Source: Amunga Eshuchi/USAID

DIGITAL ECOSYSTEM FRAMEWORK

USAID FROM THE AMERICAN PEOPLE

DigitalFrontiers SCALING DIGITAL DEVELOPMENT

DAI Shaping a more livable world.

USAID's Digital Strategy seeks to achieve and sustain open, secure, and inclusive digital ecosystems that contribute to broad-based, measurable development and humanitarian assistance outcomes. The Digital Strategy is part of USAID's holistic approach to help achieve the Sustainable Development Goals (SDGs)

Purpose of the Framework: To help achieve the Digital Strategy's goal to strengthen open, inclusive, and secure digital ecosystems, USAID developed the Digital Ecosystem Framework. This Framework is designed to provide a comprehensive overview and shared understanding of the elements that influence a country's digital ecosystem.

Framework Audience: USAID staff and partners, government agencies, donors and multilaterals, the private sector, think tanks, and the broader development community involved in designing, funding, implementing, or evaluating digital development activities can use this as a resource.

How to use this Framework: Gain a basic understanding of the three pillars of the digital ecosystem and associated cross-cutting topics to evaluate the operating environment and inform the design of inclusive, effective, and sustainable digital development activities. Readers seeking specific information about certain technical areas are encouraged to skip ahead to that section. Please refer to the At a Glance page to select the topic of most interest to you.

Introduction

Digital technologies are becoming more accessible and have brought the promise of enormous benefits from digitalization. These tools and services can advance freedom and transparency, generate shared prosperity, strengthen inclusion, and inspire innovation. They also present significant risks to privacy and security through surveillance, censorship, and other forms of digital repression. It is therefore important to understand the potential opportunities and risks associated with digital technologies within a *digital ecosystem*.


Source: USAID/Oscar Leiva

WHAT IS A DIGITAL ECOSYSTEM?

USAID's Digital Strategy explains that a digital ecosystem comprises stakeholders, systems, and an enabling environment that, together, empower people and communities to use digital technology to access services, engage with each other, and pursue economic opportunities. Building on this concept, the Agency created a framework that refines the ecosystem into a practical structure for development practitioners.

Over the course of 20 months, USAID developed the digital ecosystem framework through consultations with technical experts at USAID, including the Center for Democracy, Human Rights, and Governance (DRG); the Center for Economics and Market Development (EMD); and within the Innovation, Technology, and Research (ITR) Hub. The concepts were also tested, iterated, and refined through four pilot Digital Ecosystem Country Assessments (DECAs) conducted in partnership with USAID Missions in Colombia, Kenya, Serbia, and Nepal.

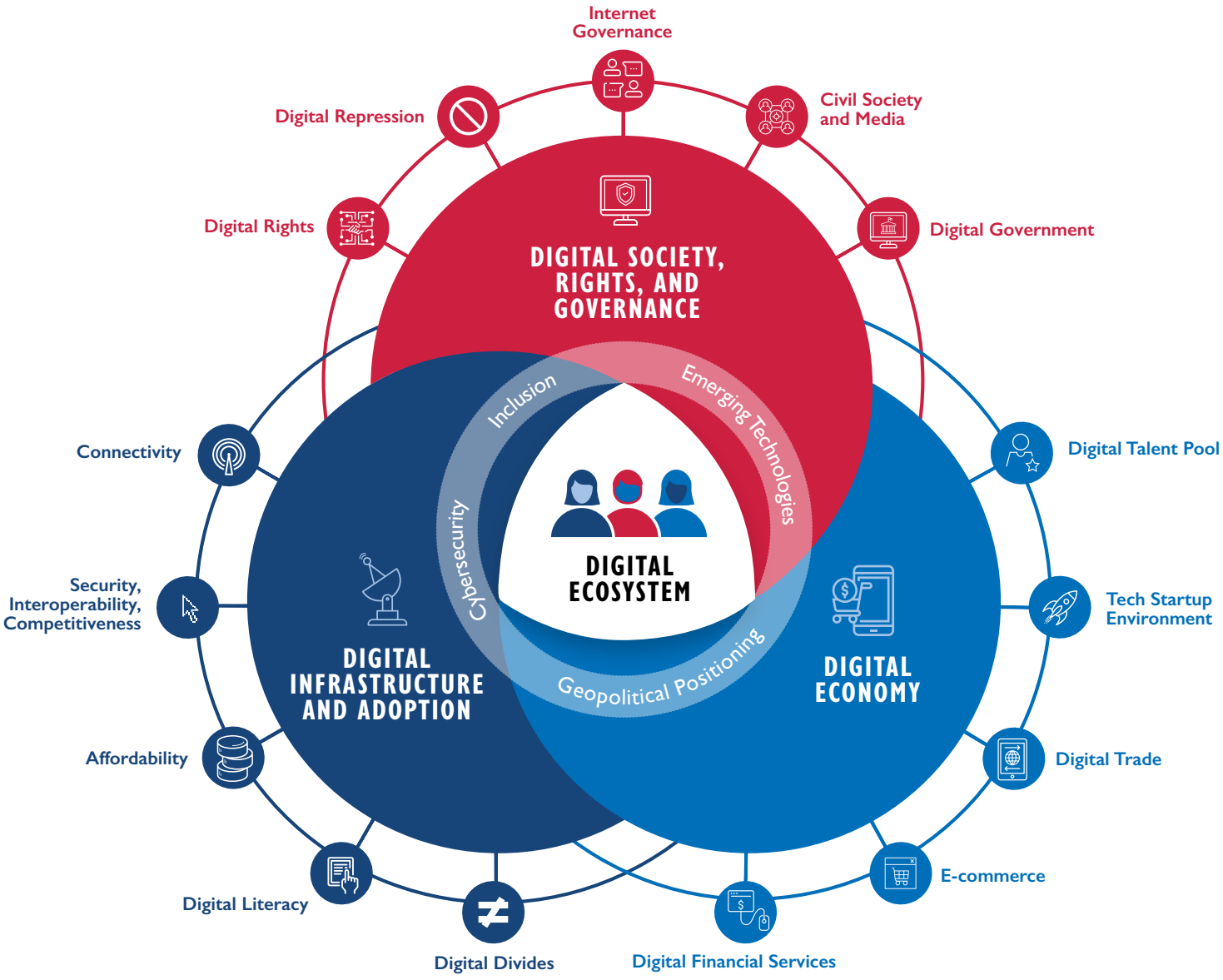
USAID's Digital Ecosystem framework is distinct from the concept of a *digital economy* – and the distinction is an important one that USAID has iterated and worked to define. It is an environment, system, and culture all at once; it is the starting point for any digital interaction, and understanding it is crucial for development practitioners.

