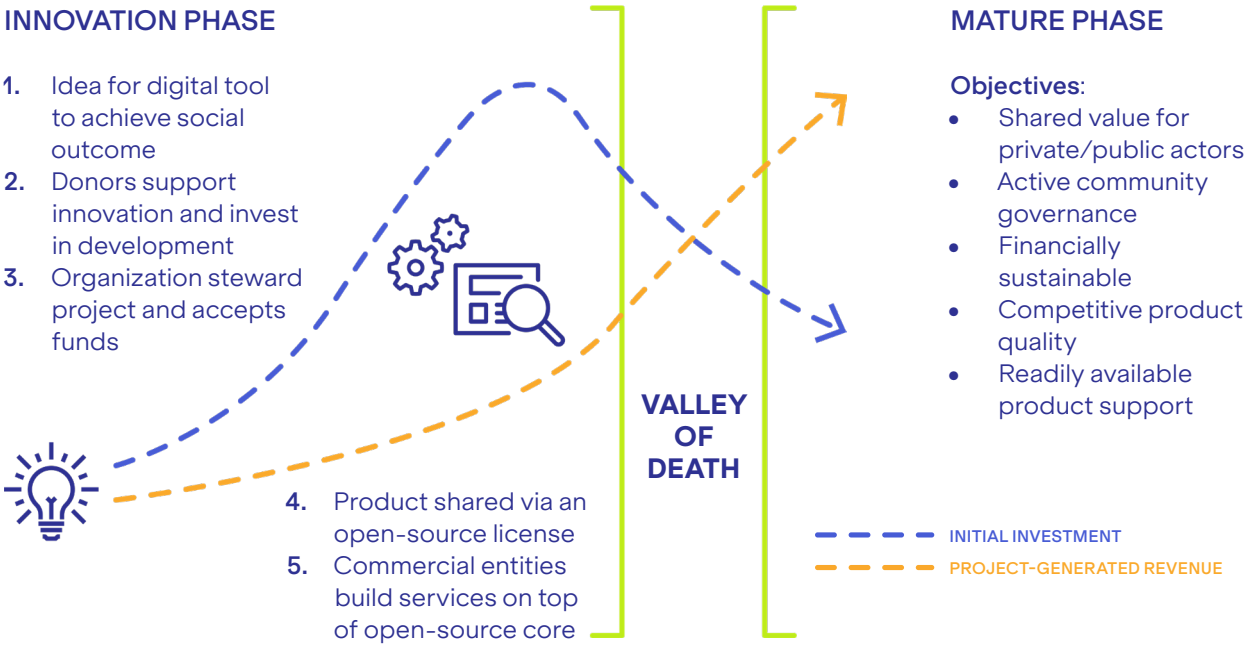


Image 3: Typical Journey of a Digital Public Good. Source: Digital Public Goods Alliance, 2022

Our experience suggests that such governance models require three key factors:

1. **A committed steward** or product owner who maintains the core codebase and product roadmaps, ensures quality, and manages both paid and volunteer staffing needs

2. **A legal host** that has the legal mandate to hold intellectual property, execute legal contracts, and accept a combination of diverse funding sources (see the discussion below on the Extended Ecosystem)

3. **An active support community** that enables community-led governance as opposed to top-down, single-vendor governance models

Community-led governance can be harder to establish, but experience suggests that the most effective models for delivering sustained positive impact are those that leverage a committed steward and legal host to coordinate decentralized community governance.[14]

2. Capacity

Implementing foundational digital public infrastructure requires new processes, standard operating procedures, and ways of working. While some of these needs are related to implementing open-source technology, most are needed regardless of the technology selected. New capacity must be built at multiple levels of society for successful deployment and maintenance of systems, particularly if they are to deliver for the public good. Note that capacity here refers both to increases in knowledge and increases in available tools.

- Governments and other institutional users require change management to adapt procurement and management policies to open-source products. Departments will need to shift towards more innovation-oriented and dynamic approaches to managing technical systems, and regulators will need to increase their capacity to develop and enforce data oversight and accountability. Capacity also includes increasing technical capacity through, for example, shifting digital government systems to affordable cloud storage.

- **System integrators,** the private technology companies that deploy and maintain solutions on behalf of users, need to increase awareness of the market opportunity provided by building out their own service offerings to include open-source platforms.

