USAID
FROM THE AMERICAN PEOPLE

DECA TOOLKIT

RESEARCH CHECKLIST

This document is your technical "North Star" to be used throughout the DECA.

Digital Ecosystem Country Assessment (DECA)

The DECA is a broad assessment and is not designed to be an authoritative, all-inclusive source. Each country's context is unique and may require the inclusion of additional topics; add them as pertinent.

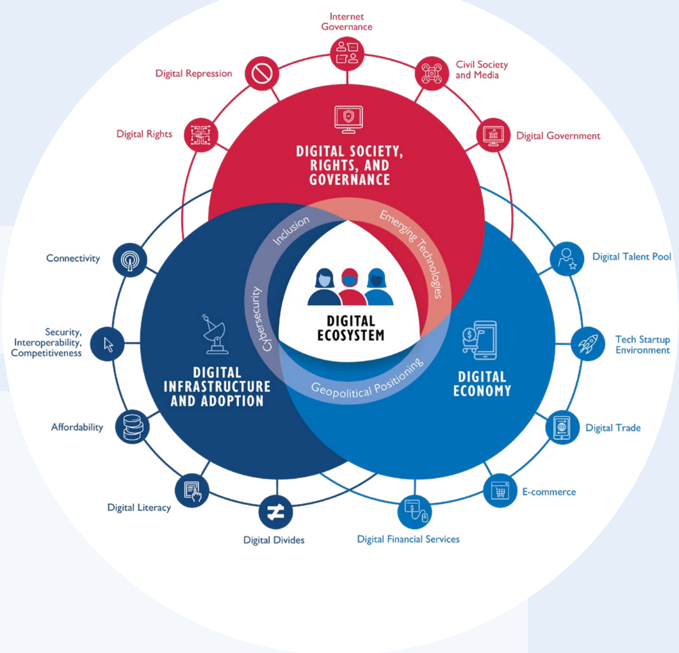
You should try to answer most of the questions in this checklist, but Mission priorities and country context may require being flexible.

This checklist is meant to help you, not make your life harder!

DigitalFrontiers
SCALING DIGITAL DEVELOPMENT

DAI
Shaping a more livable world.

INTRODUCTION TO THE RESEARCH CHECKLIST



○ Four cross-cutting topics are described first before the pillars.

For each DECA pillar this Checklist presents:

A CONCISE DEFINITION

THE IDEAL STATE

frames the "ideal" digital ecosystem for comparison, broken down at the government, institution, and individual levels:

1. Government level: the policy, legal, and regulatory environment detailing both content and processes that support a safe, inclusive digital ecosystem.
2. Institution level: the dynamics that enable private-sector actors, government entities, academia, civil society, and community-based institutions to seamlessly and safely access, leverage, and integrate digital technologies in their work.
3. Individual level: how individuals across demographic groups equally, easily, and safely engage with elements of the digital ecosystem. See the Inclusion Analysis section below for more ideas on how to address demographic groups of interest.

KEY STAKEHOLDERS

to guide interviewee identification

GUIDING QUESTIONS

- Help identify initial interviewees;
- Unpack the current state and its impact; and
- Reveal perceptions of a variety of relevant stakeholders.

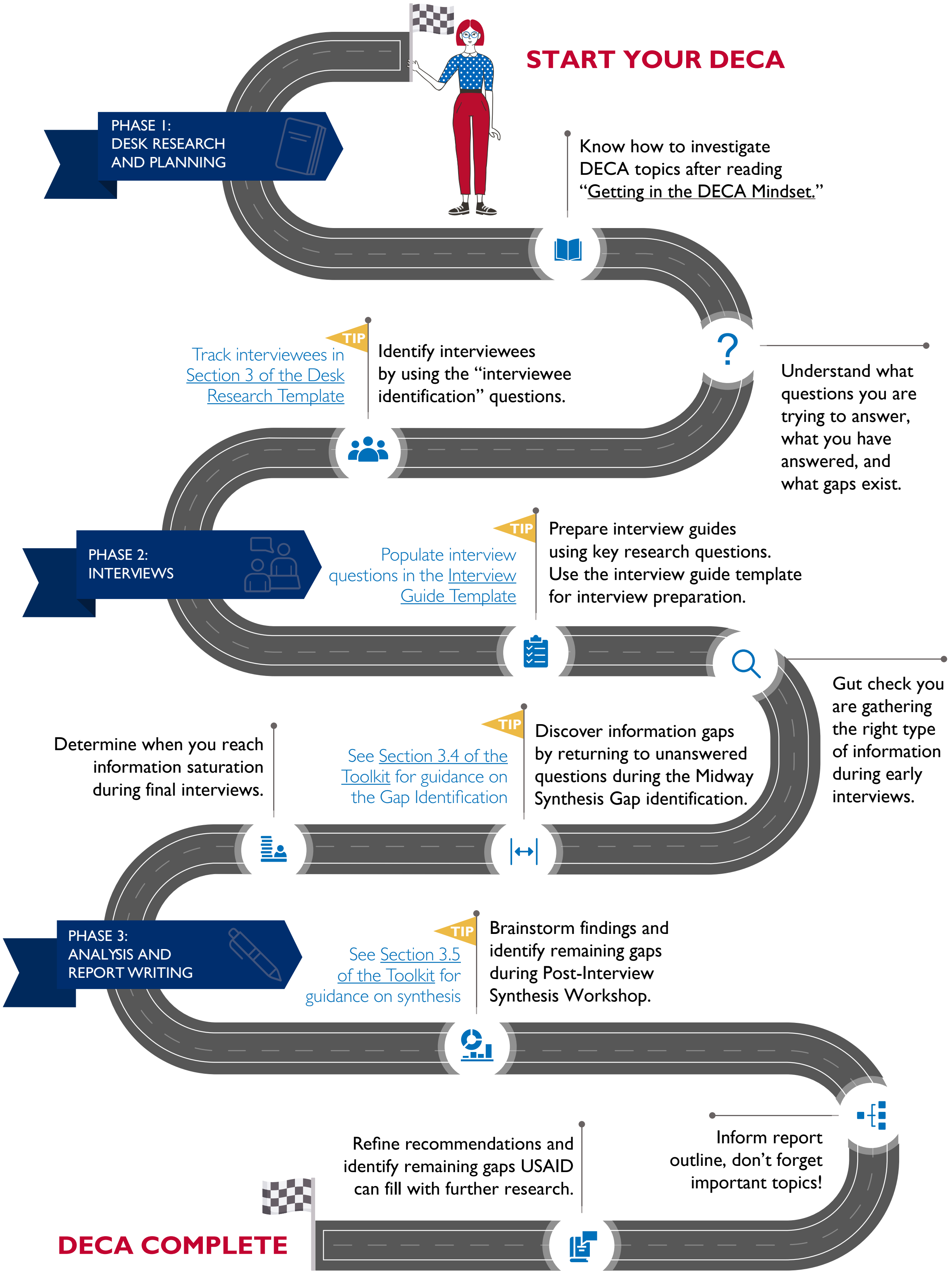
The *guiding questions* are arranged from more straightforward to more nuanced – current state and impact questions are always followed by perceptions questions. Questions that are earlier in these lists may be answerable during desk research, while later questions will be important to ask during interviews. DECA interviews can be maximized by making sure the desk research phase answers as many questions as possible. During the interview phase the guiding questions in this checklist can be tailored to be more conversational and match the background of each interviewee. Not all DECAs will answer every single question; depending on the country context, some topics may be more important or require more nuance than others.

KEY RESOURCES

These are not the only resources you should refer to, but they will serve as a good starting point for further exploration. Don't forget to use the detailed Desk Research Template and Desk Research Briefs to guide your research. If you need a refresher on the research topics, revisit the Getting in the DECA Mindset section of the Toolkit or Annex C of the Toolkit, digital ecosystem glossary.

RESEARCH CHECKLIST ROADMAP

When should you use this checklist?



START YOUR DECA

PHASE 1: DESK RESEARCH AND PLANNING

Know how to investigate DECA topics after reading "Getting in the DECA Mindset."

Understand what questions you are trying to answer, what you have answered, and what gaps exist.

Identify interviewees by using the "interviewee identification" questions.

TIP Track interviewees in Section 3 of the Desk Research Template

PHASE 2: INTERVIEWS

Prepare interview guides using key research questions. Use the interview guide template for interview preparation.

TIP Populate interview questions in the Interview Guide Template

Gut check you are gathering the right type of information during early interviews.

Discover information gaps by returning to unanswered questions during the Midway Synthesis Gap identification.

TIP See Section 3.4 of the Toolkit for guidance on the Gap Identification

Determine when you reach information saturation during final interviews.

PHASE 3: ANALYSIS AND REPORT WRITING

Brainstorm findings and identify remaining gaps during Post-Interview Synthesis Workshop.

TIP See Section 3.5 of the Toolkit for guidance on synthesis

Inform report outline, don't forget important topics!

Refine recommendations and identify remaining gaps USAID can fill with further research.

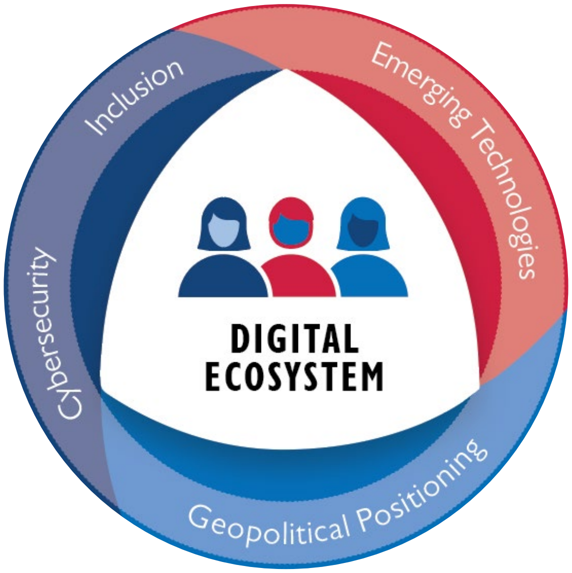
DECA COMPLETE

TABLE OF CONTENTS

INTERNET FREEDOM

CIVIL SOCIETY AND MEDIA

DIGITAL GOVERNMENT



CROSS-CUTTING TOPICS

The topics included in this section touch many areas of the DECA and should be explored in the context of various elements of a country's digital ecosystem. Therefore, in addition to the high-level questions below, questions about these topics are included throughout the checklist.

INCLUSION ANALYSIS

To understand the development implications of digital ecosystems, we need to pay specific attention to their implications for marginalized or vulnerable populations. As the USAID Education Policy puts it, "[t]hese populations vary by context, and frequently include girls, rural populations, individuals marginalized because of their sexual orientation, individuals with disabilities, indigenous peoples, and children and youth from poor households." Understanding the digital-specific implications of marginalization requires a systematic exploration of patterns of inequity and exclusion.

The Inclusion Analysis section of the Desk Review Template includes a series of high-level questions about the general state of inclusion and marginalization in the country. You'll want to complete this early in the research process, to identify particular populations as marginalized or vulnerable in your specific country context. Make sure to focus on dimensions of inequity and exclusion that relate to the digital ecosystem and how different marginalized or vulnerable identities may intersect. You'll need to refer back to this analysis at later points in the DECA to see how digital issues you're uncovering might impact each of these groups. The term "digital divide" is commonly used to describe disparities in access (see Pillar 1), but other aspects of inclusion should be considered.

GUIDING QUESTIONS

- ☐ How is the digital ecosystem shaped by the marginalization or inclusion of:
  - Women and girls?
  - Youth?
  - Elderly people?
  - Religious or ethnic groups, including immigrant and Indigenous communities?
  - Refugees, migrants, and internally displaced persons?
  - Persons with disabilities?
  - Gender and sexual minorities, and LGBTQI+ communities?
- ☐ Which specific demographic groups or geographic areas are specifically targeted by Mission programming? Are certain elements of inclusion prioritized in Mission or host-country government strategies?
- ☐ What is the geographic distribution of wealth? Are development challenges (including conflict and instability) concentrated in some parts of the country?
- ☐ What major differences exist between urban, rural, and peri-urban areas?
- ☐ To what degree do large economic actors dominate the dynamics, competitiveness, and equitability of the digital ecosystem (e.g., digital platforms, large incumbent banks)? How does this concentration of economic or market power influence the agency of individuals and businesses seeking to shape or participate in the digital ecosystem?

