CYBERSECURITY PRIMER

How to Build Cybersecurity into USAID Programming

Photo: KC Nwakalor

OCTOBER 2021

USAID
FROM THE AMERICAN PEOPLE

DigitalFrontiers
SCALING DIGITAL DEVELOPMENT

DAI
Shaping a more livable world.

ACKNOWLEDGEMENTS

The *USAID Cybersecurity Primer* is the result of significant contributions from across USAID, DAI's Digital Frontiers Project, and our partner community, including implementing organizations. The *Primer* was written by a drafting team led by Stanley Byers (USAID) and Galia Nurko (DAI's Center for Digital Acceleration) with substantial contributions from Siobhan Pangerl and Maurice Kent (USAID), Inta Plostins (DAI's Center for Digital Acceleration), and Jeff Krentel and Erica Bustinza (DAI's Digital Frontiers). Report design and graphics were provided by Amber Pitts via Digital Frontiers.

The authors extend their appreciation to all USAID staff who participated in internal discussions and review of this report, especially the dedicated guidance provided by Michelle Parker and Allana Nelson. The authors thank USAID's Digital Sector Council and Cybersecurity Working Group members for taking the time to meet and provide input and/or peer review the *Primer*.

The authors accept responsibility for any errors or inaccuracies in this report.

This publication was produced by the Digital Frontiers Project under Cooperative Agreement AID-OAA-17-00033 at the request of the United States Agency for International Development. This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID) under the Digital Strategy Cybersecurity initiative. The contents are the responsibility of the author or authors and do not necessarily reflect the views of USAID or the United States Government.

TABLE OF CONTENTS

ACRONYMS

5G	Fifth Generation of Mobile Communications
AI	Artificial Intelligence
AOR	Agreement Officer's Representative
APT	Advanced Persistent Threats
BIP	Business Innovation Partnership
C2M2	Cybersecurity Capability Maturity Model
CaaS	Cybercrime-as-a-Service
CDCS	Country Development and Cooperation Strategy
CEIP	Carnegie Endowment for International Peace
CERT	Computer Emergency Response Team
CIC APS	Critical Infrastructure Cybersecurity Annual Program Statement
CIO	Chief Information Officer
CIRT	Cyber/Critical Incident Response Team
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CLA	Collaborating, Learning, and Adapting
CMM	Cybersecurity Maturity Model
COR	Contracting Officer's Representative
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CSO	Civil Society Organization
DCCP	Digital Connectivity and Cybersecurity Partnership
DDoS	Distributed Denial of Service
DECA	Digital Ecosystem Country Assessment
DRG	Democracy, Rights, and Governance
Fintech	Financial Technology
GBV	Gender-Based Violence

GFCE	Global Forum on Cyber Expertise
GH Data	Global Health Data Analytics and Technology Advancement
GIF	Greater Internet Freedom
GSCC	Global Cyber Security Capacity Centre
ICT	Information Communication Technology
IoT	Internet of Things
IP	Implementing Partner
ISC	Information Safety and Capacity Project
ISSO	Information Systems Security Officer
IT	Information Technology
LMICs	Lower Middle-Income Countries
M/B/IO	Mission, Bureau, or Independent Office
MFA	Multi-Factor Authentication
MITM	Man-in-the-Middle
ML	Machine Learning
NCSA	National Cybersecurity Alliance
NDAA	National Defense Authorization Act
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OU	Operating Unit
PDD	Project Development Document
PII	Personally Identifiable Information
S/CCI	State Department's Office for the Coordinator for Cyber Issue
SA	Standards Alliance
SMEs	Small and Medium-Sized Enterprises
US-CERT	U.S. Computer Emergency Readiness Team
USG	U.S. Government
UTRAMS	Unified Travel and Mission System
VPN	Virtual Private Network

ABOUT THIS PRIMER

Purpose of the Primer

In April 2020, USAID launched its first ever Digital Strategy that identifies cybersecurity as a new focus area for the Agency's technical programming. USAID partner countries are adopting digital tools and services but have minimal resources to combat cyber vulnerabilities that come with increased digitalization. This Primer will introduce the concept of cybersecurity as a development challenge, present opportunities to integrate cybersecurity throughout programming, and highlight cyber threat trends by sector.

Whom this Primer is for

This Primer is intended to increase awareness and provide a basic understanding of cyber threats, cybersecurity, and cyber resilience as they relate to development programming for USAID staff. It does not provide specific cybersecurity programming or operational recommendations or address technical cybersecurity needs of USAID or its implementing partners. This Primer is a resource on cybersecurity for the broader development community and spotlights how USAID's approach to cybersecurity in development is evolving.

How to Use this Primer

The Primer is designed for development practitioners seeking a range of information around cybersecurity concerns as they relate to USAID programming. Readers interested in specific topic areas are encouraged to skip ahead to that section. Please refer to the Table of Contents or the annotated contents below to select the sections of most interest to you.

For example, if you would only like to learn more about cybersecurity's applicability to USAID's Program Cycle, please review the section linked below to your current program stage. For an understanding of how cybersecurity risks relate to your sector of interest, visit the Trends by Sector section for an overview of cybersecurity considerations for each development sector. The Annexes contain more details and additional resources from each section including, but not limited to, definitions, relevant policies, and technical assistance opportunities.

WHAT YOU WILL FIND IN EACH SECTION

Introduction

What do we mean by "cybersecurity" in terms of USAID programming? This section explains key terms that we hear frequently and looks at how emergent digital threats affect our work.

Embedding Cybersecurity into USAID's Programming Cycle

The USAID Program Cycle consists of four key stages and each include unique and critical cybersecurity considerations.

Country/Regional Strategic Planning

The Country Development and Cooperation Strategy (CDCS) planning cycle presents an opportunity to consider current and projected contextual factors in the host country's digital ecosystem. These plans can include support to the government to strengthen abilities to mitigate cyber harms through improved regulations and policies, and other system-wide investments in infrastructure, partnerships, and private sector engagement.

Project Design and Implementation

Building cybersecurity into project design will mitigate potential harms. This section identifies priorities in the design and implementation of USAID projects and discusses how to incorporate cybersecurity responsibilities and tools into projects.

Activity Design and Implementation

By prioritizing the end user while leveraging and improving upon the use of existing structures, this section helps the reader think through the creation of an enabling environment for improved cyber practices.

Monitoring, Evaluation, and CLA

Capturing and learning from successes and challenges is critical in the rapidly changing world of cybersecurity. This section includes tips for including the right indicators for measurement and learning from the data that USAID continuously collects.

Trends by Sector

Cybersecurity affects each and every sector that uses digital technology. This section includes descriptions of the manifestations of cybersecurity across USAID programming sectors.

Critical Infrastructure

Democracy, Human Rights, and Governance (DRG)

Economic Growth, Finance, and Trade

Education

Environment

Food Security and Agriculture

Global Health

Annexes	The goal of this Primer is to provide the reader with the most important information for mitigating cyber risks and improving practices in work. The most critical content to meet this objective is included within main sections of the Primer, and additional information and resources are included in the Annexes.
Annex I: Glossary	Comprehensive reference for terms found within this Primer and additional terms of relevance to understand cybersecurity.
Annex II: Cyber Actors and Cybercrime	Additional information particular to types of actors involved in cybersecurity, and a thorough explanation of cybercrime.
Annex III: Additional Resources and Recommended Readings	A continuously evolving list of recommended readings and resources, including a brief summary to guide resource selection.
Annex IV: Key USG Cybersecurity Actors	Detailed list of U.S. Government cybersecurity actors including brief descriptions of each.
Annex V: USAID's Focus on Cybersecurity Reflects Broader USG Policy Goals	Detailed explanation of how USAID's cybersecurity work is coordinated with other U.S. Government policies.

Photo: Colby Gottert

INTRODUCTION

The first reported death due to a cybersecurity breach was in September 2020, when a ransomware attack prevented a patient in Germany from getting medical help in time to save her life.[1] Cyber attacks are on the rise globally, and our partner nations are particularly vulnerable. For example, Ukraine's first known cyber attack on a power grid led to 225,000 people losing power during the depths of winter in December 2015. An even larger cyber attack in 2017 affected the radiation monitoring system at the Chernobyl nuclear plant, as well as ATM infrastructure, airport computers, and other vital online systems. Voter registration data has been leaked in countries ranging from the Philippines[2] to Mexico.[3] More recently, hackers in Georgia published sensitive documents about COVID-19 management alongside deliberately falsified versions meant to mislead the public.[4] These examples demonstrate how **cybersecurity failures pose material threats to critical USAID partner countries and undermine partner country government legitimacy in the public eye.**

Digital technologies are transforming the ways in which the world's economies, governments, and people interact and engage with one another. USAID is increasingly asked to support the digitalization of partner nations, and the Agency's new Digital Strategy encourages investment in these digital ecosystems. As countries adopt a greater number of digital systems and tools, novel and fast-evolving vulnerabilities and risks proliferate. USAID's digital investments must include analysis on the opportunities and risks presented by digitalization and ensure any digital programming addresses **cyber harms** and includes cybersecurity mitigation measures.

DEFINING CYBERSECURITY FOR USAID PROGRAMS

Adapted from a definition provided by the U.S. Computer Emergency Readiness Team (US-CERT), cybersecurity for USAID programs is:

> The activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

In simpler terms, cybersecurity is the way that people, systems, and technology protect information kept in digital formats from being taken, damaged, modified, or exploited. Information can be taken in multiple ways. Cyberattacks occur when actors illicitly access computer systems and the information—or data—they contain. A large amount of information is also widely and legally available through the tracking of social media and other online activities, meaning attacks are not needed to collect sensitive information. There is a fast growing global industry of data brokers that analyze and sell information about individuals' online behavior.[5] Typically this is used for commercial marketing, but it is also used in political campaigns or can be exploited maliciously to achieve social or political outcomes through disinformation. False and misleading information can be targeted to specific online communities to influence their beliefs and actions, all without doing anything explicitly illegal.