Digital Ecosystem Framework

The Digital Ecosystem Framework is organized around three separate, overlapping pillars:

I. Digital Infrastructure and Adoption
II. Digital Society, Rights, and Governance
III. Digital Economy

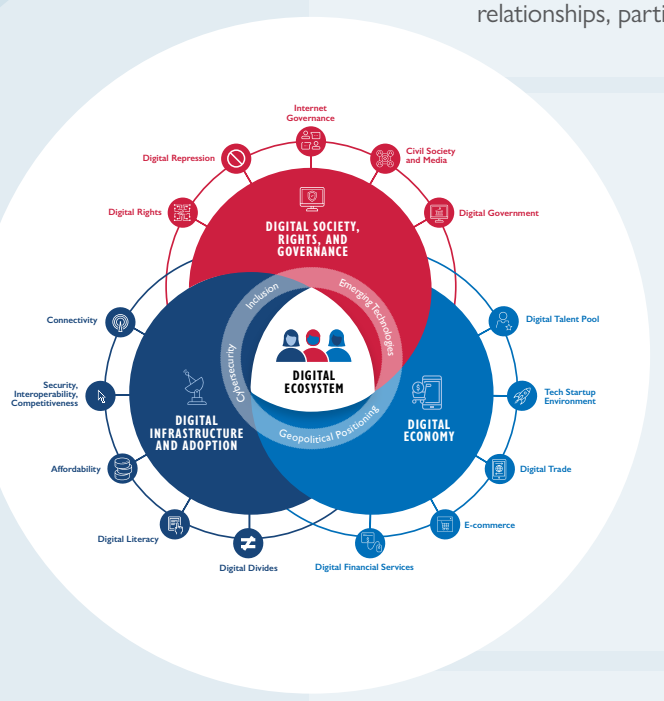
And it encompasses four cross-cutting topics: Inclusion, Cybersecurity, Emerging technologies, and Geopolitical Positioning.



DIGITAL ECOSYSTEM: AT A GLANCE

Cross-cutting Topics

Inclusion Equal access to opportunities and resources for people who might otherwise be excluded or marginalized, and intersectional elements of inclusion, i.e. gender and ethnicity.
Cybersecurity How people, systems, and technology protect information kept in digital formats from being taken, damaged, modified, or exploited.
Emerging Technologies Including artificial intelligence and machine learning, Internet of Things, drones, robotics, and blockchain.
Geopolitical Positioning How a country's digital evolution is being shaped by international relationships, particularly the global spread of technology-enabled authoritarianism.



Pillar I: Digital Infrastructure and Adoption

Connectivity Infrastructure Foundational infrastructure like fiber-optic cables and towers.
Security, Interoperability, and Competitiveness Conditions for a healthy telecommunications market.
Affordability The costs of digital access.
Digital Literacy The ability to access, manage, understand, and create information safely and appropriately through digital devices and platforms for participation in economic, social, and political life.
Digital Divides Disparities in access and use, related to gender, race, ethnicity, economic status, refugee status, geography, disability, sexual orientation, age, or other factors.