KEY RESOURCES

- G3ict (The Global Initiative for Inclusive ICTs) website
- WomanStats (global comparisons on women's inclusion and their physical, legal, and economic security)
- Indicators on youth unemployment, literacy, and more (World Bank)
- Women, Business, and the Law (World Bank)
- Disability Data Portal (country-level data on inclusions of persons with disabilities, organized around the Sustainable Development Goals)
- Migration Data Portal
- Refugee Statistics (UNHCR)
- Social Acceptance of LGBT People in 174 Countries (UCLA)
- Country-specific research by institutions such as LIRNEAsia, Research ICT Africa

CYBERSECURITY

Cybersecurity is the way people, systems, and technology protect digital information from being stolen, manipulated, controlled, deleted, or otherwise exploited by malicious actors. The topic includes understanding not only the technical measures taken by computer engineers to protect digital systems, but also the broader security threat landscape, local technology trends, government policies, and levels of governmental and social cyber awareness and capacity.

A DECA explores elements of cybersecurity at the geopolitical, governmental, institutional, and individual levels and includes topics such as the existence of cybersecurity policy, regulation, and standards; government processes and capacity to address cyber threats; the safety of critical internet infrastructure (CII), institutional response plans to cyber breaches; and individual-level understanding of and protection against cyber threats.

KEY RESOURCES

- USAID Cybersecurity Primer (USAID, 2021)
- Integrating Cyber Capacity into Digital Development Agenda (GFCE, 2021)
- Cyber-Security Maturity Model Assessments (World Bank, 2020)
- Global Cyber Security Capacity Centre: CMM Reviews around the World (University of Oxford)
- Global Cybersecurity Index [International Telecommunication Union (ITU), 2020]
- National Cybersecurity Strategies repository (ITU)
- Digital Society Project
- Global Forum on Cyber Expertise
- Cybil
- Holistic Security Manual (Tactical Tech)

GUIDING QUESTIONS

□ Have specific laws, policies, and regulations been instituted to counter cybercrime and/or promote cybersecurity for the government, private sector, civil society, and individuals? What are they?

□ Does a National Cybersecurity Strategy exist? If so, what part of the government has authority over implementing this strategy? Does an implementation strategy or roadmap exist?

□ Has the government established a Computer Emergency Response Team (CERT) or similar mechanism to respond to and manage major cyber attacks? Are there any other means for providing national or local-level cybersecurity services? What are they?

□ What are the responsibilities of the national CERT? How is it administered, staffed, and funded? What recent actions has it taken?

□ Has the government set cybersecurity standards (for example, the U.S. has adopted the NIST Cybersecurity Framework)? If so, has it shown the capacity to implement and enforce these standards? Does the government have a Standardization Body? Which external model from another country or international institution were the standards based on? Was technical assistance received to define and implement the standards? If so, from whom?

□ What is the general assessment of the local cybersecurity market? Is it sufficient to respond to the country's cybersecurity needs?

□ How sophisticated are lawmakers in their understanding of cybersecurity? Are there legislative committees or executive branch departments devoted to cybersecurity, digital transformation, or IT?

□ What cybersecurity practices are common among different actors (government, private sector, civil society)? These might include: cyber threat landscape assessments, monitoring of access and data flows, continuous information technology (IT) systems upgrading, and whole-of-institution response plans for cyber breach or catastrophic systems failure.

□ How strong is the cybersecurity talent pool in the country? What are the limiting or supporting factors in the cybersecurity talent pool?

□ What kinds of cybersecurity higher education degrees or vocational training exist in the country? What practical cybersecurity training tools (e.g. cyber ranges and other specialized software/hardware) do students have access to?

□ What are the primary cybersecurity needs of public and private sector organizations (products and services)?

□ How do public and private sector organizations ensure that their cybersecurity needs are met? Do they create internal positions, hire contractors, hire domestic or international firms, etc?

□ What are the most significant cyber threat trends in the country? Who are the primary victims or targets? Who are the primary perpetrators?

□ How do different stakeholders (e.g., private sector, public sector, civil society, media) perceive the importance of cybersecurity?

□ How do different stakeholders (e.g., private sector, public sector, civil society, media) perceive the imminence of cybersecurity threats?

EMERGING TECHNOLOGIES

Emerging technologies are those for which ethical, policy, and regulatory frameworks are struggling to keep pace with the rate of technological progress. These include artificial intelligence (AI), the internet of things (IoT), blockchain, drones, and 3D printing. As these technologies become more affordable and widespread, they may have a significant impact on digital ecosystems and on development more broadly.

For the DECA, we're mostly concerned with the enabling environment for emerging technologies. Rather than chasing down every example of where emerging technologies are being used (or could be used), we want to focus on how policy or market conditions are shaping the deployment of these technologies. The people best positioned to illustrate or explain the enabling environment may be local researchers or entrepreneurs who are trying to deploy these technologies.

GUIDING QUESTIONS

- □ What kind of strategies or policy framework has the government released for emerging technology? Strategies and policies sometimes focus on a particular technology (e.g., AI) and may focus on a specific sector (e.g., defense).
- □ If a framework exists, what does it include? How do inclusions and omissions compare with what other countries are doing? How is it being implemented (with what resources, and by whom)?
- □ Where does the funding for emerging tech projects/hubs come from? Are local investors excited about emerging tech?
- □ Which industry or higher-education groups are focusing on emerging technology? How is civil society involved in shaping norms or influencing policies, particularly regarding risks?
- □ How do different stakeholders perceive the quality and quantity of the country's emerging-tech workforce?
- □ What do different stakeholders perceive as the barriers for successful adoption of emerging technology?
- □ How does the population perceive the changing technology landscape? How are issues covered in the media? How does this compare against other countries?
- □ What conversations are happening about the ethical or responsible use of emerging technology? Are issues such as algorithmic bias and workforce automation getting much attention in the national press?

KEY RESOURCES

- Artificial intelligence topic page at USAID.gov
- Making AI Work for International Development (USAID, 2018)
- Artificial Intelligence in Global Health: Defining a Path Forward (USAID, 2019)
- Managing Machine Learning Project in International Development: A Practical Guide (USAID, 2021)
- AI Policy Observatory and Blockchain Resources [Organisation for Economic Co-operation and Development (OECD)]
- An Overview of National AI Strategies (Politics + AI Medium page, 2018)
- National and International AI Strategies (Future of Life Institute)
- Which Governments Are Researching Central Bank Digital Currencies Right Now? (Consensys, 2021)
- Global AI Index (Stanford University HAI; mostly focused on wealthier countries, but includes India and South Africa)
- AI Needs Assessment Survey in Africa (UNESCO, 2021)

GEOPOLITICAL POSITIONING

Each country-level digital ecosystem exists in a global context and is impacted by the actions of other countries. One specific area of concern is the influence of authoritarian states—including but not limited to the People's Republic of China (PRC) and the Russian Federation—which are actively working to shape the global digital space.

It is important for USAID Missions to understand how these global dynamics are playing out in the countries where they work and how global technology rivalries can affect development. While an in-depth geopolitical analysis is beyond the scope of the DECA, we should aim to give Missions a high-level overview of what's happening and help them decide whether more detailed research is needed.

KEY RESOURCES

- China.aiddata.org (includes datasets on PRC public diplomacy and development assistance)
- Networking the "Belt and Road"—The future is digital (MERICS)
- China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism (Council on Foreign Relations, 2019)

GUIDING QUESTIONS

☐ Is the country part of the Digital Silk Road initiative of the PRC? Which projects exist or are being planned?

☐ Have government officials participated in technology-focused training or capacity-building seminars hosted by authoritarian states? Highlight a few.

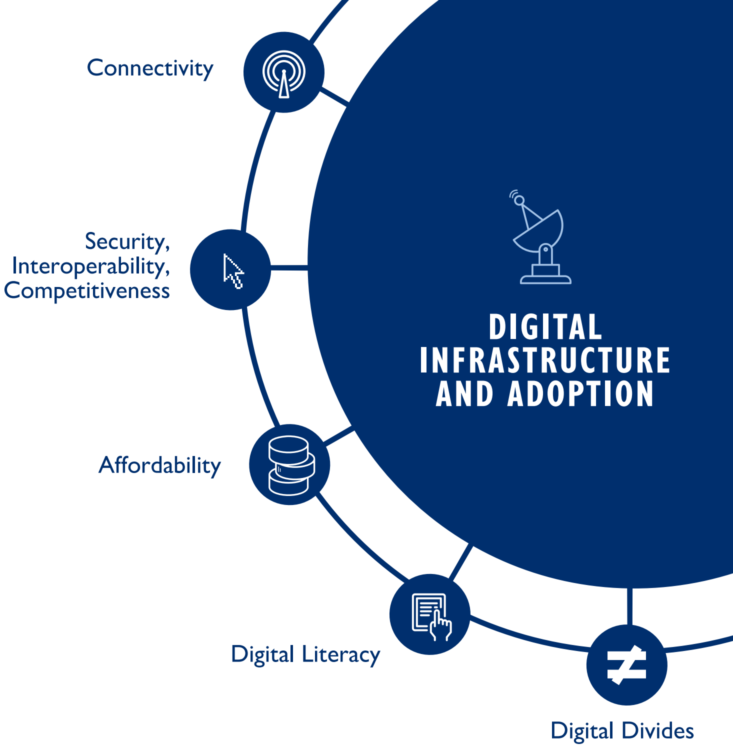
☐ What countries are providing the partner-nation government with technical assistance in technology and cybersecurity initiatives?

Photo: Beth Rubenstein, Columbia University

PILLAR I

DIGITAL INFRASTRUCTURE AND ADOPTION

Digital Infrastructure and Adoption, refers to the resources that make digital systems possible and how individuals and organizations access and use these resources. Digital infrastructure includes geographic network coverage, network performance, internet bandwidth, and spectrum allocation as well as telecom market dynamics around security, interoperability, and competitiveness. This pillar also examines behavioral, social, and physical barriers and opportunities for equitable adoption (digital divides, affordability, and digital literacy[1])—who uses and does not use digital technologies and why.


Connectivity
Security, Interoperability, Competitiveness
DIGITAL INFRASTRUCTURE AND ADOPTION
Affordability
Digital Literacy
Digital Divides

[1] 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 and social life. This may include competencies variously referred to as computer literacy, information and communication technology (ICT) literacy, information literacy, and media literacy.

PILLAR I

IDEAL STATE

GOVERNMENT/POLICY LEVEL

1. The telecommunications market is competitive with fair access to state-controlled resources and to other suppliers' networks and affordable access for secondary suppliers like internet service providers (ISPs).

2. The telecommunications regulator is independent of any supplier of basic telecommunications services (e.g., ISPs, mobile network operator (MNO)).

3. The legal and regulatory environment supports innovative approaches to expanding ICT infrastructure, particularly for marginalized or vulnerable populations (e.g., universal service fund).

4. Robust and well-resourced authorities exist for the transparent and accountable oversight of ICT infrastructure (including long-haul fiber optic cable networks, 4G mobile networks, high-bandwidth local networks, etc.). These authorities are successful at enforcing laws, regulations, and policies.

5. Telecommunications rulemaking is transparent, including an opportunity for public input.

6. Policy, regulation, and standards exist to ensure the cybersecurity of critical internet infrastructure (CII).[2]

7. Policies exist to support digital inclusion, with plans for expanding digital literacy and promoting equitable access and use of digital tools and services.

INSTITUTION LEVEL

1. All institutions can affordably access and use the internet.

2. The private sector and civil society organizations (CSOs) are working to increase last-mile connectivity, potentially using new and innovative technologies.

3. ISPs offer services at an affordable rate.

4. A community of CSOs and researchers are working on digital inclusion issues including digital divides, digital literacy, and creation of locally relevant content. (Refer to Inclusion Analysis.)