Cybersecurity is critical to the USAID Digital Strategy's goal of achieving and sustaining open, secure, and inclusive digital ecosystems. As reliance on digital technology expands within an ecosystem, so do the number of vulnerabilities. Failing to mitigate these vulnerabilities can destabilize the digital ecosystem as a whole.

BOX 1

Common Misconceptions About Cybersecurity

USAID doesn't "do" cybersecurity. Every time USAID seeks to help a country develop an important economic sector, establish a health information system, expand the capacity of government services, or educate youth on digital technology, USAID is "doing" cybersecurity. Cybersecurity is integral to, not separate from, technology efforts. It should be thought of as a core thread that runs through all aspects of USAID's technology programs in order to ensure digital sustainability and resiliency. The key to doing cybersecurity well is being aware of the risks and opportunities and planning for them intentionally.

Cybersecurity is the Chief Information Officer (CIO) or information technology (IT) staff's problem. Cybersecurity concerns everyone within an organization because individual human behavior—even something as simple as clicking on the wrong link—is a major source of cyber vulnerability. Cybersecurity is everyone's collective responsibility because sitting at a keyboard is an organizational risk.

Cybersecurity requires expensive software and equipment. Basic measures targeting human behavior, such as mandating the use of passwords and teaching basic cyber hygiene, are the most important first lines of defense against cyber attacks. Because individual behaviors are a key risk factor for cyber intrusions, cybersecurity protections do not need to be fancy to be effective.

The right cybersecurity software will solve all cybersecurity problems. Even the best available cybersecurity tools cannot prevent a cyber breach or cyber attack 100 percent of the time.

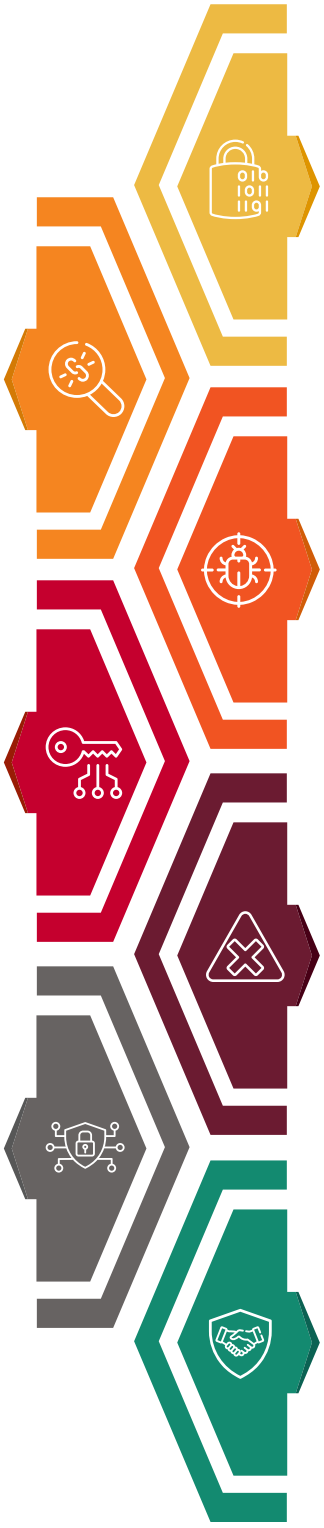
Cybercriminals and hackers will only target big companies in wealthy countries. Any organization in any country that uses digital tools—whether a business, a government entity, or a civil society actor—is at risk of a cybersecurity breach. Smaller organizations in USAID partner countries may actually be more attractive to hackers or cyber criminals because they typically have fewer cybersecurity protections in place.

Here are a few key terms used throughout the Primer that are important to understand (for a complete list of key term definitions, please see Annex I):

CYBER VULNERABILITIES are specific weaknesses in a computer system or online network, such as a lack of encryption or poorly designed firewalls that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks.[6] It can also be a deficit in capacity or skills of people to protect those systems or networks, for instance due to poor cyber hygiene (see Box 3) or insufficient available technical skills.

A CYBER ATTACK is an action taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools.[8]

CYBERSECURITY is the management of cyber risks and vulnerabilities to mitigate cyber threats, attacks, and harms.



CYBER RISKS are the potential for financial loss, disruption, or damage to the reputation of an individual, organization, or government from failure, unauthorized or erroneous use, or other malicious exploitation of its information systems.

CYBER THREAT is an action that takes advantage of security weaknesses in a system and has a negative impact on it. Threats can originate from two primary sources: humans and nature. Few safeguards can be implemented against natural disasters. Human threats are those caused by people, such as malicious threats consisting of internal (someone has authorized access) or external threats (individuals or organizations working outside the network) looking to harm and disrupt a system.[7]

CYBER HARMS are the damaging consequences resulting from cyber incidents, which can originate from malicious, accidental, or natural phenomena manifesting itself within or outside of the internet. They can affect individuals, organizations, or countries.

DIGITAL TRUST is created when users have confidence in an online system, network, or technology, and trust that their data and privacy are being protected when using them.

WHY DOES CYBERSECURITY MATTER FOR USAID PROGRAMMING?

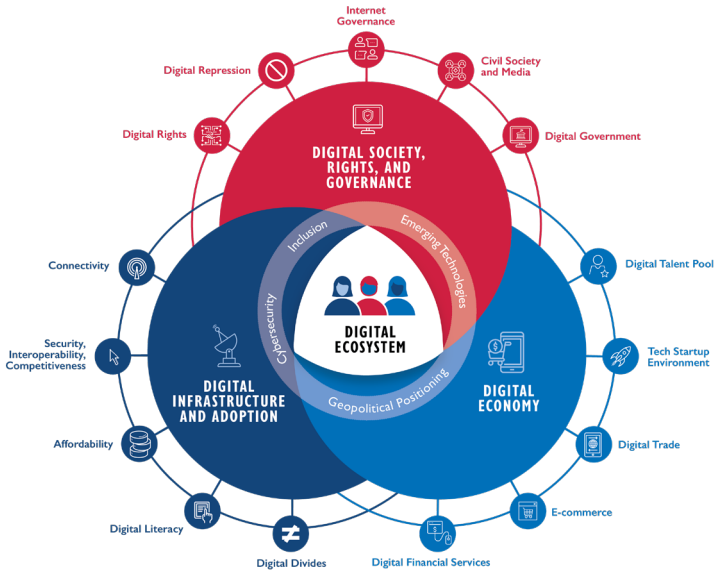
Strengthening cybersecurity is a guiding practice of USAID's Digital Strategy. In alignment with the National Cyber Strategy, USAID seeks to promote open, secure, and inclusive digital ecosystems. This entails supporting the adoption of policies that espouse global cybersecurity best practices; facilitating the protection of internet freedom; promoting the principles of the free flow of data and the protection of intellectual property; and prioritizing building the capacity of a cyber-ready workforce in the countries in which USAID works.

With global connectivity nearly doubling since 2014 to more than 4 billion people,[9] USAID is increasingly leveraging the power of technology to accelerate development outcomes. This trend has only been accelerated by the COVID-19 pandemic, which has required development actors to rely on digitally enabled approaches to development in response. However, economic and geopolitical trends, conversations with local experts, and anecdotal reporting all strongly indicate that cyber vulnerabilities pose a growing problem across the globe. This is particularly important because individual behaviors and a lack of cyber hygiene (see Box 3) are often the root cause of cyber vulnerabilities that lead to successful attacks.

In order to mitigate cyber threats to program investments, **cybersecurity must become a first-order strategic and operational priority across all phases of the USAID program cycle.** While some partner countries have already requested assistance in building up cybersecurity capabilities—often in reaction to cyber attacks—other countries may feel less urgency to prioritize cybersecurity given their geography or

BOX 2

Cybersecurity and the Digital Ecosystem



Digital ecosystem

A digital ecosystem comprises stakeholders, systems, and an enabling environment that, together, empower people and communities to use digital technology to access services, engage with each other, and pursue economic opportunities. It is organized around three separate, overlapping pillars: digital infrastructure and adoption; digital society, rights, and governance; and the digital economy. It also encompasses four cross-cutting topics: inclusion, cybersecurity, emerging technologies, and geopolitical positioning.

Cybersecurity

Effective cybersecurity requires adequate policies and strategies along with institutions that can implement those strategies. It also requires that institutions have the human and material resources to mitigate, detect, and prevent cyber attacks. Actors across governments, civil society, media outlets, and the private sector can include cybersecurity considerations in all aspects of operations including enterprise systems, procurement, supply chains, and contracting agreements.

BOX 3

What is Digital Literacy and Cyber Hygiene?

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.

CYBER HYGIENE is a key digital literacy skill that encompasses the practices and/or steps that individual users and organizations take to maintain their online security and strengthen the security of their computers or other digital devices. Many of these practices are routine and help ensure the protection of a person's identity or other sensitive information from being unknowingly accessed or corrupted. Though cyber hygiene varies by sector, several common cyber hygiene practices include:[10]

Password changes

Creating passwords or passphrases that are easy to remember but hard to guess and not repeated can prevent malicious activities and protect sensitive information.

Two-factor authentication

A method of establishing access to an online account or computer system that requires the user to provide two different types of information. According to NIST, 81 percent of hacking-related breaches leveraged stolen or weak passwords.[11] This is why it is important to employ two-factor authentication, when available, which adds a second layer of protection.

Use licensed software

To mitigate vulnerabilities, organizations should use licensed software, which is regularly updated to fix or "patch" a problem or "bug" in a computer program. Copied software leaves computers highly vulnerable to surveillance and attacks.