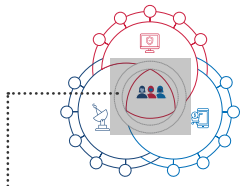
Pillar II: Digital Society, Rights, and Governance

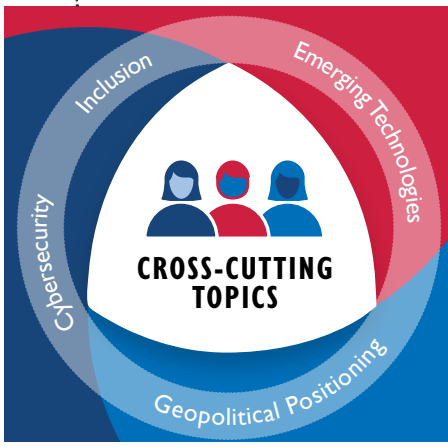
Digital Rights Protection of fundamental human rights online.
Digital Repression The use of technology to violate human rights.
Internet Governance The development and application of principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the internet.
Civil Society and Media Organizations working to expose digital repression and advocate for digital rights.
Digital Government Online delivery of government services, management of government processes, and engagement with the public.

Pillar III: Digital Economy

Digital Financial Services Using money online, through digital payments, savings, and other tools.
Digital Trade Delivery of products and services over the internet.
E-commerce Sale and purchase of physical goods using the internet.
Tech Startup Environment New businesses focused on innovative products and rapid growth.
Digital Talent Pool Training and equipping workers for a future-focused digital economy.

Cross-cutting Topics





Inclusion

Marginalized and vulnerable populations are often unable to fully participate in the digital ecosystem. Exclusion can stem from social norms or from inequities in access, literacy, income, or the availability of relevant content. Depending on the local context, people may be excluded based on factors such as gender, race, ethnicity, disability, economic status, geography, sexual orientation, language, refugee status, and age. Discussions around inclusion overlap and will often intersect (e.g., for women with disabilities). The term "digital divide" is commonly used to describe disparities in access (see Pillar 1), but there are other aspects of inclusion (e.g., gender equity in the digital talent pool) that should be considered.

Cybersecurity

Cybersecurity is the protection of information and communications systems and information against damage, unauthorized use or modification, or exploitation. Cybersecurity goes beyond the physical and digital protection of computer and communication systems. It includes individual, institutional, and national considerations. Effective cybersecurity requires adequate policies and strategies along with institutions that can implement those strategies. It also requires that institutions have the human and material resources to mitigate, detect, and prevent cyber attacks. Actors across governments, civil society, media outlets, and the private sector can include cybersecurity considerations in all aspects of operations including enterprise systems, procurement, supply chains, and contracting agreements.

Emerging Technologies

The term "emerging technology" encompasses artificial intelligence (AI), Internet of Things (IoT), blockchain, 5G and other new technologies. They can bring a range of benefits, including digital experiences that are faster, more user-friendly, and more inclusive across disability or language barriers. There are also inherent risks in applying emerging technologies. For example, if not designed carefully, some AI technologies may encode bias that can harm marginalized or vulnerable populations such as persons with disabilities.

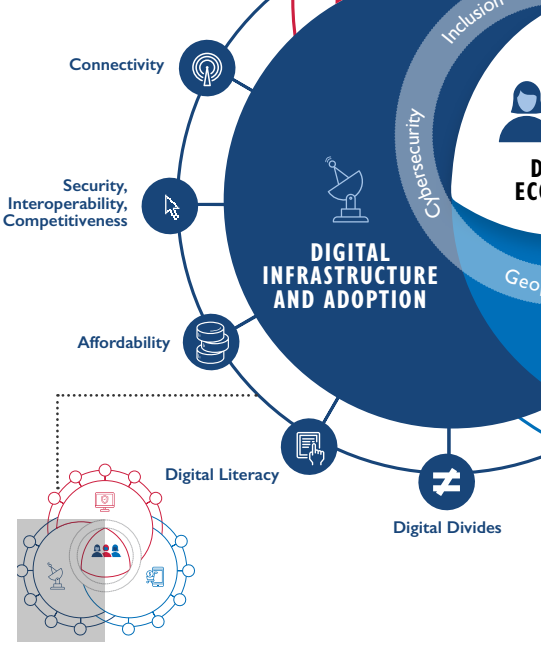
Geopolitical Positioning

Although the digital ecosystem focuses on the country-level, countries exist in a global context and are impacted by the actions of others. One specific area of concern is the influence of authoritarian states that are actively working to shape the global digital space. It is important for USAID Missions to understand how these global dynamics play out in the countries where they work and how global technology rivalries can affect development.