5. Cloud computing services are affordable, accessible, secure, and widely used.

[2] CII is essential hardware and software components that internet services rely upon. Hardware CII include fiber optic cables, wires, or routing equipment; software CII may include Domain Name System (DNS). storage systems, or authentication and authorization services,

PILLAR I

IDEAL STATE

INDIVIDUAL LEVEL

1. The internet is accessible to all.

2. Access to the internet is sufficiently available, fast, and affordable so coverage is universal and users can take advantage of all associated economic and social opportunities.

3. The infrastructure allows reliable fixed broadband for quality mobile access to the internet.

4. Use of digital tools at the basic level is equitable, easy, and accessible for all. This includes the availability of locally relevant content for all users.

5. Opportunities to build digital literacy (including cyber hygiene) are available and accessible to all.

6. All individuals understand the importance of cyber hygiene and know how to safely use and navigate digital platforms, tools, and services.

7. Social norms do not hinder access to and use of digital tools and services for marginalized or vulnerable populations. (Refer to Inclusion Analysis.)

8. Digital tools and services do not deepen power inequities. (Refer to Inclusion Analysis.)

KEY STAKEHOLDERS

- ISPs (try to include both large and small providers)
- MNOs (try to include both large and small providers)
- Telecommunications regulator
- CSOs working in digital inclusion
- NGOs or private-sector companies working in alternative connectivity solutions
- Media influencers/outlets
- Technologists/digital activists
- ICT Trade Associations
- Academia/Research Institutions
- Other donors
- USAID implementing partners
- Large tech companies (e.g., Google, Microsoft)
- U.S. Embassy Interagency: State Econ Officers, Commerce digital attachés, others depending on country team

Photo: USAID/Georgia

CONNECTIVITY INFRASTRUCTURE

INTERVIEWEE IDENTIFICATION

□ With respect to telecommunications infrastructure, who are the major stakeholders? (e.g., ISPs, regulators, MNOs, consumer institutions)

□ What stakeholders are engaged in alternative or innovative connectivity solutions? (e.g., ISPs, local institutions, private sector, academia, regulators)

CURRENT STATE AND IMPACT

□ What does internet coverage look like across the country? Is there a rural/urban divide?

□ Which areas of the country are farthest behind in digital infrastructure coverage?

□ What are the biggest barriers to increasing connectivity? (e.g., geography, infrastructure, policy, affordability, political economy)

□ Who manages fiber optic backbone networks? How do the networks managed by different operators compare in terms of quality and geographic reach?

□ What does mobile network coverage (2G, 3G, 4G, 5G) look like throughout the country? Are there plans for expansion? If yes, what actors will be responsible for the expansion?

□ Is there a universal service fund? If yes, how is it managed? How does this impact the inclusivity of digital infrastructure?

□ Is there a National Broadband Plan? Which issues does it focus on (e.g., expanding internet access, regulating the telecommunications market, guiding e-government services, fostering a digital economy)?

□ What policies (if any) are in place to motivate ISPs to increase last-mile connectivity?

□ What public-private partnerships exist for connectivity? (e.g., to build smart cities, internet exchange points, alternative connectivity solutions)

□ What alternative connectivity solutions exist? (community networks, TV White Space, WiFi relays, etc.)

□ What are universities and research institutes doing to develop innovative connectivity solutions?

EMERGING TECHNOLOGIES

□ Are emerging technologies (e.g., AI, cloud computing) being used in the telecom industry? If yes, by which actors? For what purposes?

GEOPOLITICAL POSITIONING

□ What is the role of foreign telecommunications companies and equipment manufacturers, particularly Huawei and ZTE?

□ What foreign companies are providing internet services in the country, where are they from, and what regulations are they adhering to?

CONNECTIVITY INFRASTRUCTURE

PERCEPTIONS

- □ How is the policy, legal, and regulatory environment for telecommunications perceived in terms of capacity, transparency, impartiality, and accountability?
- □ How do different stakeholders (consumers, businesses, government) perceive the reliability of existing internet infrastructure?
- □ How do perceptions of infrastructure reliability shape its use?
- □ Are different stakeholders (individuals, businesses, service providers) accessing and using telecommunications to the fullest capacity? If not, what is holding them back?

EMERGING TECHNOLOGIES

- □ How do ISPs perceive the opportunities and challenges around providing last-mile connectivity?
- □ Do ISPs embrace disruptive and emerging technologies to strengthen their competitive advantage?

KEY RESOURCES

- Mobile Connectivity Index (GSMA)
- Coverage Maps (GSMA)
- Interactive Transmission Maps (ITU)
- Network Readiness Index (Portulans Institute)
- Inclusive Internet Index (The Economist Intelligence Unit)
- Microsoft Airband (Microsoft)

Photo: USAID/Jordan Competitiveness Program

INTERVIEWEE IDENTIFICATION

- □ In the ICT market, who are the major stakeholders? (e.g., ISPs, regulators, MNOs, fiber optic or cable providers, satellite firms, community networks, consumer institutions, university research and education networks, advocacy organizations, ICT trade associations)
- □ Which research institutions or academics have studied the country's telecommunications and ICT sector?

CURRENT STATE AND IMPACT

- □ How competitive is the telecom market? What are the market shares for mobile voice and broadband service, fixed internet access service, middle-mile transport, data centers, undersea cable landing stations, and international internet gateways? (Note that these are separate and important markets for analysis.)
- □ What are the roles and structure of the regulator and/or Ministry of ICT? Is the regulator independent? What else could they be doing?
- □ Does the regulator or Ministry of ICT collect or publish data on availability, competition, price, and adoption? Do those data match the data of independent researchers?
- □ What is the extent of government ownership of firms in the market? Are there "national champions" in which the government owns or controls a stake? Do they compete on a level playing field with others?
- □ Does the government or regulator subsidize network deployment initiatives in underserved or unserved areas (such as through a universal service system)? If so, does the government award these subsidies through a transparent competitive mechanism (e.g., auction) that allows for and facilitates competition and choice?
- □ What are the processes for, policies for, and status of spectrum allocation? How does this impact telecom market competition? Does the government encourage competition between providers for spectrum licenses (e.g., through competitive bidding) or does the government use "beauty contests" or tenders to award licenses (in a potentially non-transparent way)?
- □ Is spectrum held or reserved for community use or access? Which policies are in place for shared spectrum access? Or is all spectrum licensed exclusively to existing providers?
- □ Who controls access to infrastructure—such as utility poles, rights-of-way on roads and highways, electric grid towers and rights-of-way, railroad easements—that are critical inputs to building networks? Is it the national government, local governments, private firms, or state-backed companies? Does the government have a policy to allow competitors access to these inputs? If so, are prices for that access regulated or monitored?
- □ Are providers allowed to reduce costs by sharing basic infrastructure such as towers and fiber-optic backhaul? Does the government have policies that allow for collocation of equipment on towers?
- □ Is it easy to make calls across network providers, or transfer your service from one carrier to another? Are there other barriers to interoperability?
- □ How is internet and data traffic exchanged between providers? Is there a robust market of independent internet exchange points and data centers in which interconnection and internet traffic exchange happen, or does the government or dominant firm control the location, manner, and nature of that exchange?
- □ What policies (if any) does the government have for licensing the equipment that is deployed in networks? Does it require interoperability? Are there industry organizations or working groups that ensure interoperability and exchange of traffic between different providers?

CYBERSECURITY

□ What policies and systems are in place to protect CII such as fiber optic cables, internet exchange points, undersea cable landing points, data centers, and cloud storage systems?

□ What policies, regulation, and legislation exist requiring internet and mobile providers to prevent and address cybersecurity threats?

□ What barriers or obstacles limit compliance? To what extent do institutions have the capacity to comply? What resources would help them comply? What resources are available to build their cybersecurity capacity?

GEOPOLITICAL POSITIONING

□ Is foreign ownership of internet providers, MNOs, fiber cable, data centers, or other digital infrastructure allowed? If so, what is the extent and level of foreign investment and ownership?

□ What is the presence of foreign firms (especially Western and Chinese) in the cloud computing and data center market (e.g., Amazon Web Services, Google Cloud)? What type of equipment is used in those data centers? What is the country of origin for the equipment?

□ Who are the main suppliers of network technology and equipment? What is the role of foreign technology companies (particularly Chinese) in the country's networks?

□ Are providers seeking diverse sources of supply for network equipment, through trials of interoperable equipment such as open radio access network (ORAN) technology? What technology is in trials or new deployments, and is that equipment designed to be interoperable?

□ Are internet and mobile providers in the market members of organizations that promote equipment vendor diversity, such as the O-RAN Alliance or Telecom Infra Project? Are trials underway with open radio access network technology?

PERCEPTIONS

□ Is the telecommunications market perceived as competitive, well-regulated, and fairly priced?

□ Are the telecommunications regulator and government perceived as being fair in implementing and enforcing telecommunications competition rules and policies—or is it perceived as favoring certain providers or firms?

□ If some "national champions" or firms have significant government ownership, how do others perceive competing with them?

□ What is the perception of the extent of PRC influence in the sector?

CYBERSECURITY

□ How widely trusted are the telecommunications systems?

□ How is the security of CII perceived by different stakeholders (government, private sector, CSOs, individuals)? Do cybersecurity perceptions impact adoption and use of ICT services in the country?

KEY RESOURCES

- Telecoms and Digital Economy Research (BuddeComm; may require paid access to specific reports)
- GSMA Intelligence data (paid subscription)
- Alliance for Affordable Internet (A4AI)
- Country-specific connectivity reports by World Bank, Inter-American Development Bank, Asian Development Bank, and similar institutions

AFFORDABILITY

CURRENT STATE AND IMPACT

□ How do mobile broadband data package costs compare to the Alliance for Affordable Internet's target of 2 percent or less of gross national income per capita?

- What factors influence the price of mobile broadband? (e.g., policy and regulation, market dynamics, geography)
- How does the price of mobile broadband impact the way people use the internet? Do cost-driven behaviors differ for marginalized or vulnerable populations? (Refer to Inclusion Analysis.)

□ How do device (mobile handset and smartphone) prices compare to those in similar countries? (see GSMA MCI)

- What factors influence the price of mobile phones? Basic versus feature versus smartphones?
- Across demographic groups, how do device costs impact the way people use digital tools and services? (Refer to Inclusion Analysis.)

□ To what extent do individuals have prepaid versus postpaid mobile accounts? How do people "top-up" mobile accounts?

□ What applications are zero-rated (e.g., Facebook's Free Basics program)?

GEOPOLITICAL POSITIONING

□ How popular are devices manufactured by PRC-based companies (e.g., Huawei, ZTE). Why are they popular?

INTERVIEWEE IDENTIFICATION

□ What stakeholders are engaged in policy, regulation, legislation, and implementation that affect internet affordability? (e.g., government, ISPs, private-sector tech companies, MNOs, academic researchers, CSOs, ICT trade associations)

PERCEPTIONS

□ How is the value of mobile broadband (internet) perceived differently by different groups? (e.g., value in terms of relative cost, things you can do with versus without it, is it needed to do your job)

□ What kind of mitigating strategies do consumers practice to "save" the cost of mobile broadband access or device ownership? (e.g., using multiple SIM cards, using only zero-rated apps, using prepaid accounts)

□ What is the best lever for increasing affordability of mobile broadband? What actors have the resources and motivation to do so?

KEY RESOURCES

- Mobile Broadband Affordability (A4AI)
- Good Practices Database (A4AI)
- Mobile Connectivity Index (GSMA)

DIGITAL LITERACY

CURRENT STATE AND IMPACT

- □ What government strategies or policies address digital literacy? How do they define it? To what extent are these policies implemented?
- □ What national or local curricula are in place for teaching digital literacy? How do these curricula define digital literacy?
- □ Are general digital skills taught in schools? What kind of digital skills? At what level? (primary, secondary, higher education)
- □ What options exist for someone wanting to learn digital skills? How accessible are they across demographic groups? (Refer to Inclusion Analysis.)
- □ How are digital literacy levels defined, tracked, and reported in the country? Are there any digital literacy divides? If so, what divides have the largest gaps?
- □ How do digital literacy levels vary across different demographic groups? (Refer to Inclusion Analysis.) How do these differences impact individuals' ability to safely access and receive services, productively contribute to the economy and society, and engage socially?