Updated inventory of assets

All hardware and software used should be kept in a secure inventory, including the installation of new software. This inventory will help identify vulnerabilities should the system become victim to a cyber-attack.

Software and hardware updates

Updating software on all devices is important for maintaining the health of that device. Many software updates come with patches to known vulnerabilities. Not all hardware needs to be updated to maintain performance standards, but hardware that is no longer being used should be wiped of all data and disposed of properly.

Back-up Data

All data should be backed up to a secondary source to avoid data loss as a result of a cyber attack or malfunction. Options include an external hard drive or cloud storage system.

Limit users

Not all people within your organization should (or need to) have the capability to access all the data within a network, system, or program. Access should only be granted to those who need it to perform their duties. All others should have limited capabilities.

level of connectivity, for example. However, as cyber threats grow increasingly prevalent and sophisticated, and as countries seek to gain from the dividends of the digital transformation of their economies, it is incumbent on practitioners to understand how cyber threats manifest in their programs to better meet the cybersecurity needs of partner country stakeholders.

Cybersecurity is a prerequisite to maintain the sustainability and value of development investments that leverage digital technologies. This Primer outlines how practitioners can integrate cybersecurity measures throughout the program cycle, across technical areas, and in line with the Digital Strategy and other relevant USAID and U.S Government (USG) policies, to protect a project or beneficiary's credibility, safety, and ability to deliver effective results.

Integrating cybersecurity into programming designs that use digital technologies will ultimately protect USAID investments and build the cyber resilience of partner countries.

Investment in cybersecurity also promotes U.S. values and supports the USG policy goals of national security and economic prosperity. See Annex V for more information about how USAID's work on cybersecurity aligns with USG policy documents and frameworks.

HOW CAN CYBER THREATS AFFECT USAID PROGRAMMING?

As noted, expanded use of digital technologies is dramatically improving lives while also creating the conditions for a steep rise in cyber crime, data harvesting, targeting, and surveillance. This is taxing on the severely limited cyber capacities in partner countries and threatens to undermine many efforts to improve social and economic well-being. The environments where USAID programs operate are being affected, and we need to understand these dynamics to ensure our investments are protected.

For example:

1 Digital financial systems in USAID partner countries are growing both organically and through USAID assistance. As more data and money move through these systems without comparable investment in security to protect them, they are becoming highly attractive targets for attacks. Given the interconnectedness of financial systems, "a successful attack on a major financial institution, or on a core system or service used by many, could quickly spread through the entire financial system causing widespread disruption and loss of confidence."[12] This is already happening according to a senior government official in Africa. They shared that their government has bet their country's future economy on the financial sector, but that their financial services systems are under continual and increasing cyber attacks. The official went on to say that while this was not being publicly reported out of fear of losing popular confidence, it is a major problem they currently have little ability to address, and they need help. Financial technology (fintech) leaders in Latin America echoed this concern. Programming in digital financial services must include cybersecurity measures, or a key element of digital advancement will be vulnerable.

2 COVID-19 has provided an unprecedented operating environment for cyber criminals targeting strained health systems. With hospitals across the globe at near or full capacity, attackers have been deploying disruptive ransomware against healthcare institutions in exchange for large payouts. These types of attacks cripple hospital computer systems, healthcare providers, and medical supply chains, and can lead to temporary or permanent loss of critical data.[13] A June 2020 cyber attack on South Africa's largest private hospital operator, Life Healthcare Group, affected its admissions systems, business processing systems, and email servers.[14] The 6,500-bed hospital was forced offline in order to contain the attack as it struggled to meet the influx of patients seeking treatment for

BOX 4

Cyber Harms: The Longer-Term Repercussions of Cyber Incidents

Cyber harms are defined as "damaging consequences resulting from cyber events, which can originate from malicious, accidental, or natural phenomena, manifesting itself within or outside of the internet."[15] They can potentially affect individuals, organizations, or countries. Cyber harms can be organized into six different categories: physical, psychological, economic, reputational, cultural, and political.[16] Cyber incidents affecting USAID activities can create cyber harms in any category, but cultural harms (in the form of country destabilization and violence toward the general public or specifically USAID and USAID activity staff) and reputational harms (diminished USAID standing, possible legal action, an opening for adversarial governments to further gain a foothold) are two of the most serious. Not only do cyber incidents cause immediate damage in the short-term, they can also have far-reaching secondary impacts that affect USAID safety and standing in the host country and around the globe.

COVID-19. While the financial impact of the attack is difficult to assess, the cost of simply restoring IT systems to full functionality was more than $4.2 million.[17] USAID is a leading donor in providing healthcare support to the COVID-19 crisis and has a unique opportunity to support partner nation health systems not only in providing health solutions, but in protecting the digital health infrastructure to ensure care can be available.

CROSS-CUTTING THREATS

Along with threats to specific technical areas, several cross-cutting threats also affect USAID programs:

Distrust of Digital Technology: Failure to address cyber risks may lead users to mistrust a digital tool or solution and reduce its adoption. It could also lower the public's trust in digital technology overall. For example, a financial inclusion program may propose using a fintech tool to bank underserved communities. Doing this, however, means that USAID and the implementing partner (IP) need to understand the security and privacy policies of the fintech tool being used. When these policies are not addressed and financial harm occurs as a result of a cyber attack, digital trust decreases, which can lead to reduced adoption of an otherwise valuable tool to advance financial inclusion efforts.

Misinformation and Disinformation Campaigns: Misinformation is when false information is shared, but no harm is intended. Disinformation is when false information is knowingly shared to cause harm.[18] Social media manipulation campaigns are growing across the globe. In 2019, 70 countries documented these types of campaigns, up from 28 in 2017.[19] Facebook and Twitter identified seven countries—China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela—that have carried out misinformation and disinformation campaigns beyond their borders in order to influence the events of other countries.[20] Misinformation and disinformation campaigns increasingly use licitly and illicitly acquired data to monitor and analyze target populations in order to improve the efficacy of messaging campaigns to influence outcomes and undermine trust in digital tools and services.

Increased Cyber Crime: As more data and money move through newly connected digital systems in USAID partner countries, they become attractive targets for digital surveillance and cyber attacks, especially if cybersecurity measures are weak. In addition, as cyber attack capabilities continue to become more sophisticated, threats to USAID programs will

also evolve and adapt to new security measures. A lack of data and underreporting of previous attacks prevent hard analysis, but cybercrime across regions, from Latin America to Eastern Europe, Africa, and Asia is increasing rapidly, especially in the wake of the COVID-19 pandemic. In its 2018 Global Risk Report, the World Economic Forum stated that the risks of cybersecurity are growing "both in prevalence and in disruptive potential. Attacks against companies have almost doubled in five years, and incidents that once were considered extraordinary are becoming increasingly common."

While 100 percent of attacks and information collection cannot be avoided, there are measures USAID can incorporate into programming to help beneficiaries mitigate and respond to cyber threats and attacks as they occur.

MITIGATING CYBER RISK/HARM THROUGH CYBERSECRUITY

USAID has integrated cybersecurity practices in some digital programming, led by a few of the Agency's innovative technical teams. This Primer seeks to highlight those practices that have proven effective and provide additional guidance to those new to this emerging challenge.

Capacity Development: USAID has worked with regulators and utility companies to improve their capacity to identify threats, fortify defenses, and strengthen resilience through improved response strategies and procedures. In doing so, USAID also provides an ongoing forum for regional utilities to exchange information and best practices with one another.

Cyber Hygiene: USAID provides training, technical assistance, and technology solutions that mitigate cyber vulnerabilities and risks of local organizations, such as civil society organizations, human rights defenders, and independent media organizations. Through organizational security assessments, followed by mentoring, training, and immediate triage support, USAID's support helps local partners respond to attacks while reducing their vulnerabilities.

Technical Assistance: USAID manages programs designed to help partner nations improve the cybersecurity of their critical infrastructure. This has included supporting partner countries through regional cybersecurity training to increase cyber awareness and the strategic planning capabilities of critical infrastructure operators and regulators. Specific activities included an e-learning course on cyber hygiene for university students; collaboration for cybersecurity curriculum development and delivery; the establishment of a Bug Bounty Center at a local institution; a two-stage cybersecurity hackathon competition involving U.S. and local students; and Cyber Security Improvement Grants to local institutions in critical infrastructure.

Photo: Riaz Jahanpour

BOX 5

How do Cyber Attacks Decrease the Public's Trust in Digital Technologies?