Source: Matthieu Young/USAID

PILLAR I

Digital Infrastructure and Adoption

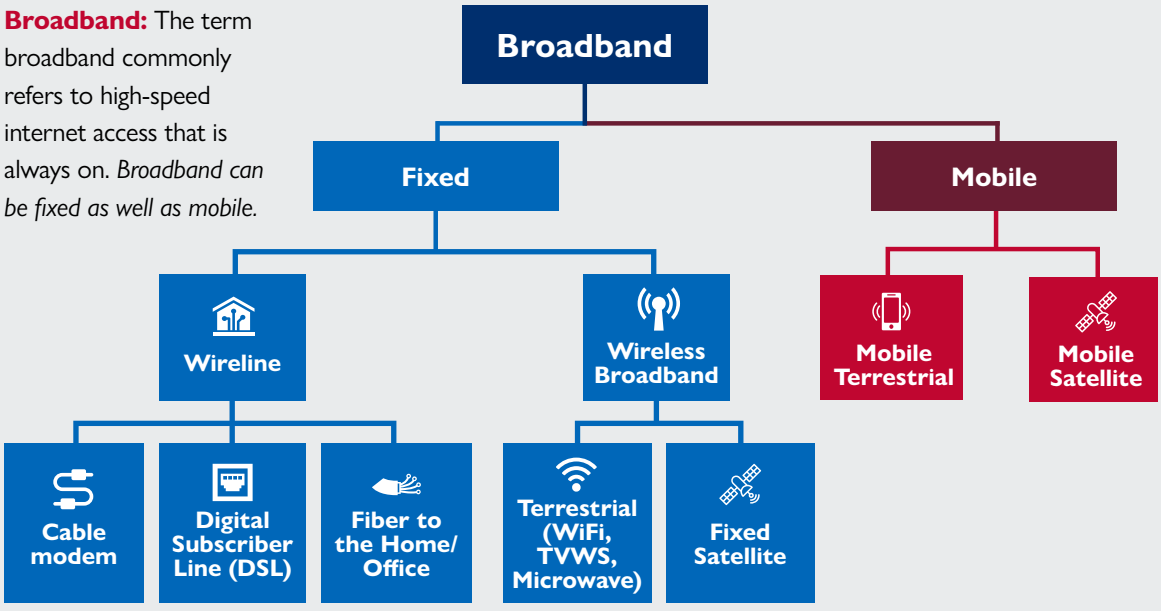


This pillar refers to the resources that make digital systems possible and how individuals and organizations access and use these resources. This pillar examines aspects of digital infrastructure like internet bandwidth, network coverage, and telecom market dynamics as well as behavioral, social, and physical barriers and opportunities for equitable adoption—who uses and does not use digital technologies and why.

Connectivity Infrastructure

Connectivity infrastructure refers to the foundational components that enable the use of data, devices (e.g., mobile phones), and other internet services and systems. Examples include fiber-optic cables, cell towers, satellites, data centers, and fixed and mobile broadband. Government and private sector choices about infrastructure directly affect who can provide digital services and where, how the internet is used, and who does and does not have access to digital tools and services. Connectivity infrastructure can also include innovative technologies and deployment models such as open radio access networks (open RAN), TV White Space (TVWS), relay stations, wireless mesh networks, and community networks that can help extend access to remote or underserved areas.

Broadband: The term broadband commonly refers to high-speed internet access that is always on. *Broadband can be fixed as well as mobile.*



Fixed

Pros	Cons
Lower data costs	Service tied to single location
Faster speed and greater reliability	User must be in coverage area of access point

Mobile

Pros	Cons
Portable – allows for user to roam freely	Requires phone number
Convenient	Reliability
Always connected	Bandwidth capacity constraints
	Higher data cost

Security, Interoperability, and Competitiveness

This topic addresses the basic features of a healthy telecommunications market. In a thriving market, government regulation is used to ensure secure, trustworthy networks, and to promote competition that drives innovation and lowers costs. Assessing the telecom market requires understanding the important policies, market players, the extent of government ownership, and the degree of interoperability.

Affordability

Affordability measures the cost of connectivity relative to local income. Device, maintenance, and data costs can be deterrents to widespread mobile phone and internet use. Effective regulation of the telecommunications market can improve affordability by promoting competition and innovation.

Digital Literacy

Digital literacy is the ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital devices and networked technologies for participation in economic, social, and political life. This topic includes competencies such as computer literacy, information and communication technology (ICT) literacy, information literacy, and media literacy. Cyber hygiene as well as media and information literacy are important components of digital literacy. Cyber hygiene is the ability of an individual to stay safe and secure online through routine practices. Media (or information) literacy is an individual's ability to search for and critically evaluate available information (data, news articles, reports, etc).