CYBERSECURITY

- □ Is cyber hygiene included in any digital literacy curricula, programming, or training? What skills do the curricula include (e.g., awareness of social engineering, phishing, and ransomware; risk mitigation and response measures)?

PERCEPTIONS

- □ How do different stakeholders (government, civil society, education institutions) perceive digital literacy programs and policies? What are their benefits perceived to be?
- □ Is low digital literacy viewed as a barrier to accessing and receiving services, productively contributing to the economy and society, and engaging socially? By whom?

INTERVIEWEE IDENTIFICATION

- □ What stakeholders are engaged in research, policy making, advocacy, or programming on digital literacy? (e.g., academia, technologists, CSOs, government ministries, development institutions, donors, media influencers/outlets)

CYBERSECURITY

- □ How do different stakeholders (individuals, government, civil society, private sector, academia) understand and perceive the benefits of learning good cyber hygiene?

KEY RESOURCES

- DigComp framework (EU Science Hub)
- A Global Framework of Reference on Digital Literacy Skills (UNESCO, 2018)
- UNESCO Institute for Statistics database
- Skills for a Digital Age Matrix (Caribou Digital, 2019)

DIGITAL DIVIDES

CURRENT STATE AND IMPACT

□ What are the most significant digital divides in the country?

□ How common are basic/feature phones? How does their availability vary across demographic groups and for marginalized or vulnerable populations? How does it impact access to and uptake of digital services? (Refer to Inclusion Analysis.)

□ How does access to connectivity, devices, and digital services differ for marginalized or vulnerable populations? (Refer to Inclusion Analysis.)

□ Why do digital access disparities exist? Who benefits from the status quo, and who might be motivated to challenge it?

□ To what extent are digital content, tools, and services adapted to meet the needs of marginalized or vulnerable populations (e.g., disabled, illiterate, or linguistic minorities)?

– What stakeholders are using these adaptations and with what populations?

– How effective and sustainable are they?

□ Do use habits differ for marginalized or vulnerable populations/groups? (Refer to Inclusion Analysis.) What factors contribute to these differences (e.g., affordability, connectivity, social norms, degree of digital literacy)?

□ To what extent is locally-relevant content available through digital channels?

□ To what extent does an individual's level of access to digital technologies impact their ability to access and receive services and information, productively contribute to the economy and society, and engage socially?

□ How are offline digital solutions used to reach last-mile and harder-to-reach populations? (e.g., including offline apps and innovations like the TalkingBook)

PERCEPTIONS

□ What is the best lever for closing digital divides, and what actors might have the resources and motivation to do so?

□ What do different stakeholders perceive as the underlying causes of barriers to access for marginalized or vulnerable populations?

INTERVIEWEE IDENTIFICATION

□ What stakeholders are engaged in research, policy making, advocacy, or programming around digital divides? (e.g., academia, CSOs, advocates for marginalized or vulnerable populations, government ministries, development institutions, donors, private sector, technologists, digital activists, media influencers/outlets)

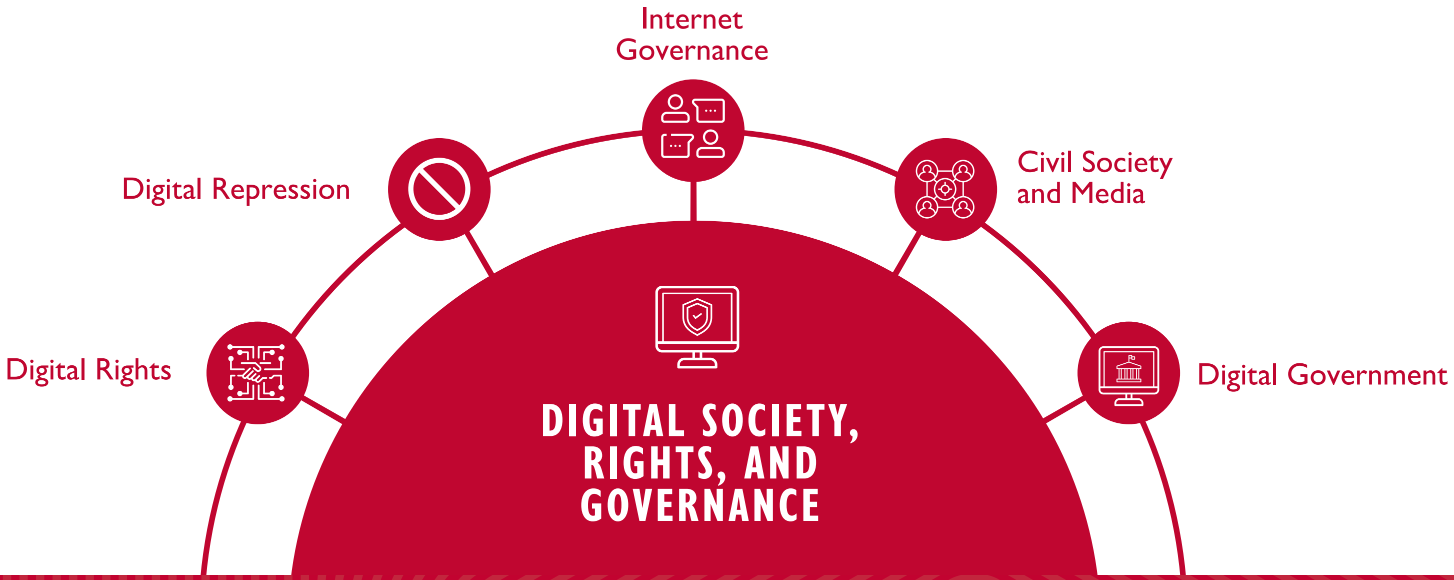
KEY RESOURCES

- Global Gender Gap Report (World Economic Forum, 2020)
- Mobile Disability Gap Report (GSMA. 2020)
- Connected Women: Mobile Gender Gap Reports (GSMA)
- Engendering ICT Toolkit (World Bank)
- The Gender Digital Divide Primer (USAID, 2020)
- Gender Digital Divide (GDD) Risk Mitigation Technical Note (USAID)
- Gender Digital Divide (GDD) Gender Analysis Technical Resource (USAID)
- Bridging the digital gender divide (OECD, 2018)
- World Report on Disability (WHO) (10 commitments)
- Google Trends

PILLAR II

DIGITAL SOCIETY, RIGHTS, AND GOVERNANCE

Digital Society, Rights, and Governance, focuses on how digital technology intersects with government, civil society, and the media. This pillar is divided into three sub-pillars: Internet Freedom; Civil Society and Media; and Digital Government. Internet Freedom explores factors that enable or constrain the exercise of human rights and fundamental freedoms online. This includes individual rights to freedom of speech, privacy, and free assembly, and the abuse of these rights through digital repression. Civil Society and Media identifies key institutions and how they report on, advocate around, and influence online freedoms. Digital Government looks at the government's efforts to manage internal information technology processes and systems, deliver citizen- and business-facing e-services, and engage with the public through digital channels.



PILLAR 2

IDEAL STATE

GOVERNMENT/POLICY LEVEL

1. ICT policy and regulations are designed to facilitate innovation and free expression online while also guarding against privacy abuses, cybercrime, trafficking in people and illicit goods, exploitation of children, violent extremism, the spread of disinformation and hate speech, and undue risk to consumers.

2. The rulemaking process for all ICT policy, regulation, and legislation is transparent, participatory, and inclusive.

3. Digital technologies are an integrated part of the governments' modernization strategies and are included in relevant national policy documents and visions. Country-level digital strategies enable collective action across the government and support its ability to deliver services, manage back-end systems, and engage with citizens.

4. Governments use digital technologies to create public value. Digital government platforms are interoperable (when appropriate) and provide access to government services through desktop, mobile, and other devices.

5. Data governance policies support the use of data for achieving development outcomes, while protecting individuals' privacy and safety and enabling cross-border data flows without localization requirements.

6. Government personnel have sufficient cybersecurity capacity to ensure effective cyber threat prevention and response for all digital government systems.

7. If a national digital ID system exists, it is inclusive, secure, and reliable and enables government service delivery.

8. Government-held data are open, freely available, and in a usable format, and the government promotes open government data including through the existence of a government-wide open data policy.

9. Multi-stakeholder internet governance forums exist, meet regularly, and are active in discussing and shaping policy.

10. Law enforcement and criminal investigation authorities are well equipped to a) detect and react to cyber crimes and b) cooperate across jurisdictions to adapt to cross-border threats. This includes the existence of a national Cyber Incident Response Team (CIRT), CERT, or a Computer Security Incident Response Team (CSIRT).

11. Regulatory requirements for cybersecurity include considerations for marginalized or vulnerable populations. (Refer to Inclusion Analysis.)

12. Digital surveillance by law enforcement or other government agencies takes place only within clear legal boundaries.

13. Online censorship, content blocking, and internet shutdowns are rare or nonexistent.

14. On paper and in practice, laws, policies, or regulations exist that constrain actions by the government itself and other domestic and foreign actors in the digital space.

15. Individual digital rights are formally protected by law, including online freedoms and rights and data privacy in accordance with Article 19 and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), respectively.

16. Policies and systems exist to protect children from digital harm.

PILLAR 2

IDEAL STATE

INSTITUTION LEVEL

1. Private-sector firms can fairly compete for government ICT contracts.

2. Institutions can rely on the national digital ID system for secure, transparent, reliable service delivery.

3. Open government data are available and accessible to all institutions, potentially enabling improved service delivery for everyone across all sectors.

4. Private-sector, academic, and civil society actors understand the importance of data governance (data production, use, protection/ privacy, etc.) and take active steps to advance human rights throughout the digital sector.

5. Private-sector actors and CSOs are involved in transparent, multistakeholder internet governance institutions.

6. Cybersecurity products and services are widely understood and used by private-sector firms and CSOs.

7. Private domestic and foreign online media and CSOs are not subject to censorship or intimidation, and do not self-censor.

8. Media influencers and outlets have public codes of conduct for moderating content and provide public reports on requests and removals.

9. CSOs and digital activists can effectively organize online, advocate for, and raise awareness about digital rights issues like freedom of expression online.

INDIVIDUAL LEVEL

1. People can access government services online safely, easily, and efficiently.

2. The vulnerability and risk exposure of all users, particularly those from opposition and watchdog organizations, and marginalized communities, is minimized. (Refer to Inclusion Analysis.)

3. People do not feel limited in their freedom of expression online and have many opportunities and platforms to engage freely in online political dialogue.

4. People (including those from marginalized or vulnerable populations) can access a variety of different digital media platforms.

5. Public trust in the media is high, and a variety of viewpoints are represented through accessible and affordable platforms.