Stoking mistrust in government processes: Following the Brexit campaign in the U.K., Members of Parliament released a report that found that malign actors (possibly foreign governments) used digital technology, including botnets and artificial intelligence, to manipulate the outcomes of the vote. This included cyber attacks on voter registration websites as well as the use of social media platforms to sway public opinion. Together, these created doubt in the process and the narratives being shared.[21]

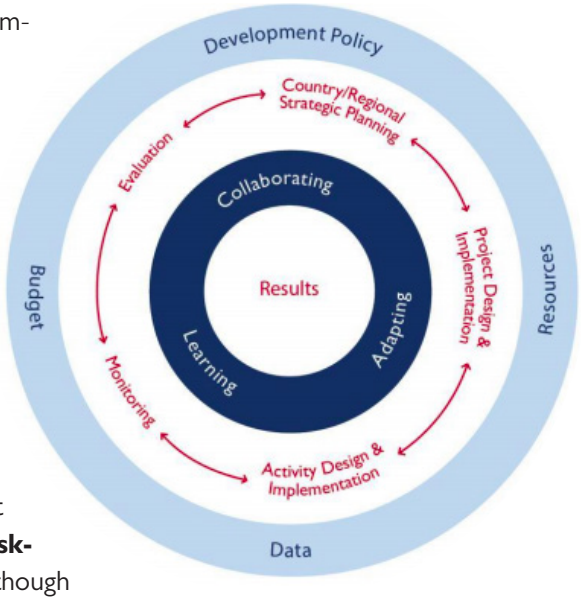
Shutting down critical government services: In December 2015, a Russian cyber attack known as Sandworm shut off Ukraine's power grid. It penetrated three energy distribution companies in Ukraine, which then disrupted the electricity supply to consumers and left hundreds of thousands of residents without power for one to six hours. This was the predecessor to the larger NotPetya attack, which aimed to target other aspects of Ukraine's critical infrastructure by taking advantage of a vulnerability in a Ukrainian accounting software. It ended up infecting millions of computers globally.[22]

Spurring violence against ethnic minorities: In 2018, the United Nations accused Facebook of facilitating violence against the Rohingya community in Myanmar by allowing anti-Muslim hate speech and dis/misinformation across their platform. In Puebla, Mexico, the spread of false information led to vigilantism and the murder of two young pollsters by mistake. [23,24]

Photo: Jack Gordon

EMBEDDING CYBERSECURITY INTO USAID'S PROGRAMMING CYCLE

NOTE: Although this Primer was originally designed for USAID Staff, the recommendations below may also be applicable to digital development programming more broadly.



Cybersecurity is critical to both the programmatic and operational success of USAID assistance, and should be a key part of each phase of the program cycle. What are the cyber risks in the partner nation digital ecosystem, and how could those affect USAID's development objectives? What mitigation measures do we need to incorporate at the strategic, project, and activity levels to support our development investments? How can we support the cyber safety and security of our beneficiaries and their data? Mission staff should ask these questions at each phase of the program cycle. This is a **risk-based approach to cybersecurity**; although digital tools will never be 100 percent secure, USAID Missions can systematically identify, understand, and prioritize the cyber vulnerabilities and threats within partner countries, and work with the governments to prioritize actions and resources to address them. This section describes how cybersecurity considerations can be incorporated into the different phases of the program cycle.[25]

COUNTRY/REGIONAL STRATEGIC PLANNING

Each country has its own unique digital ecosystem, which means cyber vulnerabilities and threats vary greatly depending on context. USAID staff need to have a broad understanding of connectivity, the IT and cybersecurity workforce, government digitalization approaches including legal and regulatory frameworks, and the digital economy such as financial services and e-trade. Geopolitics and regional dynamics can also have an outsized impact on country-specific cyber threats and cybersecurity landscapes. Effectively integrating cybersecurity into USAID's country or regional strategic planning process requires understanding the cyber risks and opportunities in our partner nation's digital ecosystem. Missions should consider the following information as they develop or update their Country or Regional Development Cooperation Strategy:

- **Assess partner country policies, strategies, and regulations around cybersecurity, data privacy, communications infrastructure, and digital tools.** Many USAID partner countries have begun developing cybersecurity policies and strategies that outline national priorities, areas of concern, and proposed solutions. USAID can identify areas of engagement with the host country government to promote an open, secure, reliable, and interoperable internet, as well as areas to avoid so as to not violate any partner country laws. Significant changes in a partner country's cybersecurity policy can also provide important clues around the changing geopolitical context of internet governance.

- **Seek input and learn from local information communication technology (ICT) and cybersecurity stakeholders**. During the initial stakeholder engagement process, USAID can actively seek out input and learn from the public sector, private sector, civil society, grassroots organizations, and other donors working on ICT or cybersecurity issues. Explicit outreach to local ICT entities that do not often interact with USAID can result in unexpected, positive collaboration. These actors can provide important country context as it relates to the broader digital ecosystem and how cybersecurity is being addressed, as well as appropriate tools and strategies to promote cybersecurity protections across USAID's portfolio in the host country.

- **Identify areas of alignment with existing USAID or USG strategies, partnerships, and initiatives.** During the CDCS development process, USAID Missions should look for opportunities to align their CDCS with the USG strategies, partnerships, and frameworks promoting USG foreign policy goals in the cybersecurity realm. USAID is promoting a values-based internet through the Digital Connectivity and Cybersecurity Partnership (DCCP). The USG is also using many of the same mechanisms—as well as the Development Finance Corporation and Indo-Pacific Strategy—to promote alternative telecommunications infrastructure options around the globe.

- **Engage with interagency partners on local cybersecurity needs and existing USG programming.** Tapping into cyber expertise at the interagency level allows USAID to build its knowledge of the local cyber landscape. Many USG actors work on different aspects of cybersecurity at the country level. An interagency approach can foster holistic, whole-of-USG responses to cybersecurity with the partner government that amplifies the impact of USAID's investments.

- **Coordinate with other donors to identify areas of alignment in cybersecurity.** Donors are increasingly funding cybersecurity programming. Aligning USAID's cybersecurity programming with the work of other donors will allow USAID to leverage their investments and knowledge in this space. This approach can also help define USAID's comparative advantage in the cybersecurity realm, so the Agency can pinpoint where its cybersecurity programming can add the most value in the local digital ecosystem.

- **Include cybersecurity concerns in each CDCS Risk Analysis and Mitigation Plan.** When drafting a CDCS, USAID Mission decision-makers should identify how local cyber capacity and cybersecurity vulnerabilities could affect USAID's ability to deliver on development

outcomes. This includes the potential implications of major cybersecurity incidents to USAID's local investments as well as the harassment of vulnerable USAID-supported civil society organizations (CSOs) and grassroots organizations. Each CDCS risk analysis and mitigation plan, or the assumptions linked to a results framework, should include cybersecurity vulnerabilities.

- **Incorporate Sub-Intermediate Results or cross-cutting elements about cyber threats, disinformation, or online harassment.** Integration of cybersecurity into a CDCS or USAID program may take the form of a discrete results framework sub-intermediate result, cross-cutting theme, or other cross-portfolio integration. Building local cybersecurity capacity helps protect the integrity of USAID investments and prepares USAID partner countries to tackle these difficult issues head-on. This proactive move would allow Missions to incorporate cybersecurity more easily into its downstream Project Development Document (PDD) and activity designs.

PROJECT DESIGN AND IMPLEMENTATION

Cybersecurity can also be integrated into project design and implementation. This is particularly important for USAID projects that have a digital element, such as projects that promote the use of digital communications tools, use digital tools to distribute information to beneficiaries, or that assist governments and industries to use information technology.

- **Research project-specific cyber vulnerabilities.** USAID Missions should be aware of how key actors within a particular sector—including host country government counterparts, private sector companies, and civil society—use technology, what systems they use, and what they use them for, as well as typical disinformation pathways. With this information, USAID can better identify cyber vulnerabilities and find modalities to address or mitigate them within each project. Even though the same cyber vulnerabilities and threats can occur in any technical sector, each sector faces its own specific and unique mix of vulnerabilities and threats. For example, major cyber concerns in the global health sector include vulnerabilities in health management information systems and case management systems (especially given the sensitive information stored therein), while major cyber concerns in the Democracy, Rights, and Governance (DRG) sector include vulnerabilities in peer-to-peer messaging platforms and the enterprise systems of individual CSOs, media outlets, or human rights defenders. Because each sector faces its own challenges, which vary from country to country as well, it is important to research country-specific and sector-specific cyber vulnerabilities. Please see the Trends by Development Sector for more information.

- Assess the importance of digital trust on a project's success. Digital trust is created when users have confidence in the digital technology they use and trust that their data and privacy are protected while using it. If hacks, online harassment, disinformation campaigns, cyber crimes, and/or cyber attacks occur regularly within a digital ecosystem, local stakeholders may no longer trust digital technology or may lose their faith in USAID programming. This can negatively affect USAID projects that seek to promote the safe and secure use of digital technologies. To remedy this, USAID can prioritize the development of digital trust within its programming and embed the principles of digital trust[26] into project design.

- **Embed cybersecurity considerations, resources, responsibilities, and management tools into every project.** To help beneficiaries address cyber vulnerabilities before they are exploited and become threats, USAID should embed cybersecurity into the project design process and thereby into project implementation. This proactive mindset around cybersecurity planning and investment at the design stage will position USAID for cost-savings through reduced financial impacts to programming from

BOX 6

Digital Ecosystem Country Assessments

USAID's Digital Ecosystem Country Assessments (DECAs) are a standardized assessment of a digital ecosystem that can help inform country-level strategic planning, the design of projects and activities, and the implementation of activities. A DECA examines a country's infrastructure; access to, and the use, collection, and analysis of, data; digital society and governance; censorship, information integrity, and digital rights; cybersecurity; digital finance; and digital trade and e-commerce. The resulting report identifies concrete areas of opportunity and risk for Mission-funded programming based on where a country currently sits. In countries in which extensive gaps in the digital ecosystem exist, Missions can build responses into sector-level programming or develop cross-cutting efforts country-wide. By taking a holistic view of ecosystem challenges and U.S. engagements and investments in-country, a DECA can facilitate interagency collaboration and private-sector engagement to strengthen the digital ecosystem. The first two pilot DECAs were conducted in Colombia and Kenya. In 2021, the Digital Strategy team will launch a DECA toolkit that USAID Missions can use to conduct the research with an implementer of their choice.

cyber attacks that are less likely to occur as a result. This may include:

- Using the findings of a DECA (see Box 6) and/or an analysis of the cybersecurity environment to inform PDDs.
- Including cybersecurity considerations in the Key Risks section of PDDs.
- Leveraging other cybersecurity resources within USAID and the USG to support the project, including the actors included in Annex IV.
- Facilitating coordination on cybersecurity issues among projects and among project activities.