Digital literacy influences adoption of digital tools and services, but should also be kept in mind for other digital ecosystem pillars. Pillar II covers government capacity to develop digital policies and programs that account for citizens with varying digital (and media) literacy levels and Pillar III highlights the importance of digital literacy in building the digital talent pool. Digital literacy is also connected to Cybersecurity, one of the cross-cutting areas. Cybersecurity looks at mitigation and prevention across an entire digital ecosystem of risks, which includes an individual's ability to operate safely online.

Digital Divides

The digital divide is the distinction between those who have internet and/or mobile phone access and are able to make use of digital communications services and those who are excluded from these services. Digital divides can stem from social norms or from inequities in access, literacy, income, or availability of relevant content. Digital divides may be associated with gender, race, ethnicity, disability, economic status, geography, sexual orientation, language, refugee status, and age among other factors. Digital divides overlap and will often have specific intersectional barriers.

Source: David Rochkind/USAID

PILLAR I: CROSS-CUTTING TOPICS

The examples below illustrate how the four cross-cutting topics may appear across Pillar 1 topics.

1. Inclusion

These examples use gender and disability to illustrate the role of inclusion in digital ecosystems. Other marginalized and vulnerable populations may experience similar challenges.

Gender: Girls and women not only face unique barriers in terms of access to and use of digital tools and services, but often lag behind boys and men in digital literacy. According to data from UNESCO, this digital literacy gap is present in almost every country in the world, regardless of geography or income. Digital tools, services, and skills education often do not consider the needs or preferences of women and girls.

Disability: Equitable access to digital tools and services must account for persons with a broad array of abilities, including those who are hard of hearing, blind, have speech impediments, or other learning, developmental, and psychosocial disabilities. It is important that persons with disabilities have access to digital tools and services that will work for them.

2. Cybersecurity

National-level cybersecurity includes the protection of critical internet infrastructure such as fiber optic cables and cloud storage systems, and the supply chain for digital infrastructure (e.g., switches, routers, base stations). Individual-level cybersecurity focuses on the cyber hygiene aspects of digital literacy, such as understanding cyber threats and taking action to protect personal data.

3. Emerging Technologies

Cloud computing and AI can help governments, companies, and institutions handle large data volumes. With more developing nations moving towards 5G networks, the amount of data will continue to increase. Internet service providers can also explore the application of emerging technologies to strengthen their competitive advantage and provide better service to last-mile customers. Emerging technologies can also help bridge digital divides, for example through speech-recognition interfaces for some persons with disabilities and those with lower literacy.

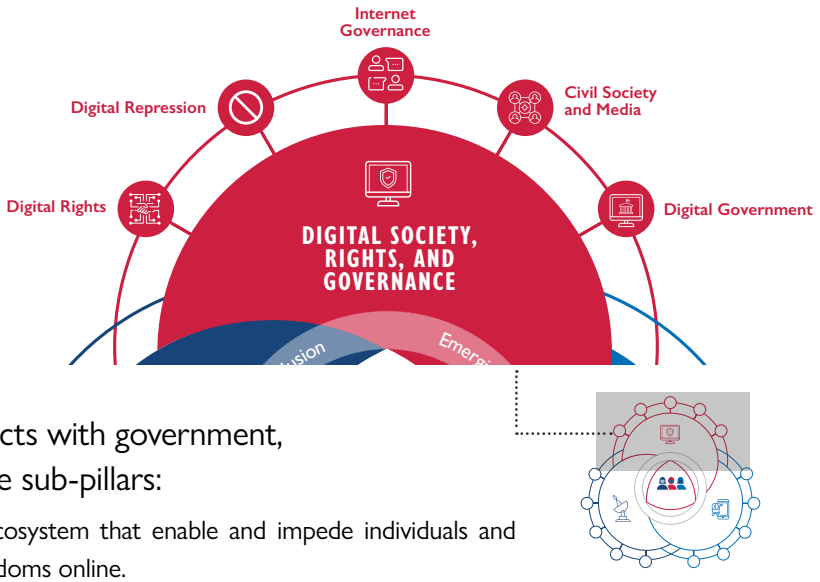
4. Geopolitical Positioning

Investments in digital infrastructure (e.g., being a part of the PRC's Digital Silk Road Initiative), and partnerships with foreign telecommunications companies and equipment manufacturers may have serious implications for security, interoperability, and financial sustainability.

Source: Melinda Donnelly for USAID/Oceans

PILLAR II

Digital Society, Rights, and Governance



Pillar II focuses on how digital technology intersects with government, civil society, and the media. It is divided into three sub-pillars:

1. **Internet Freedom** explores elements of the digital ecosystem that enable and impede individuals and institutions to exercise human rights and fundamental freedoms online.
2. **Civil Society and Media** identifies key institutions and how they report on, advocate around, and influence freedoms online.
3. **Digital Government** looks at the government's efforts to manage its internal IT processes and systems, deliver citizen- and business-facing e-services, and engage with the public through digital channels.