- **The local workforce** is critical to ensure that both governments and private-sector companies can recruit the skilled employees necessary to deploy, maintain, and grow digital public infrastructure. Creating such a workforce requires increased technical training and critical thinking skills throughout the educational curriculum.

- **Civil society,** including journalists, advocacy organizations, and community-based nonprofits, need to understand and have legal avenues to raise citizen concerns and hold the government accountable for data misuse and overreach.

- **Individuals and communities** need mobile and broadband connectivity; access to affordable devices; data awareness and tools to manage informed consent; and user-friendly interfaces that account for different spoken languages, literacy levels, cultural sensitivities, and physical abilities.[15]

> **"Open-source products are 'free' just as a puppy might be free: you don't have to pay to take it home, but you better be ready to pay for the food, the vet, dog walkers..."**
>
> *Consultation with IBM and Red Hat, September 2022*

3. Implementation

When a country implements an open-source service or platform, it is ultimately the country's responsibility to maintain its own local instance.[16] The committed steward or product owner needs to maintain and update the core product. However, the user (likely the government) is responsible for any customization of or specific needs for its local copy. Furthermore, governments will, in all cases, have existing digital systems in place (e.g., a digital management information system for each ministry) and these systems will likely not be open source. Yet, governments will have to develop an approach for integrating all of these systems into a coherent digital architecture in order to successfully develop end-to-end digital public infrastructure that delivers value to people and communities.

Thus, the development of this type of foundational, end-to-end digital public infrastructure supported by DPGs requires that countries have sufficient funding, technical capacity, strategies, and processes in place for implementation. In addition to the capacity needs described above, this requires:

- Donor funding that allows governments to spend on cross-sectoral issues such as digital infrastructure and is coordinated within country to avoid redundancies and overlap

- Systems integrators with experience in blending open-source solutions with legacy systems

- Planning for ongoing costs and required personnel by considering long-term budget and staffing needs early on

- Planning for the ownership of business processes and the responsibility for their development, modification, and simplification,[17] which may require new institutional structures, such as Open-Source Program Offices (OSPOs).

4. Safeguards and Inclusion

Safe, inclusive, and trusted digital public infrastructure must be designed and governed with effective safeguards and intentional efforts to include all people. Effective safeguards start with recognizing political realities. We live in an age of democratic backsliding. As of 2020, 43% more countries saw democratically elected governments systematically working to dismantle democratic processes and institutions than in the five years prior. Without getting the design and governance of foundational digital systems right, platforms risk being of little value to citizens and will fail to empower all people, regardless of their underlying technology. Therefore, a strong underlying trust framework between government and the rest of society is required.

Much of the excitement for digital public infrastructure has arisen out of the success of the society-wide digital government systems of two very different countries: India and Estonia. The success of these countries' core digital infrastructure—particularly digital identity, digital payments, and data exchange—is due to unique circumstances in these countries, including a number of checks and balances. Some of these safeguards can easily be implemented by design, such as Estonia's X-Road system, which notifies citizens every time their data is checked. Others must be implemented through governance and democratic institutions like **India's Supreme Court,** which has made several rulings to ensure that the country's digital identity system balances usefulness with people's right to privacy.

Preventing a **"DPI dystopia"** and digital repression requires a wide-ranging set of safeguards implemented along with efforts to actively encourage the inclusion and active participation of vulnerable and marginalized groups, including women. Such measures include:

- **Policies, regulations, and oversight bodies** to promote trust and institutions that can enforce these legal frameworks. Legal measures include data protection frameworks, laws for identifying and clarifying financial entanglements, and cybersecurity regulations. Institutions include data protection authorities, competition authorities, and independent bodies empowered to check government overreach and misuse of personal data.

- **Well-implemented consent networks.** These give individuals greater control over their digital data; enable them to approve/reject data requests, revoke access to data, and share data at a granular level; and enable greater efficiencies in the economy by reducing friction across transactions, regardless of where data is held.[18]

- **Civil society actors** who are empowered to create, improve, and sustain safeguards that create accountability in how digital public infrastructure is designed and implemented. Civil society organizations such as the **Africa Digital Rights Hub** and **CIPESA** play a big role in holding governments and the private sector to account for delivering on the promises of digital inclusion and digital rights. These organizations can strengthen implementation of both technical and ethical safeguards by creating additional, independent checks against abuse. Examples include providing knowledge and training on digital rights for consumers, activists, and companies; leading issue-based advocacy campaigns; publicizing citizen concerns and reports of abuse; and litigating illegal use of digital systems.