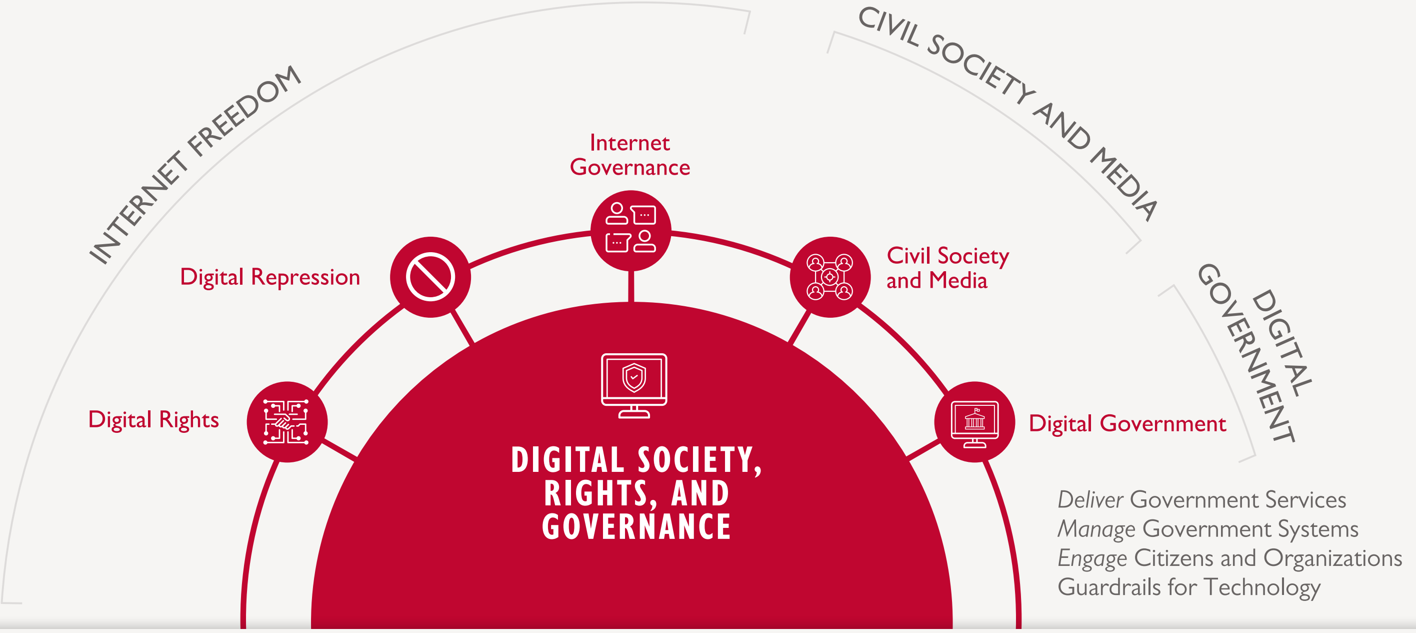
6. The importance of data protection and privacy is widely understood and reflected in terms of service agreements and built-in security and privacy features.

7. Media literacy among the population is sufficient such that individuals can identify misinformation and disinformation online.

KEY STAKEHOLDERS

- Government ministries
- Public media institutions
- Private media institutions
- Media influencers
- Civil society watchdog institutions
- Internet Governance Forum members/ stakeholders
- Academia/research institutions
- Independent think tanks
- Former government officials
- Religious leaders/ institutions

PILLAR 2 IS DIVIDED INTO THREE SUB-PILLARS


INTERNET FREEDOM
CIVIL SOCIETY AND MEDIA
DIGITAL GOVERNMENT
Internet Governance
Digital Repression
Civil Society and Media
Digital Rights
Digital Government
DIGITAL SOCIETY, RIGHTS, AND GOVERNANCE
Deliver Government Services
Manage Government Systems
Engage Citizens and Organizations
Guardrails for Technology

INTERNET FREEDOM

explores elements of the digital ecosystem that enable and impede individuals and institutions to exercise human rights and fundamental freedoms online; it focuses on how digital rights are protected, repressed, and governed

CIVIL SOCIETY AND MEDIA

identifies key institutions and how they report on, advocate for, and influence freedoms online

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

INTERNET FREEDOM

DIGITAL RIGHTS

CURRENT STATE AND IMPACT

□ To formally protect digital rights, what laws exist regarding:

- Freedom of expression online
- Freedom of association online
- Data privacy and protection
- Content moderation

□ To what extent are these laws enforced? By whom?

□ Do these laws exist within a broader data governance framework or policy? Was this policy based on any existing frameworks?

□ How do the laws, regulations, and policies that protect digital rights impact different stakeholders? (businesses, CSOs, individuals)

□ When ecosystem stakeholders (ISPs, FinTechs, government agencies, etc.) collect personal information, what do they do to protect it? (particularly for marginalized or vulnerable populations including children; refer to Inclusion Analysis.)

- How is this ensured? Are individuals aware?
- How is consent of collection, storage, and sharing communicated and ensured?

□ Generally, do individuals, opposition political figures, journalists, and bloggers feel protected and safe when posting content online? If yes, why? Under what legislation are they protected?

□ To what extent do private-sector actors conduct human rights impact assessments (HRIAs)? How are they used? (e.g., Facebook's HRIA for Myanmar)

PERCEPTIONS

□ How comfortable do people feel engaging in political discussions online? To what extent do they fear arrest or attack? Do people engage using their own names or remain anonymous?

□ To what extent do different actors (individuals, CSOs, private sector, media influencers/outlets) believe they have human and legal rights to access, create, and publish content online?

□ How do people and institutions perceive their right to privacy from the government? From the private sector?

INTERVIEWEE IDENTIFICATION

□ What stakeholders advocate for the protection of digital rights including data privacy and protection, freedom of expression online, and safety for marginalized or vulnerable populations online? (e.g., CSOs, private-sector tech companies, government ministries, academics, religious institutions)

□ What government ministries address issues around freedom of expression online, data protection and privacy, and digital crimes?

KEY RESOURCES

- Freedom House Freedom on the Net
- Human Rights Watch
- Digital Society Project
- Transparency International
- Privacy International
- Global Tables of Data Privacy Laws and Bills
- Ranking Digital Rights Project
- Monitor.civicus.org
- The Citizen Lab
- ICCPR (see article 19 for protection of online rights and article 17 for data privacy)
- Google Transparency Reports
- Facebook Transparency Reports
- Twitter Transparency Center
- The Engine Room: Tech Tools for Human Rights Documenters

INTERNET FREEDOM

DIGITAL REPRESSION

NOTE: Throughout this topic, when digital repression "techniques" are referenced, they include the following five digital repression techniques:

- surveillance
- censorship
- social manipulation and harassment
- internet shutdowns
- targeted persecution against online users

See guidance on "Research in Closing Civic Spaces" on pg. 43 of the Toolkit document

CURRENT STATE AND IMPACT

☐ What state and non-state domestic and foreign actors have been accused of deploying digital repression techniques? (e.g., foreign and/or domestic government actors, private sector)

☐ What non-government actors are involved in spreading state-sponsored disinformation? (e.g., public and private media institutions, CSOs, private sector)

☐ How do non-government stakeholders enable digital repression? (e.g., private-public sector engagements, provision of surveillance technology, content filtering by ISPs)

☐ What digital repression techniques are commonly used, how are they used, and by what actors?

- What technological tools are used to pursue digital repression? (e.g., surveillance cameras, commercial malware, social media "botnets," access-blocking firewalls)
- How often do they occur?
- How do they impact different groups (individuals, businesses, CSOs, government actors)?

☐ How often are platforms that are used for online political engagement censored or shut down?

☐ Around what local, regional, or geopolitical topics is disinformation most prevalent and harmful to democratic norms and values?

☐ Are any marginalized or vulnerable populations explicitly targeted by digital repression, especially by targeted persecution tactics? (Refer to Inclusion Analysis.)

☐ To what extent are private domestic and foreign online media institutions subject to censorship or intimidation? How often do they self-censor? Why?

☐ Are censorship circumvention technologies commonly used (e.g., Virtual Private Networks (VPNs) like Psiphon and UltraSurf, encrypted messaging apps like Telegram)? What is the main motivation for their use? Who are the main users?

GEOPOLITICAL POSITIONING

☐ Have surveillance technologies or major "Safe City" (or "Smart City") projects with foreign backing been deployed?

CYBERSECURITY

☐ What cybersecurity measures are put in place by the government, private sector, and civil society to prevent or discourage digital repression?

EMERGING TECHNOLOGIES

☐ Have AI and other emerging technologies been used to spread disinformation, including through deepfakes?

☐ Are emerging technologies, like AI, being used for advanced surveillance systems? If yes, what specific technologies (e.g., facial recognition)? Who develops them? Who deploys them?

INTERNET FREEDOM

DIGITAL REPRESSION

PERCEPTIONS

- □ What are the perceptions about the drivers of disinformation? What are the motivations and mechanisms supporting it?
- □ What is the perception among different stakeholders (individuals, CSOs, private sector) of repressive disinformation in terms of impact, public believability, and how widespread it is?
- □ To what extent are individual citizens aware of digital repression techniques? Whom do they see as being responsible for digital repression? How do people perceive repression (as a necessity, as a threat, as a violation, etc.)?

INTERVIEWEE IDENTIFICATION

- □ What stakeholders combat, research, or report on digital repression? (e.g., CSOs, private-sector tech companies, government ministries, academics)

KEY RESOURCES

- Information Disorder: Definitional Toolbox (First Draft, 2018)
- List of Perceived Internet and Social Media Harms (Oxford Internet Institute)
- Media Manipulation Casebook (Harvard)
- OpenNet Initiative
- Open Observatory of Network Interference
- Citizen Lab
- Omelas
- Rule of Law Index: Open Government Index (World Justice Project, 2019)
- Google Transparency Reports
- Facebook Transparency Reports
- Twitter Transparency Center
- The Engine Room: Tech Tools for Human Rights Documenters

Photo: Afandi Djauhari

INTERNET GOVERNANCE

CURRENT STATE AND IMPACT

☐ What international internet governance agreements has the government signed on to? Is the country consistently in compliance with these agreements? (e.g., Budapest Convention, regional trade agreements requiring privacy regulation)

Internet Governance Organizations

☐ What institutions, forums, or multi-stakeholder groups exist around internet governance? How well do they follow a multi-stakeholder format?

☐ What domestic internet governance bodies exist? (e.g., national domain name registry, network operators' groups)

☐ What actors, if any, from the country participate in international internet governance fora (Internet Governance Forum (IGF)—regional, international meetings, International Telecommunications Union (ITU), Internet Corporation for Assigned Names and Numbers (ICANN), African Network Information Centre (AFRNIC), Latin America and Caribbean Network Information Centre (LACNIC)? (see, for example, attendee list for IGF 2020)

- Does the IGF have a national initiative? How often does it meet? Does it follow a multi-stakeholder approach? Who is involved?
- Is the country a member of the ICANN Governmental Advisory Committee (GAC)?

☐ Outside of more formal internet governance structures, do actors (especially private sector or civil society) lobby to regulate the internet? What are they lobbying for?

GEOPOLITICAL POSITIONING

☐ How does the country align with others on issues like internet sovereignty? Is there evidence of efforts to align with other international actors (U.S., European Union, PRC, etc.)?

Illicit Activity Online

☐ Is any legislation proposed or approved on cyber crime, online child protection, consumer protection, and/or intellectual property?

☐ To what extent is the internet used to harass or threaten women, children, and other marginalized or vulnerable populations (Refer to Inclusion Analysis.)

- Are specific groups repeatedly targeted?
- What legal measures are in place to protect against and punish online abuse?

☐ How often do data breaches occur?

- What actors are responsible?
- What preventive action is taken by different actors (government, private sector, civil society)?
- Following major breaches, what is messaged to the public by different actors (government, private sector, civil society)?

☐ Is the internet or other digital technologies used to carry out financial crimes (e.g., scams, extortion)?

- What actors are responsible? (domestic, foreign, private)
- How widespread is online extortion?
- What institutions monitor, publicize, and counter these crimes?
- What formal regulatory, legal, or policy guidelines exist to prevent or punish these efforts?
- What formal systems exist for victims to report this type of activity?

☐ To what extent is the internet used for illicit activity including spreading hate speech, promoting and recruiting for violent extremism, and exploiting children and other vulnerable groups?

- What groups are primarily responsible for these activities?
- How widespread are they? How often do they occur?
- What institutions monitor, publicize, and counter these activities?
- What formal regulatory, legal, or policy guidelines exist to prevent or punish these efforts?

INTERNET FREEDOM

INTERNET GOVERNANCE

Photo: Jack Gordon for USAID/Digital Development Communications

PERCEPTIONS

☐ To what extent is internet governance perceived as important by different stakeholders (government, civil society, private sector, media influencers, individual citizens)? Why?

☐ Do stakeholders think a multi-stakeholder approach to internet governance is important?

INTERVIEWEE IDENTIFICATION

☐ What stakeholders are engaged in research, policy making, advocacy, or programming around internet governance? (academia, CSOs, private sector, digital activists, government, media influencers/outlets)

☐ What internet governance institutions exist, and who is involved in them (individuals and institutions)?