I. Internet Freedom refers to the ability of individuals to access the internet without obstacles, produce and consume content without censorship, and have their fundamental human rights respected online. Assessing internet freedom requires understanding which online rights are recognized, how those rights might be violated, and what institutions and processes exist to govern the online space.

Digital Rights

Digital rights refers to the rights and freedoms that individuals are able to exercise online, including rights related to privacy and data ownership. It includes topics such as freedom of expression online, access to online media, data privacy and protection, and other human rights issues, such as journalists and bloggers having the freedom to post information online without the fear of arrest or attack, protecting children from digital harms, and protecting women and girls from online gender-based violence. The digital rights topic also considers the extent to which private sector companies use human rights impact assessments (HRIA) to identify and prioritize human rights impacts. For example, Facebook's HRIA in Myanmar shaped their stance and implementation plan to address human rights in the country.

Digital Repression

Digital repression refers to the use of digital tools and technology to violate human rights and includes five techniques—surveillance, censorship, social manipulation and disinformation, internet shutdowns, and targeted persecution of online users. While digital repression is common under authoritarian regimes, democracies have also used these techniques. Digital repression is not limited to government actors; non-state and foreign actors (including private sector and religious groups) can also deploy these techniques for political, social, and economic reasons. Digital repression can be deployed using various technological tools including surveillance cameras, commercial malware, social media "botnets", and access-blocking firewalls. Censorship and surveillance circumvention technologies (e.g., VPN, encrypted messaging applications) are used by people in many countries to mitigate some elements of digital repression.

Internet Governance

Internet governance is defined as the development and application of principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the internet. There are two primary models of internet governance:

1. Multi-stakeholder, the model USAID supports, is a collaborative effort involving governments, the private sector and civil society; and

2. State-based, in which processes, decisions, and actions are dominated by the government with little to no stakeholder input.

Internet governance touches on a range of public policy issues including trade, civil liberties, cybersecurity, and sovereignty. Internet standards affect how people can access online resources, how businesses expand on a global scale, and how governments use the internet to manage their internal processes and deliver citizen services. Internet governance includes multi-stakeholder responses to illicit activity such as data breaches, scams, child exploitation, or extremist recruiting on the internet.

A multi-stakeholder approach to internet governance ensures that processes are driven by mutual consensus, and that a single stakeholder group does not monopolize control. Two notable internet governance institutions are the Internet Governance Forum (IGF) and the Internet Corporation for Assigned Names and Numbers (ICANN). The IGF operates at a global, regional, and national level to create an open and inclusive dialogue on internet governance issues. ICANN coordinates internet protocol addresses and domain names that people and devices use to connect to the internet. This topic also looks at a country's participation in and compliance with international agreements (e.g., Budapest Convention on Cybercrime, regional trade agreement requirements).

2. Civil Society and Media

Civil society organizations (CSOs) include formal non-government organizations (NGOs) as well as formal and informal membership associations (e.g., labor unions, business and professional associations, farmers' organizations and cooperatives, and women's groups) that articulate and represent the interests of their members, engage in analysis and advocacy, and conduct oversight of government actions and policies.

CSOs and the media play an important role in a digital ecosystem by promoting the inclusion of diverse perspectives and calling attention to abuses. This topic emphasizes how CSOs and the media report on, advocate for, and influence online freedom. It explores how these institutions serve a watchdog role in the face of declining online freedoms, strategies they use to uphold online freedom and inclusion, how digital media is used and accessed, how social media is used for activism (both online and offline), and how the internet is used for political organizing. Media includes both state and independent media, as well as informal, media influencers who publish and/or share content that triggers and shapes broader conversations.

3. Digital Government

Digital government refers to the use of digital technologies as an integrated part of government modernization strategies to create public value. It relies on a digital government ecosystem comprising government actors, non-governmental organizations, businesses, citizens' associations and individuals, which supports the production of and access to data, services, and content through interactions with the government. Digital government can be divided into three broad categories of systems, used by governments to deliver, manage, and engage.

- **Deliver Government Services**: Government services refer to the use of technology such as online government service portals and digital ID to enable and improve how public bodies provide services to people (G2P) and to businesses (G2B). Online government portals bring together government information and services for individuals and businesses to access information and carry out administrative procedures. This topic also includes the availability and usability of open government data and, when applicable, Open Government Partnership (OGP) commitments.
- **Manage Government Systems**: Digital government systems include back-end IT systems, management information systems, financial management information systems, and data storage solutions (e.g., cloud storage and government data centers). Strong digital government systems are interoperable, well managed and maintained,

widely used, and well-protected. When high-quality solutions are available and suitable, governments can promote security and interoperability by embracing open-source software solutions.