- **Develop standalone cybersecurity elements within projects with digital components.** If technology comprises a significant part of a specific PDD, USAID Missions should include cybersecurity (including countering mis/disinformation) as a cross-cutting activity. This will help ensure it is built into any activity design that supports and protects digital investments.

ACTIVITY DESIGN AND IMPLEMENTATION

Given the risks that cyber threats pose to USAID programs and beneficiaries, USAID activities should incorporate cybersecurity best practices, which are grounded in the Principles for Digital Development:

- **Design activities that support development of resilient cybersecurity in host countries.** In addition to embedding cybersecurity into all USAID activities, USAID Missions can also design and procure activities with the goal of improving cybersecurity and cyber resilience (including countering misinformation and disinformation) in the partner country. This is especially important for partner countries that are vulnerable to cyberattacks.
- **Protect digital tools/solutions.** USAID should build cybersecurity protections into the design and operation of program-funded digital tools/solutions, including mobile

applications websites and case management systems, for example. The below considerations should be taken:

Install licenced hardware and software: Ensure that proper hardware and only licensed software are installed.

Consider interoperability needs: Interoperability is the capability of systems, devices, and applications to share information. It can help users access information more easily, while helping institutions manage costs. To effectively secure information in interoperable systems, cybersecurity should be considered across systems, and not only for a single component. Adopting cybersecurity standards, as opposed to bespoke solutions, can help set up partners for success when they connect systems at a later date.

Digital literacy and resources for partners and end-users: Government officials, organizations, or others responsible for the implementation and maintenance of the digital solution need to be trained on appropriate cybersecurity measures to protect the system and data, or those entities should hire staff with the appropriate skills. Furthermore, end users of the digital tool should also be educated on cyber protections and receive cyber hygiene training. End users must understand how to use the digital tool safely and appropriately through cyber hygiene training in order to protect their privacy, stay secure, and maintain their trust in the digital tool. Box 3 highlights how individuals practicing good cyber hygiene provide the first line of defense against cybersecurity threats and attacks from mal-organizations.

Budget appropriately: Activity budgets should include sufficient financial and human resources for a beneficiary to procure, install, secure, and maintain the digital tool or solution.

- **Build trust into activity design and implementation.** If partner organizations or beneficiaries do not trust the digital tools, equipment, or systems that USAID activities use, they are less likely to participate in those activities. This is especially true in countries with low levels

BOX 7

What Type of Cybersecurity Investments Can be Made at the Project or Activity Level?[27]

- Promote informed investments in the development of communications infrastructure and digital markets, especially as USAID partner countries make key decisions about 5G.
- Support the adoption of policies and regulations that espouse global best practices in digital infrastructure, cybersecurity, and multi-stakeholder internet governance.
- Strengthen the capacity of partner governments to secure their data systems against attacks.
- Facilitate the protection of internet freedom.
- Prioritize the development of a cyber-ready workforce, including adding cyber/digital education at all levels (K-university)
- Promote cooperation with the private sector in key industries (e.g., finance, energy, health) to improve capacity to strengthen cybersecurity and preserve trust in digital services.
- Promote and facilitate the participation of domestic stakeholders in relevant international fora.
- Support the creation of trusted mechanisms for sharing information about breaches and attacks.
- Provide training or support resources to smaller, local groups that have to confront disinformation or harassment campaigns.
- Support training on critical use of information in general education programs.

of digital trust, where online harassment and mis/disinformation run rampant, and where citizens are wary of using digital technology in the first place.

Following Digital Principles such as Design with the User and designing with local ownership from the beginning can help ensure that a tool is appropriate and trustworthy. Designing together means partnering with users throughout the project lifecycle, co-creating solutions, and continuously gathering and incorporating users' feedback, instead of designing a "black box." When appropriate, Agreement Officer's Representatives (AORs) and Contracting Officer's Representatives (CORs) can ensure that IPs dedicate time and resources within the work plan and budget to:

Engage local technical working groups and community groups for feedback.

Perform a rapid assessment to identify which digital tools are trusted by beneficiaries and why.

Engage local stakeholders, IPs, and donors to understand how trust has played out in other digital activities.

Establish a plan for quality assurance and customer support.

Develop a change management plan; and

Support local stakeholders to play a meaningful ownership role throughout the project cycle, from design to maintenance.

- **Find creative, low-cost ways of incorporating cybersecurity into IP meetings and events.** For example, CORs/AORs can designate cybersecurity as a core topic during regular IP meetings and request cybersecurity documentation during site visits. Such methods will also help ensure that cybersecurity remains top of mind for IPs.

MONITORING, EVALUATION, AND CLA

Monitoring and evaluating cybersecurity-related strategies, projects and activities can generate evidence that can be fed back into the collaborating, learning, and adapting (CLA) phase of the program cycle in order to drive Agency-wide decision-making on cybersecurity. Below are some suggested actions for beginning the feedback loop:

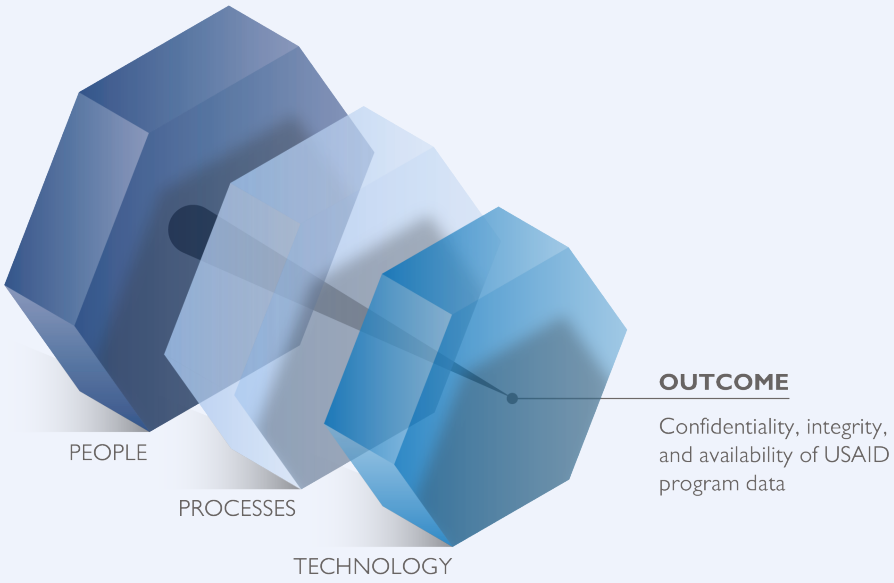
- **Develop cybersecurity-related indicators to measure the effectiveness of cybersecurity interventions.** Develop and use cybersecurity-specific indicators to measure and evaluate the success of its projects and activities with a cybersecurity or technology focus, as appropriate. To do this, consult with other USG agencies working on cybersecurity issues, adapt existing indicators from ongoing programs such as Digital APEX (managed by the Technology Division in the Innovation, Technology and Research Hub) or Greater Internet Freedom (managed in the Democracy, Rights, and Governance Center), and/or collaborate with private sector actors to adapt their existing cybersecurity tools for monitoring and evaluation purposes. Once data is collected, these indicators will be used to measure and evaluate the effectiveness of the cybersecurity program over time. For example, a new activity promoting cybersecurity upskilling and workforce development may include an indicator specific to cybersecurity capacity building. This indicator can then gradually be rolled out to other USAID activities with a cybersecurity or technology component, helping the Mission evaluate which types of cybersecurity capacity building interventions work best in-country.

- **Compile lessons learned from implementing cybersecurity interventions.** Once specific cybersecurity indicators are developed, implemented, and collected, this information can be consolidated to identify successful cybersecurity approaches and interventions. Key takeaways should be integrated into future PDDs, activity designs, and CDCS development and planning. Through this approach, USAID can scale interventions that have proven successful and learn from the failures of the less successful ones.

BOX 8

A Systems Thinking Approach for Cybersecurity Integration

For USAID staff considering the development of a standalone cybersecurity component or cybersecurity integration across a program, an emerging best practice among some existing USAID projects is to utilize a **people, processes, and technology conceptual lens** to assess potential interventions that result in a systems thinking approach to cybersecurity. Application of this approach will also help to ensure the confidentiality, integrity, and availability of USAID program data.



PEOPLE

Examines the capacity, behaviors, and resources that an individual within an organization must maintain and update their own cyber hygiene in order to remain secure in any digital business activities they carry out. Beyond individuals, USAID staff should consider the cyber-capable workforce working in the targeted digital ecosystem and whether the existing capacity and sustainability of that workforce is in place. This element of the framework is the most critical but often neglected due to predominant focus on technology-based approaches.

PROCESSES

Assesses the processes for procuring appropriate technology, response protocols for cyberattacks, and approaches for knowledge sharing on best practices for networked organizations. This element requires coordination between leadership, staff, and potentially partners to ensure cybersecurity practices are institutionalized and sustainable, even when key staff turnover.

TECHNOLOGY

This includes sector-specific risk assessments and organizational maturity assessments to determine appropriate and cost-effective technology solutions in order to keep an organization's digital ecosystem secure given the level of risk in the system they operate. Also ensuring that the organizations being supported have adequate capacity to support, operate, and sustain the effective use of cybersecurity technology is critical.

Photo: Riaz Jahanpour

TRENDS BY SECTOR

This section provides a high-level glimpse at cybersecurity vulnerabilities in USAID sectors, and demonstrates the importance of learning from previous cyber attacks to protect USAID investments. While there are general threats that are sector-agnostic, sectors in which USAID works have different vulnerabilities that merit individual review. These examples are by no means exhaustive. Annex III provides additional resources to stay current on cybersecurity trends and prevention measures.