KEY RESOURCES

- Internet Governance Forum
- ICANNwiki
- ICANN GAC member directory
- New America's "The Idealized Internet vs. Internet Realities"
- Regional internet registries: AFRINIC, APNIC, LACNIC
- Human Rights Watch
- Freedom on the Net country analysis

CIVIL SOCIETY AND MEDIA

CURRENT STATE AND IMPACT

- □ What are the priorities of the major civil society stakeholders?
  - – What techniques do they use to protect and advocate for digital rights?
  - – How do they counteract misinformation and disinformation?
  - – What techniques do they use to uphold freedom of expression online?
  - – What are their key topics of concern?
  - – What specific marginalized or vulnerable populations do they focus on protecting? (Refer to Inclusion Analysis.)
- □ Are laws in place that enable journalists and CSOs to make Freedom of Information requests? How well does this work in practice?
- □ Is information available for journalists and CSOs through open data platforms?
- □ To what extent do CSOs and media associations collaborate online to advocate for change and accountability?
- □ To what extent do CSOs enable or promote political organizing online? What techniques do they use? What are the demographics of their target audiences/members?
- □ What are the most commonly used social media platforms? What are they used for? Who is using them? What makes these platforms popular?
- □ Do people generally have the ability to critically consume and create digital media content?
  - – How much trust do people place in digital media?
  - – Do people have the ability to discern where the information they consume online is coming from? (who is creating it)
  - – How does this ability vary across demographic groups? (Refer to Inclusion Analysis.)
  - – How do public trust and media literacy impact the digital media ecosystem?

PERCEPTIONS

- □ How do people and institutions perceive the role of government in public media?
- □ How are the major watchdog, independent media, and/or CSOs perceived by different stakeholders (individuals, government, private sector)?
- □ What is the perceived strength of CSOs and media to organize online and advocate for change and accountability?
- □ How do different stakeholders perceive the state of media literacy, demand for independent media, and trust in media integrity?
- □ What are the perceptions about the drivers of misinformation and disinformation? What are the motivations and mechanisms supporting its spread?

INTERVIEWEE IDENTIFICATION

- □ What are the major watchdog, independent media, and CSOs that are involved in political organizing online and combating digital repression?
- □ What media outlets/platforms report on digital repression?
- □ What stakeholders are engaged in research, policy making, advocacy, or programming around digital media? (e.g., academia, CSOs, tech companies, government ministries, donors, media influencers/outlets)

CYBERSECURITY

- □ How well can CSOs protect themselves and the people they serve from cyberthreats? What efforts exist to improve this capacity? Do CSOs have access to cybersecurity training? Are available cybersecurity products and services affordable for CSOs?

GEOPOLITICAL POSITIONING

- □ What is the role of foreign media outlets? Has the country been targeted by foreign disinformation campaigns?

KEY RESOURCES

- ■ Media Sustainability Index (IREX)
- ■ Reporters Without Borders
- ■ Global Investigative Journalism Network
- ■ Data Reportal (We are Social)
- ■ "Learn to Discern" Media Literacy Pilot (IREX)
- ■ Ciudadanía Inteligente

INTERVIEWEE IDENTIFICATION

- □ Which government ministries have citizen- and business-facing e-service platforms?
- □ Which government ministries are in charge of maintaining citizen- and business-facing e-service platforms?
- □ Are private companies involved in building and maintaining citizen-facing online government service portals?
- □ What stakeholders are involved in the national ID system (if it exists)? (e.g., private-sector tech companies, government ministries, CSOs)
- □ Which government ministries are most involved in releasing open data?
- □ Who are the primary users of open government data? (e.g., research institutions and higher education institutions, international development institutions, private-sector companies)

CURRENT STATE AND IMPACT

- □ What government-to-person (G2P) and government-to-business (G2B) e-service delivery platforms exist?
  - – For what purposes do people and businesses primarily use the government e-service delivery platforms? (e.g., registering a business, filing taxes, accessing birth/health records, applying for social services)
  - – Does the presence, level of advancement, and usability of these platforms differ across sectors?
- □ Are government e-services platforms safe and accessible for marginalized and vulnerable populations? (Refer to Inclusion Analysis.)
- □ If a national ID system is in place, how does it use digital technology?
  - – What factors influenced the government's decision to institute a digital ID system (including potential foreign influence)?
  - – When was it rolled out?
  - – How much of the population does it cover?
  - – What biometric data are collected as part of the national ID system?
  - – To what extent can third parties like banks and businesses rely on the national ID system for authentication of their customers?
  - – What services are linked to the national digital ID system?
  - – How does the ID system incorporate proprietary or open-source (e.g., Modular Open Source Identity Platform) components? Are there concerns about vendor lock-in (i.e., governments being "stuck with" a vendor long term because of early design choices)?
  - – What groups are excluded from the national digital ID system? (Refer to Inclusion Analysis.) What excludes them from access and use (e.g., documentation requirements, literacy, refusal to participate)? Why?

CYBERSECURITY

- □ How well does the national ID system ensure cybersecurity, privacy, and data protection?

- □ To what extent are government data freely available? What are the processes for accessing open government data? How do they differ across government ministries and by level?
- □ How are open government data formatted? How does this impact usability? (e.g., PDFs are less usable than raw data in spreadsheets; nationally aggregated data are less usable than locally disaggregated data)
- □ What open government data portals exist? Is a single national data portal in place or does each ministry maintain its own? Who manages the portals?
- □ Do government open data sites appear to be actively maintained? Have new datasets been added recently?
- □ Is an open data policy in place? Do government actors promote open government data? At what levels (federal versus local)? Which specific ministries?
- □ Does the level of availability of open government data differ across sectors? Why? What impact does this have on stakeholders working in different sectors?
- □ How are open government data currently used? By whom?
- □ Is the country a member of the Open Government Partnership (OGP)? If yes:
  - What actor facilitates OGP? Which stakeholders are members?
  - How far along is the country in implementing the commitments it has made through the OGP?

CYBERSECURITY

- □ What measures are in place to protect government e-services platforms from cybersecurity threats? Who is responsible for ensuring adaptation to new threat types?

EMERGING TECHNOLOGIES

- □ Is the government trying to enhance government services through the use of emerging technologies? (e.g., blockchain-backed data registries, AI-powered citizen e-service delivery)

PERCEPTIONS

- □ What factors affect citizen engagement with government e-service platforms? (e.g., trust, digital literacy, portal navigability, type and extent of services provided)
- □ How do citizens and businesses perceive the benefits of government e-service platforms? What do they think works well (or does not work well)?
- □ How do different stakeholders (individuals, businesses, government) perceive the national digital ID system in terms of usability, trust, data privacy, efficiency, and utility? Do they have sufficient trust in the system and the value it provides?
- □ How do different stakeholders perceive open government data in terms of benefits and risks?
- □ How do different stakeholders perceive the government's willingness to create and share open government data?
- □ What appears to motivate the government to promote or impede open government data?

KEY RESOURCES

- GovTech Projects and Research (World Bank)
- E-government Knowledgebase (UN)
- Open Government Partnership
- Global Open Data Index (Open Knowledge Foundation)
- Open Data Handbook (Open Knowledge Foundation)
- ID4D (World Bank)
- Digital ID report (USAID)
- Digital ID How-to Guide (USAID)

Manage Government Systems

INTERVIEWEE IDENTIFICATION

□ What government ministries are responsible for building and maintaining internal IT systems (including data centers)?

CURRENT STATE AND IMPACT

□ To what extent are government records digitized and housed in digital databases? (e.g., social assistance registries)

□ How are government data stored and managed (local data storage, cloud storage)?

- If cloud storage is used, what motivated this transition? What provider is used? What was the provider selection process like?
- To what extent are data interoperable between government ministries? What impact does interoperability have on day-to-day operations? What impact does it have on citizens?
- Does the government access and use data to make data-driven policy decisions?
- Do management information systems (MIS) exist? If yes, what data in what sectors? (e.g., education, health, social services) What actors use the MIS and for what?

CYBERSECURITY

□ What security exists for government IT systems (including government data centers)? Do government IT systems undergo information audits (like penetration testing) to ensure robust cybersecurity is in place? Who is responsible for checking and maintaining cybersecurity and combating threats?

□ Have there been any recent high-profile data breaches or cybersecurity incidents on government systems? At what scale? How were they handled? Was there any communication issued by the government?

□ What is the capacity of government personnel to understand and use cybersecurity products and standard practices to protect against cyber threats to government IT systems? What efforts, if any, exist to increase their capacity?

GEOPOLITICAL POSITIONING

□ Have government personnel participated in technology-focused training or capacity-building seminars hosted by authoritarian states?

- □ Do government data centers exist? How many? Where are they located? What are their purposes? What government entities manage them?
- □ Is there a financial management information system (FMIS)?
  - – Who manages it? (e.g., the Treasury, the Ministry of ICT)
  - – Is it used across government ministries and levels?
  - – What is it used for? (e.g., public financial management processes like budget formulation, execution, accounting, and reporting)

PERCEPTIONS

- □ How do government personnel across ministries perceive the benefits of increased digitalization of government back-end systems and operational processes, and digitization of paper records?
- □ How do government personnel across ministries perceive the usability of government IT systems?
- □ How do government personnel perceive the importance of protecting government IT systems from cybersecurity threats?
- □ What is the perception by different stakeholders (individuals, CSOs, private sector, media influencers/outlets) of government capacity to monitor, detect, and react to cybersecurity threats on government IT systems?

KEY RESOURCES

- ▪ Operational Guidance Note on FMIS (World Bank, 2020)
- ▪ E-government Knowledgebase (UN)
- ▪ X-Road (e-Estonia)

Engage **Citizens and Organizations**

INTERVIEWEE IDENTIFICATION

- □ Which government agencies use online platforms for public participation and feedback?
- □ Who are the most prominent government champions for public engagement platforms?
- □ Who is responsible for setting up and maintaining these platforms (both government agencies and any private-sector partners)?
- □ What civil society or public-interest groups engage most heavily with public participation platforms?
- □ Which government agencies are responsible for election technology?

CURRENT STATE AND IMPACT

- □ What online platforms exist (or have existed) for public engagement and feedback?
  - – What motivated the government to establish them?
  - – What is their legal basis? (i.e., is public engagement required by law under some circumstances?)

- What features do they include?
- Have there been notable instances of online public engagement affecting government decisions?
- Are online platforms used for citizen and voter education?
- What measures exist to ensure safety and security?

□ Are plans in place to expand (or create) online public engagement channels in the future? What are their intended purpose? Which government entities will manage and use them?

□ How does the government engage the public through social media?

□ How do digital engagement efforts interact with bigger-picture trends around transparency, citizen participation, and consultative governance? Are these efforts in tension with the culture of government institutions?

□ How is digital technology used in elections?

- Are online voting models being implemented or considered? If so, why?

□ Does the government have any government innovation or incubation hubs (e.g., 18F in the U.S.)?

- What are their purposes?
- What are the results of their work?
- How do they ensure inclusion of marginalized and vulnerable populations? (Refer to Inclusion Analysis.)

PERCEPTIONS

□ How do different stakeholders perceive public engagement platforms in terms of usability, credibility, and safety?

□ How do different stakeholders (including government) perceive government responsiveness to the feedback they receive through public engagement platforms?

□ How do different stakeholders perceive the benefits of online public participation?

KEY RESOURCES

- E-Participation index (UN)
- Perceptions of electoral integrity (includes an indicator on online voting) (Electoral Integrity Project)

Guardrails for Technology

INTERVIEWEE IDENTIFICATION

□ What government ministries or specific actors oversee the government's adherence to the regulations, laws, and policies governing technology use?

□ What actors are involved in or report on the government's recent deployments of new digital technology? (e.g., smart cities, digital ID systems)

□ Is a national CIRT, CERT, or a CSIRT in place? What individuals or institutions are members?

CURRENT STATE AND IMPACT

□ What technology-related policies exist that ensure basic safeguards for all users? (e.g., laws prohibiting online gambling, intellectual property protection laws, blocking/filtering access to certain content)

- What civil and political rights are reflected and protected in the regulations, laws, and policies that govern the government's use of technology?
- How do the regulations, laws, and policies ensure the protection of individuals against the malicious use of technology?
- Is there an explicit focus on inclusion and accessibility, especially for marginalized and vulnerable populations? (Refer to Inclusion Analysis.)