- **Engage Citizens and Organizations**: Digital technology can provide a powerful way for governments to collect feedback and input from the public. This can include reports of service outages; online polls, surveys, and petitions; and potentially even online elections. These feedback mechanisms are an essential piece of participatory governance in a digital world, but require careful attention to inclusion, privacy, and transparency. Government innovation hubs provide platforms for the government to work directly with innovators to solve particular challenges and foster connections with the private sector (e.g., 18F in the U.S.).
- **Guardrails for Technology**: Effective digital government systems build public trust by respecting individual rights. This often means being explicit about what will not be done with citizen data—limiting the use of technology by government and other actors for malign purposes. Governments can visibly constrain misuse by adopting and enforcing data governance policies and ethical guidelines (e.g., with AI and similar emerging technologies). Governments can choose to use transparent procurement and to consult impacted communities when deploying new technologies (e.g., for digital IDs, Smart Cities, and e-citizen portals).

PILLAR II: CROSS-CUTTING TOPICS

The examples below illustrate how the four cross-cutting topics may appear across Pillar 2 topics.

1. Inclusion

These examples use gender and disability to illustrate the role of inclusion in digital ecosystems. Other marginalized and vulnerable populations may experience similar challenges.

Gender: Online violence targeting women and sexual minorities can take many forms such as cyber stalking, defamation, identity theft and hacking, or exploitative threats and shaming—all of which are violations of their digital rights.

Disability: Digital government services can consider inclusive design elements to ensure they are accessible for everyone. This can include providing services through websites or portals for those who can't travel, voice-based interfaces, alternative text for images, and chat support. Digital ID systems (particularly those incorporating biometrics) can provide alternatives to retina scans or fingerprints. Persons with disabilities may also be uniquely vulnerable to online harassment, personal data breaches, and mis- and disinformation.

2. Cybersecurity

National-level cybersecurity requires the protection of government data and IT systems, cross-border data flow agreements, and continued adaptation to new threats. Cyber attacks on government systems can decrease public trust in government processes and services. Government cybersecurity institutions such as Computer Security Incident Response Teams (CSIRTs) are critical but require adequate staff and resources. Government, civil society and digital media outlets can make choices to ensure data protection and privacy as well as individual and institutional protection against cyber harms that violate digital rights. These harms may be caused by actors (state and non-state) employing digital repression tactics such as mis- or disinformation, censorship, and surveillance.

3. Emerging Technologies

Government services can be enhanced by emerging technologies such as through blockchain-backed data registries and AI-powered citizen e-service delivery. Emerging technologies also pose potential risks including "deepfakes," (which can spread disinformation through falsified images, audio, and video) and advanced surveillance systems that employ facial recognition.

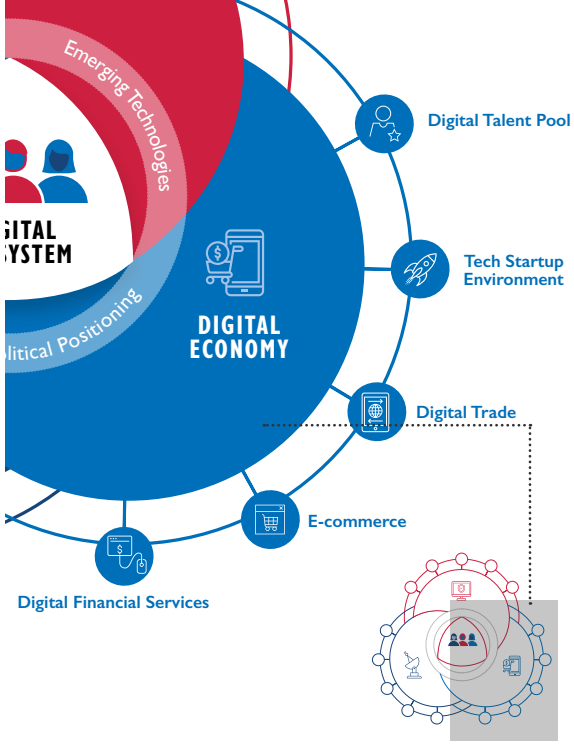
4. Geopolitical Positioning

Foreign powers can use digital technologies in several ways to exert and broaden their global influence. In some cases, such as the export of surveillance technologies or commercial spyware, foreign companies can enable the illiberal instincts of local actors. In more extreme cases, foreign actors can attempt to undermine the legitimacy or stability of a government through disinformation or cyber attacks.

PILLAR III

Digital Economy

This pillar explores the role digital technology plays in increasing economic opportunity and efficiency, trade and competitiveness, and global economic integration. This pillar assesses the opportunities and barriers to adoption of digital financial services, e-commerce, and digital trade. It also examines strengths and weaknesses in the local digital talent pool and the tech startup environment.