CRITICAL INFRASTRUCTURE

According to the Department of Homeland Security, critical infrastructure includes the "assets, systems, and networks, whether physical or virtual, considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." There are 16 critical infrastructure sectors that underpin the functioning of any country, many of which USAID supports through programming. These include energy, communications, transportation, health, defense, chemical, commercial, emergency services, water, nuclear, information technology, financial, manufacturing, and dams.[28]

These sectors use digital technologies to capture data, improve and expand service delivery, and optimize system performance. While this improves the agility and integration of services, it also creates opportunities for actors looking to disrupt or prevent critical service delivery. This can include cyberattacks as part of a warfighting effort (see Box 5), or an attempt to gain a competitive edge gone horribly wrong. In October 2016, a massive Distributed Denial of Service (DDoS) attack caused half of Liberia to go offline. The perpetrator was a young and unemployed hacker contracted by a local Liberian telecommunications company to gain a competitive edge over Liberia's only other telecommunications company. The self-taught hacker modified a virus freely available on the dark web and unintentionally disrupted the country's connectivity for almost a week. This affected banking transactions, internet access, and even communications between international agencies and health workers responding to the Ebola crisis.[29]

These are just two examples of how critical infrastructure can be disrupted by a cyber attack—either intentionally or not. As networks across sectors become more interdependent, securing critical infrastructure sectors is a prerequisite to the uninterrupted operation of essential services.

DEMOCRACY, HUMAN RIGHTS, AND GOVERNANCE (DRG)

DRG programs often work in areas considered to be politically sensitive by some partner governments, including elections, human rights, and counter-trafficking in persons. In addition, DRG programs frequently work directly with groups that are the targets of authoritarian governments, like human rights defenders, independent media, and marginalized groups like the LGBTQI community and ethnic minorities. Cyber surveillance, cyber attacks, and the exposure of personally identifiable information (PII) are increasingly employed by authoritarian governments and other nefarious actors looking to disrupt or manipulate these programs and threaten their beneficiaries.

Mobile social networking and messaging apps like Facebook, Twitter, WhatsApp, and Instagram are often used to share

BOX 9

5G and Secure Digital Infrastructure

5G stands for the fifth generation of mobile communications. This follows in the footsteps of 2G, 3G, and 4G connectivity. Unlike its predecessors, 5G is expected to be extraordinarily fast, with download speeds at least 300 percent faster than 4G and low latency that will support services such as driverless vehicles.[30] In the way that the internet revolutionized modern life, 5G is expected to unlock new technologies, new business models, and new ways of life that we cannot yet fully conceptualize. Check out this USAID-supported website on Civic Space and 5G to learn more.

5G represents a powerful advancement in connectivity and will require upgraded infrastructure such as cell towers and new regulatory frameworks. U.S. and European companies are developing their own 5G infrastructure to deploy in their home countries or to sell abroad. Authoritarian countries are following suit. Insecure networks provide a potential mechanism for digital espionage as a means for social control, restriction of information, inappropriate use of personal health or financial data, and disruption of business and public sector activities. An insecure digital infrastructure will adversely affect data privacy and trade in digital goods and services, and potentially undercut the autonomy of host country governments. USAID partner countries are already making decisions on 5G infrastructure deployment; choosing untrusted network equipment could endanger their national interests along with U.S. national security interests.

USAID support in mitigating cyber harm will be more critical as 5G rolls out across the globe. This support is envisioned to include: 1) assisting governments in developing legal, regulatory, and policy approaches that protect citizen privacy and security; 2) ensuring civil society watch dogs have the tools and know-how to report on government management of 5G roll out; and 3) providing digital literacy training so that citizens are able to protect themselves from cyber harms.

news and information in low- to middle-income countries (LMICs). This is creating massive amounts of personal data,

news and information in low- to middle-income countries (LMICs). This is creating massive amounts of personal data, which are now available to a variety of interested parties if they have the means to acquire it. They can scrape data directly from social media itself, buy from the fast-growing data broker market, or illegally obtain it by penetrating a digital system. Research studies have found that by only using publicly available Facebook "likes" as a measure, AI-enabled computer models are able to predict detailed characteristics of users—including age, race, education, income, sexual orientation, drug use, political attitudes, artistic preferences, and physical health—often more accurately than close friends, spouses, and even users themselves.[31] The combination of these methods with the growing market and use of surveillance technology (see Box 11) only further muddles the landscape for DRG programming.

With these detailed user profiles, it is possible to identify and define social divisions, exacerbate those social divisions, or influence the opinions of voters, and then easily and cheaply scale this capability across an entire population through digital tools. These trends are well-documented in high-income countries and are becoming increasingly popular tools in LMICs, which often have weak institutions and social cohesion, making them much more vulnerable to digital manipulation campaigns.

For instance, in 2019 the Tunisian-based company UReputation was found to have operated a complex digital manipulation campaign across several digital platforms to influence the Tunisian presidential election as well as other elections across the African continent.[32] Such campaigns can also erode a citizenries' trust in information, making it difficult for an independent media to operate effectively either due to distrust from the public or manipulative information campaigns used as an excuse by the national government to limit media's independence.

Censorship is another way in which governments can limit the use of digital platforms to repress opposition or minorities within the country. This can take the form of censoring both online or offline communications. When it comes to online communications, there are examples of countries arresting activists following a social media post they did not like. For instance, in Vietnam, several activists in the last five years have been arrested for anti-government social media posts.[33] Such an environment discourages individuals from using social media or other internet-based applications out of fear of being identified. As a result, many move their operations to more secure digital platforms or other alternatives.

BOX 11

Why Should USAID Promote Alternative Infrastructure Models?

A key U.S. foreign policy objective is the promotion of open, interoperable, secure, and reliable information and communications infrastructure. However, this can be difficult to achieve in practice.

Even though U.S. and European companies are recognized as world leaders in information and communications infrastructure development, they may not be able to match the low-price points offered by other countries. If USAID, other USG agencies, and the U.S. private sector can partner to offer alternative financing and infrastructure models to USAID partner countries, as well as tools and expertise for cybersecurity oversight, this can serve as an effective tool to promote U.S. technologies, investments, and national security interests abroad. Connectivity infrastructure can present cyber vulnerabilities and should be considered when developing programming that includes the use of digital tools and technologies.

ECONOMIC GROWTH, FINANCE, AND TRADE

In a 2019 survey, 300 global CEOs cited the lack of cybersecurity as the single greatest threat to the global economy over the next decade.[34] In the majority of USAID partner countries, small and medium-sized enterprises (SMEs) generate a significant portion of GDP. Because SMEs tend to have low levels of cybersecurity, they are common targets for cyberattacks including cybercrime, especially if they serve as part of a supply chain for larger companies or government institutions. For instance, a study carried out by the National Cyber Security Alliance found that about 25 percent of SMEs surveyed do not have a cybersecurity plan in place, despite the evidence that cyber-attacks can have devastating financial consequences on the business.[35] This vulnerability has been exacerbated as the COVID-19 pandemic ravages the global economy.[36] For instance, cyber criminals have targeted financial institutions and health care systems, including the SMEs like medical suppliers and local banks linking these supply chains.

SMEs only represent a small piece of how weak cybersecurity can affect an economy. In thinking about the issue at a macro-level, it is important to consider the level of cybersecurity of institutions deemed critical to the function of the economic and financial vitality of a country: ministries of finance, central banks, and large banks.[37] If any of these institutions were to be a victim of a cyberattack, the loss of data or cost of recovering from the attack could be detrimental to a country's economy, causing financial harm to a range of actors including, but not limited to, the national government, businesses, or individuals.

The use of financial technology to improve or automate financial services adds another layer of complexity to a cyber-secure financial sector.[38] Any entity that offers financial services online—whether it is a fintech start-up, a microfinance institution, a community bank or credit union, or a non-bank financial institution—is at risk of a cybersecurity breach. A study of some of the most popular fintech apps in major markets found that 86 percent had major cyber vulnerabilities.[39] In Asia, the rising cybersecurity concerns are slowing the deployment of new fintech services. In particular, there has been an increase in the use of phishing and spoofing to trick unwary consumers into entering their PII and passwords on fake sites, stealing the information to obtain access to people's accounts.[40] In Kenya, Techonomy reported that a leading local cybersecurity expert "likened the Kenyan digital economy to a slow, plump gazelle stumbling through the 'cyber savannah' in the full view of agile and hungry cyber predators."

EDUCATION

There is a direct link between increased global connectivity and increased access to education. To reach a wider audience, both formal and informal education institutions are providing more educational material online. In-person education now utilizes technology to track student progress and assign homework. Simultaneously, these same institutions are using technology to manage human resources, budgets, and student information, and to share research. As such, these institutions host a wealth of data, including personal information of staff, faculty, and the student body, making them attractive targets for cyber-attacks.

Cyber criminals interested in financial gain within the education sector are not the only perpetrators. State-sponsored actors also seek to gain access to sensitive research, stop research that might be politically embarrassing, or influence institutions to adopt more favorable policies to a specific country.[41] Students, faculty, and visitors increasingly using their own personal devices to connect to Wi-Fi networks further complicates this issue, resulting in a growing emphasis on protecting the digital privacy and security of children and youth.[42]

Global data on the number of cybersecurity attacks on the education sector is limited, although some high-income countries are starting to pay more attention. For example, in 2019 alone, ransomware attacks targeted more than 1,000 U.S. schools.[43] With the average cost of addressing a ransomware attack in the United States estimated at approximately $8 million,[44] these attacks have a huge financial impact on schools and can

BOX 11

What is Surveillance Technology?

Surveillance technology refers to the use of digital technology to monitor the behavior or movement of people in public and private places. Governments and private companies can use it to target, intimidate, or otherwise influence individuals and groups. Surveillance technology typically includes cameras with facial recognition software (often combined with artificial intelligence and machine learning), mobile phone-based monitoring with GPS, social media monitoring, including encrypted messaging applications like WhatsApp and Signal, and the monitoring of digital financial transactions.