□ How are consultative processes used when the government deploys new technology (e.g., smart cities, 5G)? How are affected communities involved throughout the process?

□ How does the government procure digital technologies/digital government initiatives? Is the process competitive and transparent?

EMERGING TECHNOLOGIES

□ If the government has adopted strategies or roadmaps for emerging technologies (such as AI or smart cities), what concrete ethical guidelines are included?

GEOPOLITICAL POSITIONING

□ Are policies in place intended to mitigate supply chain risks (e.g., limiting the role of untrusted ICT equipment vendors)?

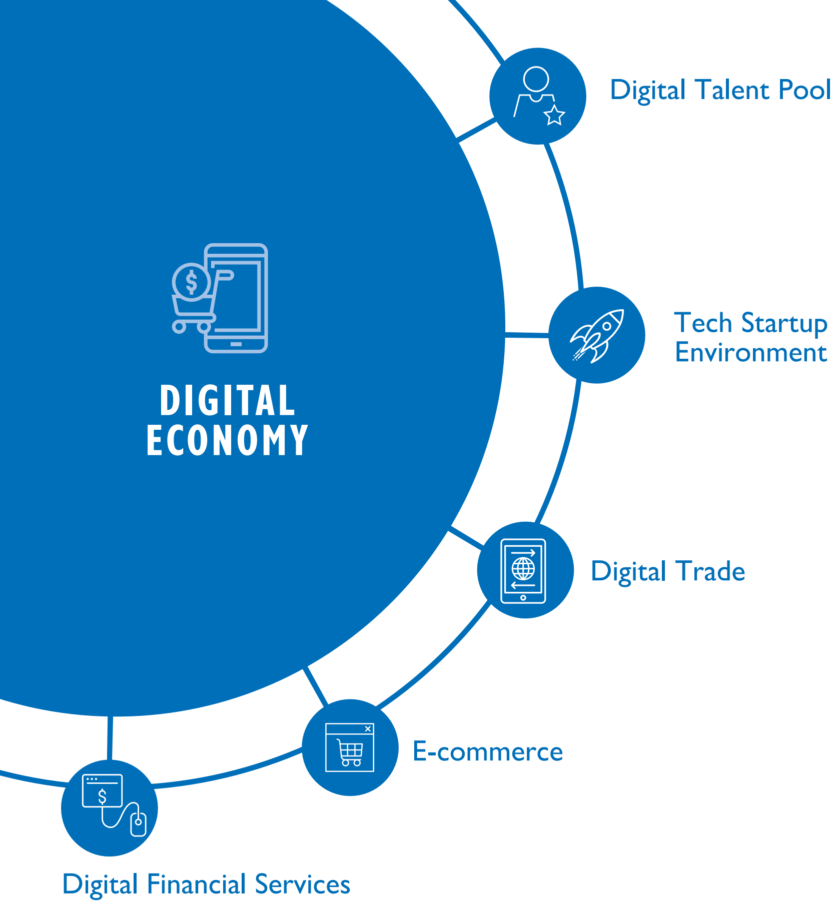
PERCEPTIONS

□ How do different stakeholders (businesses, civil society) perceive government technology procurement processes in terms of transparency, competitiveness, and accountability?

□ How do different stakeholders (especially domestic and foreign businesses) perceive digital supply-chain restrictions in terms of necessity, proportionality, and fairness?

KEY RESOURCES

- The global landscape of AI ethics guidelines (free preprint version here) (Nature Briefing, 2019)
- ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies (Carnegie Endowment for International Peace, 2019)
- National Cybersecurity Strategies Repository (ITU)
- National Cyber Security Index (NCSI) (e-Governance Academy)



PILLAR III

DIGITAL ECONOMY

Digital Economy, explores the role digital technology plays in increasing economic opportunity and efficiency, trade and competitiveness, and global economic integration. Areas of inquiry include digital financial services (credit or debit cards, payment apps, mobile money, and digital savings and loan products), financial inclusion, regulation of digital finance, digital trade, e-commerce, and the financial technology (FinTech) enabling environment. This pillar also assesses strengths and weaknesses in the local digital talent pool and the tech startup environment; a healthy digital economy requires a supply of ICT skills that matches the demand and an ecosystem that promotes technological innovation.

PILLAR 3

IDEAL STATE

GOVERNMENT/POLICY LEVEL

1. The government's digital modernization strategy (see Pillar 2) addresses the financial sector and promotes interoperability, financial inclusion, and transparent consumer protection standards. An overarching digital strategy may also be linked to a national financial inclusion strategy.

2. The financial regulator is prepared to be agile when responding to ongoing technology innovations and with respect to emerging technologies, using measures such as regulatory sandboxes and tiered know-your-customer (KYC) requirements to balance innovation, inclusion, and risk. The legal framework is not so strict as to discourage innovation in digital financial services (DFS), nor so amorphous or lenient as to place users at risk.

3. Financial regulations clearly articulate core principles and requirements for cybersecurity in the financial system including payment security, data encryption, and data privacy.

4. Regulators may access consumer financial information only to a clearly defined, limited extent and must be accountable for any access.

5. Digital transactions are secured through electronic signature and authentication methods; protections against unauthorized access to or loss, destruction, use, modification, and disclosure of data; and prohibitions against localization requirements.

6. Key government stakeholders are aware of the impact of e-commerce on traditional methods of cross-border trade.

7. The legal framework pertaining to e-commerce and e-commerce-related transport and infrastructure is clear; regularly reviewed and updated through an inclusive, multi-stakeholder process; and transparently administered.

8. Consumer protection authorities have sufficient resources to implement a regulatory framework that reflects good practice and takes account of unique risks posed by online economic activity for consumers and businesses, particularly those reliant on digital platforms (e.g., for e-commerce-reliant businesses to include equitable, prompt resolution of complaints, combating platform fraud or the sale of counterfeit goods).

9. Competition authorities have sufficient resources to implement a regulatory framework that reflects good practice and takes account of unique risks posed by digital platforms and other online business models that might engage in anticompetitive practices or facilitate undue market concentration.

10. The country is making timely progress on digital components of international trade facilitation commitments, such as the World Trade Organization's (WTO's) Trade Facilitation Agreement or the World Customs Organization's Revised Kyoto Convention.

11. A national trade facilitation committee exists and shows a commitment to inclusive membership of both public- and private-sector participants.

12. Government policy supports the growth of technology entrepreneurship through suitable tax and regulatory frameworks.

13. Public policy encourages female participation in the online platform workforce; the growth of women-dominated digital services industries, including health, education, business services, and social services; and social protection systems for new forms of work.

PILLAR 3

IDEAL STATE

INSTITUTION LEVEL

1. Businesses have access to a variety of safe, accessible, and reliable digital payment systems, including account-based systems (credit cards, debit cards, mobile payment systems, and facilitated services such as PayPal) and electronic currency (such as prepaid cards or digital currencies).

2. A full suite of DFS is offered, including safe and enhanced access to credit, savings, loan, and insurance products for producers, retailers, and consumers. Financial service providers (including microfinance institutions, banks, and FinTechs) have a digital core (i.e., all core functions can be performed online) and are connected to each other.

3. Financial service providers understand and comply with requirements set forth by the financial regulator, including for cybersecurity of the financial system.

4. Digital payment systems are interoperable. To facilitate payments from buyers located abroad, sellers can access third-party e-payment service providers that are linked to domestic ones.

5. Cross-border e-commerce does not face burdensome transaction limits.

6. Public- and private-sector trade logistics systems use risk management systems to guard against criminal and terrorist activity while facilitating low-risk trade, including through regular review and adaptation to prevent new threats.

7. Small and medium enterprises (SMEs) and micro, small and medium enterprises (MSMEs) throughout the country can easily leverage local and foreign e-commerce platforms to reach new markets. These businesses benefit from robust, efficient, and equitable protections (particularly from digital platforms) and policies against risks from conducting online business (e.g., platform fraud, the sale of counterfeit goods, non-payment for goods/services).

8. Companies have the capacity and access to adopt and use technology (including e-commerce) to improve their internal operations.

9. Digital platforms and other firms that facilitate online economic activity for consumers and small businesses define and implement industry-level practices, policies, and systems that protect consumers and businesses from risks posed by conducting online business.

10. Tech startups have access to resources to help them start, scale, and sustain their businesses, including business acumen training and mentorship, startup capital, and diverse, flexible long-term investment opportunities.

11. Tech startups are incentivized to design inclusive solutions that improve the livelihoods of last-mile and marginalized customers.

12. IT firms have a competitive field from which to hire highly skilled IT talent, which they continue to attract, acquire, and retain, contributing to the country's competitiveness in the IT sector.

13. Third-party service vendors are held accountable to responsible data guidelines, algorithmic transparency, public codes of conduct, and terms of service agreements.

PILLAR 3

IDEAL STATE

INDIVIDUAL LEVEL

1. Consumers have access to a variety of safe, accessible, and reliable digital payment systems, including account-based systems (credit cards, debit cards, mobile payment systems, and facilitated services such as PayPal) and electronic currency (such as prepaid cards or digital currencies).

2. The range of available DFS includes savings, loan, and insurance products and safe and advanced access to credit for producers, retailers, and consumers designed to meet the diverse needs of consumers across demographic groups (refer to Inclusion Analysis) and with varying levels of digital financial literacy.

3. The availability of DFS enhances economic opportunities for marginalized and vulnerable populations communities. (Refer to Inclusion Analysis.)

4. Consumers trust and use DFS offerings and e-commerce platforms regularly.

5. Consumers have the capacity to apply standard cyber hygiene precautions when using DFS and e-commerce.

6. Trade, transport, and border policies and practices are responsive to the needs of woman-owned enterprises and women traders, including through steps that provide for their access to information and resources and that address their personal safety issues and vulnerabilities.

7. Agencies charged with promoting commerce, trade, and investment are committed to connecting traditionally disenfranchised groups—which may include women, minority groups, refugees, migrants, or rural entrepreneurs—to critical trade logistics information and guidance.

8. Tech entrepreneurship is viewed as a viable career option.

9. IT curricula (at all levels where they exist) are often revisited and updated and equip students with appropriate IT skills to meet employer demand.

KEY STAKEHOLDERS

- Trade associations
- E-commerce platforms
- Consumer protection and advocacy groups
- Financial institutions (e.g., banks, FinTech startups, payment providers, lenders)
- Tech startups
- Tech innovation hubs and business incubators
- Universities focusing on STEM/ICT education
- National customs and border control agencies
- Other donors
- USAID/other donor implementing partners
- Tech firms and third-party service vendors (e.g., data management, software development, digital marketing, cloud-computing, AI/ or machine learning (ML)-based data analytics firms)

DIGITAL FINANCIAL SERVICES (DFS)

CURRENT STATE AND IMPACT

□ What policies, regulation, and legislation exist around DFS (e.g., transaction limits, payment service provider licensing requirements, KYC requirements, fees and taxes on digital transactions, FinTech), and to what extent are these policies implemented?

□ What consumer protection laws exist for DFS?

□ Does a national payment gateway exist? When was it launched? What regulation exists around it? Who regulates it?

□ Does an automated clearinghouse exist? What is the membership and fee structure? How does this enable interoperability between financial service providers?

□ How are non-financial entities that want to provide DFS treated? Do they need to be registered or licensed?

□ What products do the main financial service providers offer? How do they differ by financial service provider type (commercial bank, development bank, microfinance institutions, non-bank financial institution)?

□ What are the common consumer and business uses for DFS? (e.g., vendor payments, input payments, remittances, mobile top-ups, travel, salaries)

□ To what extent are DFS used for government-to-person (G2P) and person-to-government (P2G) payments? (e.g., taxes, subsidies, social benefit payments, cash transfer programs, government salaries)

□ What does digital financial inclusion look like across demographic groups? (Refer to Inclusion Analysis.)

□ What types of DFS do consumers use, and how does this differ across demographic groups? (e.g., bank transfers, mobile money, cheque, Quick Response (QR) codes, cash-dependent)

□ What DFS products are designed to specifically increase women's financial inclusion? What DFS products cater to other marginalized or vulnerable populations? (Refer to Inclusion Analysis.)