- **Technical safeguards,** including decentralized data storage. Centralized data storage can allow for many of the efficiency gains promised by digital transformation, such as the ability to quickly cross-check an individual's status against government databases. But highly centralized digital architectures can create a "honey pot" of personal data that can be accessed by nonstate actors, rogue government actors, and authoritarian regimes. More research and debate are needed to understand how to balance these tradeoffs and decentralize data storage without sacrificing convenience.

5. Supporting Ecosystem

The previous sections covered several critical actors within the DPI ecosystem, including DPG product owners, government users, private-sector systems integrators, and civil society. However, there is an extended ecosystem of support that is also needed to ensure that DPI remains safe, inclusive, and trusted over the long term. This includes associations, think tanks, and accelerators. Some of these institutions already exist and simply need support; others are missing entirely and need to be created.

Institutions that exist, but need to be nurtured:

- **Open source program offices (OSPOs) to support governments.** First, more countries need to establish an OSPO to provide advice on how to create and enforce policies that promote the use of DPGs in government. Second, OSPOs must be strengthened by linking them to networks that allow for information sharing between OSPOs and other institutions and communities of practice.

- **Peer learning networks.** Networks such as the **Africa Data Leadership Initiative** build communities of practice that embed open principles, point to new and emerging research of relevance, and advise on emerging good practices.

- **Advisory networks.** These provide policy advice and legislative support and are critically important to helping governments create cultures for using open-source technology in government. Advisory bodies can **help** governments create and enforce policies around using open-source technology in the public sector, as well as promote the use of digital public goods and the development of open digital public infrastructure through national digital strategies.

- **Research bodies.** Universities, think tanks, and consulting firms can conduct research on good practices for governance and community engagement; generate evidence on impact; promote standards for interoperability; and build registers of qualified systems integrators.

Missing institutions include:

- **Custodians.** Custodians or custodian-like entities such as foundations (e.g., the Linux Foundation, **Eclipse Foundation**, **Apache Foundation,** and **Apperta Foundation**) have played a critical role in maintaining open-source software for decades. Custodians are often set up as a **foundation**, which serves as a legal entity for products and coordinates communities and operations. Regardless of their form, custodians can **help** products scale by covering common services, making legal governance and acquisition and use of funding easier, and helping scale new digital public infrastructures as digital public goods for use by other countries. They can act as a legal fiscal entity; provide shared services such as human resources, recruiting, and payroll to drive down operational costs; and provide stopgap funding support.

- **DPG Accelerators.** DPG Accelerators help mature digital infrastructure into reusable, shareable products for the benefit of other users. Accelerators can both improve the quality of existing DPGs while also creating new ones either from scratch or by transitioning existing solutions to open-source. As countries increasingly embrace DPGs for use in their digital infrastructure, there are few if any quality supported DPGs to choose from for many use cases. As these countries then choose to build their own solutions, there is a willingness to share these with others as DPGs. Accelerators will play an important role in transitioning these to shareable DPGs with a clear product roadmap, governance, sustainable business model, and product support.

SECTION 4

Recommendations

To help move forward in addressing the challenges outlined above, we offer recommendations that are:

- Non-exhaustive and intentionally leave out high-level recommendations that have been stated in other publications on the subject
- Divided into quick wins that set the stage for driving a long-term positive impact, middle-term efforts, and long-term shifts that should start today but will take the most time to realize
- Divided into recommendations for donors, governments as users of digital public goods, and ecosystem actors, including the think tanks, private-sector companies, civil society organizations, and others that are interested in realizing the benefits of safe, inclusive, and trusted foundational digital public infrastructure