How pervasive is surveillance technology?

A 2018 Freedom House report found that 18 out of 65 countries reviewed used AI-based surveillance technology.[49] Just a year later, the Carnegie Endowment for International Peace (CEIP) found 47 of the same countries now use such technologies, representing a 160 percent increase.[50] CEIP expects the number of countries to continue to increase rapidly as technology systems proliferate and mature. They also found that the "most important factor determining whether governments will deploy this technology for repressive purposes is the quality of their governance." Even if governments do not misuse the technology, the systems and the data they produce are unlikely to be sufficiently protected to prevent access by sophisticated or well-resourced third parties.

force scarce resources to be diverted away from computers and textbooks to recovery efforts. The education sector in USAID partner countries are no less vulnerable to malicious cyber behavior; the University of Limpopo in South Africa was a victim of a cyber attack at least twice in 2016.[45] As a sector that already struggles with adequate funding in many of USAID's partner countries, cybersecurity prevention measures (and the budget to do so) need to be put in place to protect the massive benefits that increased connectivity provides the education sector.

ENVIRONMENT

A 2019 Siemens/Ponemon Institute study found that more than half of gas, wind, water, and solar utilities around the world have suffered from at least one cyber attack.[46] As industrial systems digitize and increasingly incorporate emerging technology, like IoT (Internet of Things)-enabled sensors, the likelihood of a cyber attack increases. State-sponsored cyber attacks or other cyber criminal activity find these systems to be an attractive target precisely because they can cause severe damage.

In the last two decades, attempts to disrupt these systems and cause environmental damage have been documented globally. For instance, in 2000 a cyber criminal caused the release of over 8,000 liters of untreated sewage in Australia. In 2009, a disgruntled employee shut off the leak detection system of three off-shore oil rigs in Long Beach, California.[47] More recently, City Power—the city of Johannesburg's electricity utility—suffered a ransomware attack that prevented its customers from accessing its website or purchasing electricity units.[48] These cyber incidents, if undetected, can cause severe damage to the environment, costing millions of dollars in recovery.

As USAID partner countries begin to digitize their industrial systems, and as their reliance on IoT devices to detect natural disasters (like floods) increases, USAID will need to consider

BOX 12

Leadership as a Lynchpin to Organizational Cybersecurity Investment

A promising approach to getting organizational buy-in for cybersecurity investment with key partners has stemmed from USAID's work in the energy sector. In line with the people, processes, and technology lens, the USAID Bureau for Europe and Eurasia's Energy and Infrastructure Division developed targeted outreach to decision-makers in partner nations, including C-Suite level leaders of utilities and regulatory bodies, who are in positions to make key decisions about cybersecurity investments. This was an iteration of USAID's prior approach that worked directly with IT departments that understood the challenges posed by weak cybersecurity but were unable to make concrete commitments to strengthening their cybersecurity because they were not the key decision maker.

On the utility side, the project convened utility CEOs from across the region, along with heads of large U.S. utilities to raise awareness on the risks and significant potential costs related to cyber threats. Initial results indicate that a shift in organizational culture among the CEOs was taking shape and that IT staff were given more license to participate in USAID activities, share knowledge and problems more openly, and suggest better approaches to managing cyber threats within their organizations.

On the regulation side, regulators were introduced to enhanced cyber-related regulations that could help them overcome the challenges of working in a common law regulatory environment and capacity building on developing strategies and tools that can be used to assess the maturity of utility cyber preparedness. Initial results of this effort include some new regulations and increased uptake of the tools to better interface with the utilities in order to develop strengthened approaches to facing the increasingly dynamic threat landscape in the sector.

how to protect these systems from cyber vulnerabilities. In this regard, coordination with local actors, including government and private sector actors, will be critical, as will working closely with IPs to ensure that the systems they deploy across USAID programs have the right people, processes, and technology in place to prevent cyber attacks.

FOOD SECURITY AND AGRICULTURE

Digital technologies have been and will be increasingly relied on to boost agricultural productivity in order to meet global food demand. As the move to precision agriculture quickens over the coming years, automated machinery, high-resolution multispectral imagery, drones, soil sensors, and a range of other IoT technologies will proliferate and farms will generate an ever-greater amount of agricultural data.

Current analysis and trends suggest that most agricultural technology devices will be produced by a small number of companies in foreign countries, rendering them highly vulnerable to cyber attacks and data theft and manipulation, and creating a wide range of possible threat vectors. Foreign governments could use another country's agricultural data to give themselves an advantage in trade negotiations or commodities markets.[51] Activists or competitors could steal, manipulate, and then publicly publish false and harmful data to undermine local industry. Following trends in other sectors, easily deployable ransomware attacks on critical data and equipment that threaten to destroy farmers' data and systems unless the ransom is paid will become more common, especially during time-sensitive windows for planting and harvesting.[52] The weaker, more exploitable links

in the chain of IoT devices will be used as a stepping stone to access connected systems further up the supply chain, leading to much broader risks such as sector-wide cyber attacks. Lastly, building trust among farmers to try new technology is another key barrier. Many farmers are rightly concerned that valuable and private information about their land and crops could be stolen or used against them, leading some to resist joining agricultural co-ops that could help boost farm productivity by aggregating data across farms to improve forecast accuracy and lower input costs.

GLOBAL HEALTH

Technology is shaping the future of health care across the world, expanding access to underserved communities, empowering patients with information, and lowering the cost of care. However, health is also one of the sectors most fraught with cybersecurity concerns. For example, the detailed nature of personal information contained in medical records make them high value targets by cyber criminals on the dark web who use stolen PII to facilitate other crimes. Health care providers have experienced a surge of ransomware attacks in the past few years. The 2017 WannaCry ransomware virus is perhaps the most damaging, and well-known. In the U.K., it crippled the national healthcare system for nearly a week and cost the National Health Service $114 million to repair.[53] In just the last three months of 2019, one industry report tracked a 350 percent increase in healthcare ransomware attacks, and there has been an uptick in attacks as hospitals and healthcare systems grapple with their response to the COVID-19 pandemic. A June 2020 cyber attack on South Africa's largest private hospital operator, Life Healthcare Group, affected its admissions systems, business-processing systems, and email servers as the hospital struggled to meet the influx of patients seeking treatment for COVID-19 symptoms.[54] The growth of online mis/disinformation in the health sector also poses a clear threat to our wellbeing, as evidenced by COVID-19 "infodemic."

Cybercriminals continue to target the health sector because of its many vulnerabilities, the high black-market value of its data, and the willingness of many healthcare providers to pay to recover access to their systems. The health sector's commitment to interoperability and open source technologies and systems may actually increase the likelihood of a cyber incident; the more open and interconnected our systems are, the greater the likelihood of a cyber vulnerability and an attacker who will exploit it. Given the quantity of data collected by healthcare systems in higher income countries, they have been the target of the majority of cybersecurity attacks. These incidents provide valuable lessons on cybersecurity risk management in healthcare that can be applied to USAID programs in developing countries seeking to strengthen and protect incipient healthcare systems.

Photo: David Rochkind

CONCLUSION

Cybersecurity is a critical development challenge that increases in importance as the world's population comes online. Digital technologies are the backbone for public and private systems, yet safeguards on those systems and for the data contained within lag far behind.

These developments have direct impacts on USAID programming and present an important new frontier of development. The Agency's Digital Strategy highlights the importance of digital technologies for programs across technical sectors and various geographic regions. From a cybersecurity perspective, this means USAID, unlike most other organizations, must try to understand and monitor the digital threat landscape across sectors as diverse as healthcare, agriculture, governance, media, education, infrastructure, and environment.

USAID programs are often implemented in high-threat environments by hundreds, or even thousands, of implementing partners and beneficiaries that do not have access to sufficient resources or skills to mitigate cyber threats effectively. A failure of cybersecurity by any one of these organizations creates risks for all others to which they are digitally connected, including USAID.

The cyber challenges USAID will face are also evolving rapidly, and require all stakeholders to become more adaptable, build new capabilities, establish more agile operational systems and procedures, and refashion decades-old development models to reflect the opportunities and challenges of the digital era.

As internet connectivity and usage is becoming fully global, interdependencies between different parts of these networks are growing, along with our reliance upon them. This means the range and scale of vulnerabilities and attack vectors and the possibility of catastrophic failure is increasing. New technologies such as Artificial Intelligence (AI) are also changing the game, allowing hackers to automate attacks, increasing both their speed and scale, and improving their precision and efficacy while making evasion of monitoring easier. Though network defenders are also using AI to detect and counter attacks, it remains unclear which side will prove more effective in wielding this powerful tool.

In short, analysis of these various trends strongly suggests that unless significant improvements are made in the near-term, including the rapid development of new cyber capacities, tools, policies, and procedures, our systems will be increasingly vulnerable.[55]

The above description is not intended to portray an overly dire situation, but to explain why cybersecurity is now a first order priority in Agency programs. Fortunately, there are many lessons to be learned from other agencies and private companies, and USAID is well positioned to be a leader in designing and implementing the models necessary for improving cybersecurity in development and helping to safeguard the immense progress of the past several decades.

Photo: John O'Bryan

Photo: KC Nwakalor

ASSESSING CYBERSECURITY RISKS AND OPPORTUNITIES

Now that you understand the need to incorporate cybersecurity into programs, where should you start?

UNDERSTANDING THE CYBERSECURITY LANDSCAPE

Below are questions included in USAID's Digital Ecosystem Country Assessment, which are useful for providing a general overview of the cybersecurity landscape of a partner nation. Estonia's e-Governance Academy manages the National Cyber Security Index that provides an overview of every country's cybersecurity maturity and includes primary data sources. These resources are not exhaustive but are meant to be simple guides in helping a Mission begin to understand the partner nation's cybersecurity landscape and how it may affect the portfolio. For additional resources, see Annex IV.