□ Are payment services interoperable? What implications does this have for adopting and using DFS across different demographic groups? (Refer to Inclusion Analysis.)

□ What impact do digital financial literacy levels have on DFS adoption and use? How is financial literacy taught (in schools, by employers, etc.)?

□ What role does consumer and business trust in DFS play in adoption and use?

□ What level of merchant uptake of DFS exists in harder-to-reach areas? What are the biggest barriers to increasing merchant uptake of DFS?

□ What does the DFS provider agent network look like? Is there a dominant provider? How does coverage throughout the country vary?

□ Do DFS providers embrace disruptive technologies? What is the motivation? Does this strengthen their competitive advantage?

CYBERSECURITY

□ What laws, regulation, and policies exist requiring formal financial institutions to prevent and address cybersecurity threats to the financial system?

— What barriers or obstacles limit compliance? To what extent do institutions have the capacity to comply? What resources would help them comply? What resources are available to build their cybersecurity capacity?

EMERGING TECHNOLOGIES

□ How are emerging technologies (e.g., AI, machine-learning, blockchain) used in the financial sector?

DIGITAL FINANCIAL SERVICES (DFS)

PERCEPTIONS

- ☐ What do consumers perceive to be the biggest opportunities or challenges of using DFS?
- ☐ What perceptions prevent financial service providers from serving last-mile customers? Do other stakeholders agree that these perceptions are accurate?
- ☐ How do businesses that use DFS perceive the capacity, transparency, and accountability of the financial regulator?
- ☐ What potential does the regulator see for DFS?
- ☐ What is the preferred DFS policy approach: restrictive initially and then incremental loosening to avoid stifling innovation versus hands off initially and then tightening to reduce systemic and consumer protection risks? Which approach presents more beneficial gains? (for consumers, local and foreign firms, and the country's economy)

INTERVIEWEE IDENTIFICATION

- ☐ What stakeholders are engaged in research, policy making, advocacy, service delivery, or programming around DFS? (e.g., academia, financial service providers, MNOs, financial regulators, international development institutions, CSOs)

KEY RESOURCES

- Global Findex (World Bank, 2017)
- Global Microscope 2019: The enabling environment for financial inclusion (The Economist Intelligence Unit, 2019)
- Mobile Money Metrics (GSMA)

Photo: KC Nwakalor

E-COMMERCE

INTERVIEWEE IDENTIFICATION

- □ What stakeholders are engaged in research, policy making, advocacy, service delivery, or programming around e-commerce? (e.g., academia, trade associations, regulators, local platforms, international platforms, customs agencies, financial regulator, postal services, government ministries, civil society, or consumer advocacy institutions)

CURRENT STATE AND IMPACT

- □ What policies, regulation, and legislation exist around e-commerce? To what extent are these policies implemented?
- □ What consumer protection and competition laws or regulations exist for e-commerce? To what degree are general consumer protection and competition laws and regulations being applied to online economic activity?
- □ To what degree have businesses, particularly SMEs, adopted digital tools and services for e-commerce and other purposes?
- □ What are the major e-commerce platforms (local versus international)? What impact do international e-commerce platforms (e.g., Amazon, Alibaba) or informal online marketplaces (e.g., Facebook) have on the e-commerce sector?
- □ What payment methods are commonly used for e-commerce transactions (cards, cash-on-delivery, etc.)?
- □ Who conducts online business through digital platforms, and how does it differ across demographic groups? (Refer to Inclusion Analysis.)
- □ Is it easy or hard to transact using e-commerce across borders?
- □ What laws exist around e-signatures, paper-based transactions, transferable and records and instruments? Are they aligned with the United Nations Commission on International Trade Law (UNCITRAL) Model Laws?
- □ Does the postal system provide affordable, high-quality service that can support e-commerce businesses?
- □ Which express shipping companies (e.g., UPS, DHL, FedEx) have a presence? Do they offer small-parcel services suitable for e-commerce? What is their reach throughout the country? Is expedited shipping given special treatment by customs and border control agencies?
- □ How does e-commerce logistics support or hamper the growth of the sector?
- □ What opportunities exist to link SMEs to new markets through e-commerce? Are there opportunities specifically for SMEs owned by women and members of other marginalized groups? (Refer to Inclusion Analysis.) Do they account for the specific needs and vulnerabilities of marginalized business owners?

CYBERSECURITY

- □ What policies, regulation, and legislation exist requiring e-commerce companies to prevent and address cybersecurity threats?
  - – What barriers or obstacles limit compliance? To what extent do institutions have the capacity to comply? What resources would help them comply? What resources are available to build their cybersecurity capacity?

EMERGING TECHNOLOGIES

- □ How are emerging technologies (e.g., AI, ML) used by businesses?

E-COMMERCE

PERCEPTIONS

- ☐ How do e-commerce firms perceive the policy, legal, and regulatory environment around e-commerce in terms of capacity, transparency, and accountability? Is the e-commerce market perceived as fairly and sufficiently regulated?
- ☐ How do different stakeholders (government, consumers, e-commerce platforms) perceive local and international e-commerce companies in terms of capacity, transparency, accountability, and influence?
- ☐ Do consumers and small businesses that rely on e-commerce platforms trust the platforms and the associated infrastructure? Why or why not?
- ☐ What do e-commerce firms perceive to be the greatest barrier to the sector? Greatest opportunity? What about consumer advocacy institutions?

KEY RESOURCES

- UNCTAD country reports
- B2C E-commerce index (UNCTAD)
- Model Laws on E-commerce (UNCITRAL)
- Model Law on Electronic Signatures (UNCITRAL)
- UN Convention on Contracts for the International Sale of Goods

Photo: Oscar Leiva/Silverlight Photo Video

INTERVIEWEE IDENTIFICATION

- ☐ What stakeholders are engaged in research, policy making, advocacy, or programming around digital trade? (e.g., academia, trade associations, regulators, international corporations, government ministries, customs agencies, e-commerce platforms)

CURRENT STATE AND IMPACT

- ☐ What policies, regulation, and legislation exist around digital trade/digital trade facilitation?
- ☐ To what extent are these policies implemented?
- ☐ To what extent have the WTO Trade Facilitation Agreement commitments been implemented?
  - Have the digital-specific agreements been implemented? (e.g., information on procedures and requirements made available through the internet; electronic payments enabled for duties, taxes, fees, and customs charges)
  - What are the key barriers to implementation?
  - What are the implications of lagging or leading implementation?
- ☐ What are the documentation requirements for import and export processes, and to what extent are they digitized? What is their impact on enabling cross-border trade?
- ☐ What are the biggest bottlenecks to cross-border trade (e.g., transport and shipping, logistics, postal service, infrastructure, customs, delivery to end-consumer)?
- ☐ To what extent does trade take place in digital services/business process outsourcing (BPO)? What policies and regulations exist on this? What impact do they have on the potential of trade in digital services/BPO?

GEOPOLITICAL POSITIONING

- ☐ To what extent does the country participate in digital trade initiatives led by the People's Republic of China (e.g., the Electronic World Trade Platform)?

PERCEPTIONS

- ☐ How is the policy, legal, and regulatory environment for digital trade perceived by different stakeholders (consumers, private sector) in terms of capacity, transparency, and accountability?
- ☐ What do individuals and corporations perceive to be the biggest barriers and enablers to digital trade? (domestic and cross-border)

KEY RESOURCES

- WTO Trade Facilitation Agreement Database
- UN Global Survey on Digital and Sustainable Trade Facilitation

TECH STARTUP ENVIRONMENT

INTERVIEWEE IDENTIFICATION

□ What stakeholders are involved in the tech startup environment? (e.g., academia, company founders and employees, investors, innovation hubs, international startups, regulators, media influencers/outlets)

CURRENT STATE AND IMPACT

□ What policies or regulations are in place that hinder or promote tech startups? To what extent are these policies implemented?

□ How easy or hard is it to start and sustain a business? What fees, taxes, or registration processes are in place?

□ What policies or regulations are in place to attract or discourage potential investors? To what extent are these policies implemented?

□ What type of innovation hubs and accelerator programs are in place? How many are supported by the government or are all reliant on outside donors or outside foundations? What services do they offer? How effective are they? Are they based at higher education institutions? What types of tech startups do they target? Do they have programming targeted to marginalized communities? (Refer to Inclusion Analysis.)

□ Do angel investor networks exist? What is the general member profile (local vs. international)?

□ Are tech startups focused in a particular sector?

□ What is the make-up of the tech startups in terms of local versus. diaspora versus international founders?

□ Where are most tech startups located? Are particular cities tech startup hubs?

□ Do founders represent demographic diversity? (Refer to Inclusion Analysis.)

□ What are the major challenges to starting and scaling? Are there barriers specific to different demographic groups? (Refer to Inclusion Analysis.)

□ Are there tech startups that offer solutions targeting the last-mile? Are any incentives provided for new tech startups to offer such solutions (e.g., tax incentives, training programs, investment sources)?

□ How are the innovations of tech startups affecting the production and consumption of local media content (news, entertainment, etc.)?

PERCEPTIONS

□ How do individuals perceive careers in entrepreneurship and tech startups? What guidance do they receive from schools, parents, and others?

□ What do tech startup founders and entrepreneurs perceive to be the biggest barriers to take-off?

□ What do investors perceive to be the biggest barriers to investing in the country's startup ecosystem?

KEY RESOURCES

- Startup Genome
- Startup Blink
- CBI Insights
- Global Startup Ecosystem
- Global Entrepreneurship Index 2019
- Ease of Doing Business (World Bank)

DIGITAL TALENT POOL

INTERVIEWEE IDENTIFICATION

□ What stakeholders have the capacity and influence to support the digital talent pool? (e.g., government, schools, higher education institutions, non-degree programs, innovation/tech bootcamps, IT companies)

CURRENT STATE AND IMPACT

□ What skills are most sought after by employees in the IT sector?

□ Is a national IT curriculum in place? At what levels (primary, secondary, higher education, non-degree programs)? What skills does it primarily focus on? When was it last updated?

□ Are the policies or plans in place for attracting and retaining skilled IT professionals at local higher education IT programs?

□ Does the supply of IT skills match the demand in the sector?

□ How much demographic diversity exists at different levels (entry, mid, C-suite) of the digital talent pool? (Refer to Inclusion Analysis.) What factors limit diversity?

□ What programs exist to increase demographic diversity in the IT sector? (e.g., mentorship and internship programs for women and girls, workplace policies catered to women)

□ Are there populations currently out of work or in transition that might be well-suited for reskilling/upskilling into the IT workforce? What resources exist for reskilling/upskilling programs?

□ What role do private-sector IT companies (large and small) play in cultivating a strong digital talent pool? (e.g., apprenticeship or mentoring programs with IT students)

□ What does IT talent retention look like in the private sector? Public sector? Are private-sector or public-sector policies in place to ensure IT sector talent retention?

□ Are there concerns about skilled IT talent leaving the country? How does this impact the local IT sector?

CYBERSECURITY

□ Which higher education institutions offer programs or degrees in cybersecurity? How are these programs adequately prepared for the current and future demand for information security workforce skills (high quality instruction, access to cyber ranges/other specialized software and hardware)?

GEOPOLITICAL POSITIONING

□ Which major digital workforce development efforts are sponsored by foreign actors?

PERCEPTIONS

□ How do individuals perceive careers in the IT sector?

□ What motivates individuals to seek careers in the IT sector?

□ How do private-sector IT companies perceive the quality of recent university graduates?

□ How is the IT talent pool perceived by foreign companies currently working or looking to recruit/set up offices in the country?

KEY RESOURCES

- Meetup.com (possible way to meet local entrepreneurs)
- Global Skills Index 2020 (Coursera)
- Digital Risers 2020: Tech Ecosystem and Mindset (European Center for Digital Competitiveness, 2020)
- Labor Force Survey (Employment by sex and occupation) (ILOSTAT)

USAID
FROM THE AMERICAN PEOPLE

BUREAU FOR DEVELOPMENT, DEMOCRACY, AND INNOVATION (DDI)
INNOVATION, TECHNOLOGY AND RESEARCH HUB (ITR)
digitaldevelopment.org