Quick Wins

Donors

- **Take a minimal, funder-of-last-resort approach.** When funding DPG core products, fund the minimal amount to keep neutrality; stress the need to maintain low-cost structures; after the initial start-up phase, ensure that donor funding is only relied upon when other contributions and shared resources cannot be obtained, while offering assurances that this minimal level of funding will be sustained over the long term to provide confidence to the implementer. Investing in the supporting ecosystem will help lower overall costs by providing shared resources for DPGs to draw upon as needed.
- **Fund DPG core products in addition to DPG implementations.** To create a competitive, sustainable market of DPG products that are properly designed, governed, and deployed, more funding needs to be available for products, given that this funding takes a minimal, funder-of-last-resort approach.
- **Invest in a robust set of actors that help translate global best practices into practical insights for implementation.** This includes strengthening existing efforts to build global and country-level DPG repositories; building the evidence based on cost drivers and pathways to impact; expanding peer learning and communities of practice, such as the Africa Digital Leaders Initiative (ADLI); and deepening advocacy efforts.
- **Invest in DPG accelerators to help bridge the so-called "valley of death" between start-up and scale.** The supply of supported and financially sustainable DPGs must be increased if they are to be a viable option for governments implementing DPI. Accelerators should focus on ensuring that a product is fully open-source with effective community governance and sustainable financing.

Governments:

- **Invest in setting up open-source policies and open source program offices to help manage relationships with the open-source ecosystems they depend on.** Given the open-source nature of digital public goods and their centrality to digital public infrastructure, OSPOs within and outside of governments can provide crucial coordination for local open-source ecosystems, building capacity in the process.

- **Reform procurement guidance to ensure that open-source technology can be procured as easily as proprietary software.** This includes allowing for incremental costs over time supporting in-country product customization, as well as one, large, upfront capital investment.

- **Decentralize the storage of sensitive data where possible.** New models for storing and sharing data such as federated ecosystems help avoid creating "honey pots" of personal data. This minimizes the risk that rogue actors will breach DPI systems to access large amounts of personal data. These actors could be foreign entities, existing government entities with bad intentions, and others who could use such data for surveillance or persecution.

Ecosystem actors:

- **Test, iterate, and scale alternative funding models.** It is necessary to move away from single grants that only cover deployments costs and towards financing mechanisms that support both products and deployment over the long term. New financing mechanisms may include pooled procurement, three-sided marketplaces, joint funds, and others. These go along with new governance models, such as co-ops, that help ensure DPGs are governed long term for the public good. A key priority in the near future will be documenting the effectiveness of these different models.

Medium-Term Efforts

Donors

- **Overcome existing restrictions and earmarks that require allocating donor funds to specific sectors.** This will open up more funding for foundational, infrastructure-level investments and allow for long-term product support of priority DPGs.

- **Promote custodian models that offer shared legal and fiscal resources to multiple digital public goods.** By operating as a central coordinating body, custodians can play a role in absorbing grant funding and revenue from users; facilitating contributions from the community; and lowering operational costs through shared services such as human resources, recruiting, and payroll.

Governments:

- **Be willing to share and reuse.** Governments are showing increased willingness to share aspects of their digital infrastructure. This is a positive step, as it helps build the digital commons and, in turn, provides a tool for that country's soft diplomacy. At the same time, governments must be willing to reuse other countries' tools when they are relevant and high quality. Reusing should be viewed with just as much pride as sharing.

- **Invest in change management in addition to digital skills and resources.** Change management is supported by integrating digital public goods and infrastructure as part of national digital transformation strategies and working to use a whole-of-government approach to deliver on all of the use cases demanded by government, the private sector, and individuals.

- **Implement a consent network as a foundational layer of DPI.** Through its Data Empowerment and Protection Architecture (DEPA), India has led the way on reimagining consent in ways that can truly empower people to manage their own data. Other countries will benefit from testing their own iterations on consent that shift the data economy from an organization-centric architecture to an individual-centric one.

Ecosystem actors:

- **Provide existing champions within government the resources they need to advocate internally for digital public goods.** This can happen by highlighting concrete outcomes, such as support for local entrepreneurs, job creation, and increased cost-efficiency. Similarly, assessing the opportunity costs—both financial and in terms of unrealized socio-economic gains—incurred by failing to build interoperable platforms helps build political will.

- **Strengthen the building block approach to DPI.** A building block approach will make it easier to integrate different types of technology, whether open source or not, into a country's digital stack. GovStack is a multistakeholder initiative promoting such an approach, thereby helping governments simplify the digital transformation process and reduce the cost, time, and resources required to create digital platforms and services.

Long-Term Shifts

Across governments, donors, and ecosystem actors, we recommend working toward the following long-term shifts:

- **Put people and communities at the center of all decisions related to digital public infrastructure.** This is the only way to ensure that DPI maximizes benefits and minimizes risks, thereby delivering on the promises of creating a more inclusive society.