Digital Financial Services

Digital financial services (DFS) are financial services enabled by or delivered through digital technology (e.g., mobile phones, cards, the internet). These services (e.g., payments, credit, insurance, savings, advisory) can be offered by a range of providers, from banks to a host of non-bank financial institutions, such as microfinance institutions, digital credit providers, payment providers, technology vendors, and electronic money issuers. Well-developed national payments systems are likely to include infrastructure such as a national switch and automated clearing houses. Well-designed DFS products are created and piloted with the target users and to operate in an environment that prioritizes consumer protection . Given that many USAID programs serve low-income, marginalized groups, it is important to understand the concept of "digital financial inclusion"—defined as digital access to and use of formal financial services by excluded and underserved populations. Inclusive digital financial services are suited to the customers' needs and delivered responsibly, at a cost that is affordable to customers and sustainable for providers.

E-commerce

OECD defines e-commerce as "the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders." E-commerce may be conducted through formal (e.g., Amazon, Etsy) and informal (e.g., Facebook, Whatsapp) digital platforms. Physical goods may need to be shipped domestically or overseas; virtual goods and services (such as streaming video or a telehealth consultation) can be delivered digitally. In addition to digital tools (such as payment platforms), e-commerce depends on physical infrastructure for the warehousing and delivery of goods. E-commerce growth has implications for traditional methods of cross-border trade and domestic transport infrastructure, postal, and logistics systems. This topic also considers the degree to which businesses, particularly SMEs, use digital platforms (like e-commerce platforms) to interact with customers and streamline and protect internal processes.

Digital Trade

The U.S. International Trade Commission defines digital trade as "The delivery of products and services over the internet by firms in any industry sector, and of associated products such as smartphones and internet-connected sensors." This includes services such as cloud storage, software-as-a-service, banking and e-commerce platforms, and digital media content, as well as ICT hardware. Whereas e-commerce focuses on the purchase and delivery of physical goods, digital trade takes a broader view, including trade in digital services and media and emphasizing cross-border transactions. Digital trade facilitation refers to a range of topics from international payment services to e-signatures and digitized customs processes. Exploring this topic involves understanding how enterprises buy and sell goods and services across borders and what regulations and agreements shape their work.

Tech Startup Environment

The tech startup environment is an indicator of technological advancement in a country. Tech startups include both social enterprises and profit-oriented businesses focused on business services, transportation, or even gaming. In many developing countries, digital startups cater to an international market rather than aiming for local adoption. A promising startup environment can attract foreign investment, incentivize skilled IT professionals to remain in-country, and encourage innovation.

Digital Talent Pool

The digital talent pool describes the availability of skilled workers who can support the growth of the digital ecosystem in a country. This can range from IT technicians and specialists, to entrepreneurs, and from young STEM graduates to academics and policymakers. A digital talent pool can also include digital media professionals such as marketers, social media influencers, and journalists. A skilled digital talent pool can help build a strong, globally competitive digital economy and pave the way for a country's digital transformation.

PILLAR III: CROSS-CUTTING TOPICS

The examples below illustrate how the four cross-cutting topics may appear across Pillar 2 topics.

1. **Inclusion**

These examples use gender and disability to illustrate the role of inclusion in digital ecosystems. Other marginalized and vulnerable populations may experience similar challenges.

Gender: STEM is frequently seen as a "male" field, and men often participate in higher numbers in both higher education and the ICT workforce. From a young age, girls may be discouraged from entering STEM fields; the absence of women in visible roles may further discourage them. When women do enter ICT fields, they often face barriers to career advancement. Other barriers for women in the digital economy may include financial exclusion due to safety and social issues surrounding interactions with male agents, or due to a lack of products or services tailored to their needs.

Disability: Digital financial services and e-commerce platforms need to be accessible for persons with disabilities. ICT education programs can be developed in a way that enables and encourages inclusion of students with disabilities.

2. **Cybersecurity**

Cybersecurity in the digital economy involves measures that protect consumers and systems against cyber threats to the financial system and to e-commerce platforms. Ministries of Finance, central banks, commercial and microfinance banks, and FinTechs alike can ensure a cyber-secure financial sector. Threats include ransomware attacks and large-scale consumer data breaches.

3. **Emerging Technologies**

In the digital economy, AI and machine learning can be used to improve back-end business processes or customer-service chat bots. FinTechs also use AI, blockchain, and machine learning across a range of services such as digital banking, credit scoring, and predictive analytics. Cryptocurrencies and other digital assets are challenging regulators and central banks around the world by enabling the creation of currencies that are outside the control of any state institutions.

4. **Geopolitical Positioning**

Geopolitics may affect a country's digital trade policies, such as their accession to the World Trade Organization.

If you are interested in learning more, please contact digitaldevelopment@usaid.gov.