- **Shift towards more holistic views of how governments use and sustain open infrastructure.** Such a view would emphasize persistent monitoring and feedback over a project's entire lifecycle to help break feedback loops that lead to an overemphasis on deployments rather than long-term maintenance. This view also allows for governments to run their core DPI on a variety of different types of technology (proprietary, open-source, and custom-built), while moving toward more open and interoperable infrastructure over time. Open infrastructure, in other words, is a long-term mentality shift, rather than something that occurs overnight.

- **Strengthen local talent pipelines.** This can be done by investing in digital education and critical thinking skills throughout the educational continuum, moving away from training programs that focus on providing single skillsets such as learning to code one type of software. Ultimately, the goal should be to move away from relying on a handful of digital champions to establishing a workforce across government, civil society, and the private sector that has a digital mindset, and is able to proactively use data, algorithms, and machine learning to open up new possibilities and chart a path for success in an increasingly technology-intensive world.

SECTION 5

Appendix

Abbreviations

AI	Artificial intelligence
ADLI	Africa Data Leadership Initiative
ADRH	Africa Digital Rights Hub
BB	Building block
CDL	Core digital layers
CSOs	Civil society organizations
DIAL	Digital Impact Alliance
DPI	Digital public infrastructure
DPGs	Digital public goods
EU	European Union
ID	Identification
ITU	International Telecommunication Union
OSPO	Open-Source program office
PDD	Principles for Digital Development
PPP	Public private partnership

Endnotes

1 Nordhaug, Liv Marte and Harris, Lucy (2021). "Digital public goods: Enablers of digital sovereignty." Development Co-operation Report 2021, OECD. Available at: https://www.oecd-ilibrary.org/sites/c023cb2e-en/index.html?itemId=/content/component/c023cb2e-en

2 Over the years, these efforts have been described using different terms, including digital government, digital transformation, e-government, e-governance, and civic tech (outside of the international development community).

3 Feldstein, Steven (2021). The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance.

4 For more, refer to the Digital Public Goods Sustainability Workbook. Available at: https://dial.global/wp-content/uploads/2022/12/Sustainability-Guidbook.pdf.

5 Stürmer, Matthias; Tiede, Markus; Nussbaumer, Jasmin; and Wäspi, Flurina (2023). "Digital Sustainability and Digital Public Goods: An Updated View of Open Knowledge Shaping Sustainable Development." Bits & Bäume Journal, January.

6 Note that building blocks do not have to be open-source or digital public goods, by definition. For more information, refer to https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf.

7 Results as reported during an interview with the Ministry of Digital Transformation of Ukraine, February 2023.

8 Gartner (2021).

9 Blind, K. and Böhm, M. (2021). The Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy, Final Study Report, European Commission, Brussels, https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and

10 Ibid.

11 Burt, C. (2018), "Vendor lock-in hindering African identity projects," Biometric Update,

12 The vendors (called systems integrators) that help implement and maintain open-source technology can create their own forms of lock-in by offering highly customized products. These products, while based on open-source code, can cause lock-in if they can only be maintained by one vendor.

13 Per interviews conducted in September 2022 and March 2023.

14 For more on different models of open-source governance, refer to "Open Source Archetypes: A Framework for Purposeful Open Source." Mozilla (2019). Available at: https://opentechstrategies.com/archetypes-files/open-source-archetypes-v2.pdf.

15 For more, refer to the USAID Digital Government Model. Available at: https://www.usaid.gov/sites/default/files/2022-12/USAID_Digital_Government_Model_1.pdf.

16 An instance is a specific realization of an open-source core product. In other words: Open-source technology means that the source code is freely available. Converting that source code into runnable code for a specific user (in this case, a government), creates a new "instance" that is the responsibility of the user. The instance may still benefit from updates to the source code.

17 For more detail, refer to the USAID Digital Government Model, available at: https://www.usaid.gov/sites/default/files/2022-12/USAID_Digital_Government_Model_1.pdf

18 Hariharan, Venkatesh (2022). "How India Is Reimagining Consent to Empower People." Digital Impact Alliance. Available at: https://docs.google.com/document/d/1YovKRkV3CN-cShIw58nCICxEHKaa-ZE9OM8L5zLPReY/edit.