CYBERSECURITY ACTORS

- Who are the primary cyber threat actors related to your environment and programs? (e.g. criminal entities, domestic actors, foreign nation states, businesses, political parties, hacktivists, etc.)
- What stakeholders are engaged in policymaking, advocacy, or programming on cybersecurity? (e.g., civil society organizations, tech companies, government ministries, donors)
- What stakeholders are responsible for monitoring and enforcing cybersecurity threats?
- Is there a national Cyber/Critical Incident Response Team (CIRT), Computer Emergency Response Team (CERT), or a Computer Security Incident Response Team (CSIRT)? Which individuals or organizations are members? What is its mandate?

CURRENT STATE AND IMPACT

- What information is publicly available on the state of cyber threats and trends, particularly through government and private sector analysis and reporting? How might these threats and trends affect your programming?
- Are your programs involved in any activities that may be perceived as politically sensitive (e.g. advocacy for democratic norms, human rights, or anti-corruption initiatives) that may increase the likelihood of attacks and data breaches?
- Do your programs utilize and depend on any hardware or software that is vulnerable to attacks? Have these technologies been designed from the start with security as a priority? Is the software used by partners and beneficiaries licensed and current?
- What cybersecurity policies, regulations, and legislation exist in the partner nation? To what extent are they implemented?
- What, if any, organizations exist that raise awareness of cybersecurity risks? How do they raise awareness? What impact do they have on increasing cybersecurity practices?
- Does higher education offer curricula on cybersecurity? Are these programs adequately prepared for the current and future demand for information security workforce skills?
- What does the competitive landscape look like in terms of cybersecurity providers? (e.g., many vs. few; local vs. international companies)
- Have there been any recent high-profile data breaches or cybersecurity incidents (private or public sector)? At what scale? How were they handled? Was there any communication issued by the government? By the private sector?
- Do institutions or organizations undergo information audits (such as penetration testing) to ensure the validity of cybersecurity strategies and policies in place?
- What cybersecurity measures are in place to protect critical internet infrastructure?[56]
- What is the extent of different actors' (user, business, government) capability to understand and use cybersecurity products and standard practices?
- Do cybersecurity standards limit the growth of tech startups and SMEs?

PERCEPTIONS

- How do different stakeholders (civil society, private sector, government, individuals) perceive the importance of cybersecurity?
- How is the policy, regulatory, and legal environment for cybersecurity perceived by different stakeholders (individuals, private sector, business associations, civil society organizations)?
- What is the perception by different stakeholders (individuals, civil society organizations, private sector) of government capacity to monitor, detect, and react to cybersecurity breaches?
- How do people's concerns around cybersecurity threats affect their online activities?
- To what degree do cybersecurity concerns deter investment in new technologies?

IDENTIFY OPPORTUNITIES AND RISKS

Once the Mission is comfortable with its understanding of the cybersecurity landscape, technical offices can discuss how the programs with digital components are affected by the cybersecurity threats and protective measures. Here are some tips to consider in this discussion:

- For any programs that are politically sensitive or have a strong digital component, expect that the program's digital systems at some point have and/or will come under cyber attacks through technical vulnerabilities or social engineering.
- Identify what digital capabilities and data are most important to program implementation and focus efforts on understanding the technical and human vulnerabilities of these components.
- If significant vulnerabilities exist, work with USAID resources and cybersecurity experts to develop a plan for mitigating threats and risks. Depending on the program, this could include working with partner government agencies to develop new regulations and other policies, engaging with IPs, or working directly with beneficiaries to raise awareness and capacities.
- In all cases, important data should be backed up on a frequent and regular schedule in more than one secure digital location.
- Develop a response plan, working with the actors relevant to the program, for what to do in the event of a successful cyber attack or data loss, including steps to restore lost data, partners you will work with to identify the method of the attack and patch vulnerabilities, and who will represent the program to external and participating stakeholders and explain what happened and how it is being addressed.

SAMPLE INTERVENTIONS

Below is a list of illustrative actions that can be taken when designing programs across sectors. This is not limited to cybersecurity-specific programming, rather all programming that may leverage digital tools or services to advance USAID objectives in a partner country. These considerations are organized into categories covering people, processes, and technologies as key elements of the cybersecurity ecosystem.

PEOPLE

- Build the capacity of USAID Mission staff to understand why cybersecurity and its societal implications are relevant for programs across sectors. This ranges from understanding how geopolitical challenges may manifest themselves through cybersecurity as well as how criminals may take advantage of an increasingly digitized world to find and exploit victims.
- Encourage digital literacy and cyber hygiene training across all programming.
- Build or strengthen a robust pipeline of cybersecurity and technology professionals in the partner country, by working closely with appropriate institutions or with other donors.
- Leverage USAID programming to support the local technology ecosystems, who can then provide local talent to solve local cybersecurity challenges.
- Support the development of cyber-resilient civil society that monitors digital trends in a country, advocates for open,

secure, and interoperable digital systems, and educates the population on cyberthreats and security.

Processes

- Conduct a Digital Ecosystem Country Assessment to understand the digital context of the partner country, including legislation related to cybersecurity or related issues. If resources do not permit for this, conduct a review of legislation in the country of operation to understand how existing laws or policies affect the digital marketplace, including but not limited to cybersecurity or cybercrime legislation. Such a review should also expand cybersecurity-specific laws or policies and include an understanding of the country's position on data storage, data management, and interoperability between networks.

- Build trusted initiatives that encourage local processes or frameworks for non-governmental actors—CSOs, non-governmental organizations, private sector—to share information on observed cybersecurity attacks or trends in the country or region. This will allow for pooling of resources or proactive mitigation.

- Encourage partners to adopt risk-based approaches to cybersecurity, including clear processes to identify, protect, detect, respond to, and recover from cyber attacks. Such processes are resource heavy. They require labor and appropriate technology. USAID staff should consider how their programming can assist USAID partners to strengthen their capacity to follow such processes. This may include facilitating connections between CSOs or other organizations and cybersecurity service providers.

- When designing programs, incorporate lessons learned from existing USAID cybersecurity programming, including, but not limited to, the Cybersecurity for Critical Infrastructure program in Ukraine, the Digital Connectivity and Cybersecurity Program, or Digital APEX.

- Establish a cybersecurity donor coordination group in-country to discuss cyber challenges and opportunities.

- Across USAID programming, encourage information sharing related to cyber-attacks or cybersecurity vulnerabilities. For instance, if a global health program has been a victim of a phishing attack, share that information with other USAID programs operating in the country to help them avoid also becoming victims.

- Leverage USAID programming and resources where available to support partners to conduct compromise assessments of digital assets used to advance USAID programming. Provide or work together with local partners to provide a list of remediation resources if vulnerabilities are identified.

TECHNOLOGY

- Consider reviewing or conducting an assessment of potential risks associated with proposed digital solutions for your sector by an implementing partner or USAID beneficiary or partner.

- Encourage partners to understand the Virtual Private Network (VPN) marketplace, including whether they are legal in a country of operation, before using them. Furthermore, encourage partners to learn who built different VPNs in order to understand whether they may be monitored by foreign agents.

- Encourage the transparent procurement of software and hardware technology assets by USAID partners in-country to prevent or limit the use of pirated digital assets that may be compromised.

ANNEXES

ANNEX I: GLOSSARY

NOTE: This glossary is intended as a comprehensive reference guide for USAID staff. It contains terms not found in the above text.

Term	Definition
5G	5G stands for the fifth generation of cellular network technology. According to a World Bank report, 5G will leverage new wireless technologies and additional spectrum bands to enable not only faster mobile broadband, but also massive Internet of Things (IoT) and mission-critical services. Here is an introduction to 5G and the development context. See Box 9 for more information.
Advanced Persistent Threats (APTs)	According to NIST, APT is an adversary with sophisticated levels of expertise and significant resources, allowing it, through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future. Moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Artificial Intelligence (AI)	According to USAID's Digital Strategy, AI is the science and technology of creating intelligent systems. Machine learning (ML) often enables AI systems, which apply data-derived predictions to automate decisions. While ML focuses on learning and prediction, AI applications often create, plan, or do something in the real world. Automated decisions might be directly implemented (e.g., in robotics) or suggested to a human decision maker (e.g., product recommendations in online shopping). For information on how AI can be used in development, please see Reflecting the Past, Shaping the Future: Making AI work in International Development.
Asset	An entity of value that could take the form of a person, structure, facility, data, information and records, IT systems and resources, material, process, relationships, or reputation (Microsoft Digital Defense Report).
Attack Vectors	Hackers use attack vectors to gain access over a network or a computer. Attacks are done to infect the system with malware or to harvest data. Common attack vectors include man-in-the-middle, drive-by, Structured Query Language (SQL) injection, and zero-day attacks.

Term	Definition
Bots	According to the Center for Internet Security (CIS), "bots are automated applications or scripts designed to perform repetitive tasks without requiring human input." While bots can have safe applications online, they can also be used to "maliciously to distribute spam, conduct distributed DDoS attacks, operate as malware command and control infrastructure, or flood public forums with fraudulent commentary to propagate a specific message" (per CIS). Here is a *Stop, Think, Connect* factsheet on bots and botnets and a factsheet from DHS about social media bots, specifically.
Botnet	According to CIS, "when a collection of multiple bots is controlled by a single source, it is known as a botnet. A botnet is typically used to amplify the capabilities of its component bots and launch large-scale attacks." More information is provided from the *Stop, Think, Connect* campaign.
Breach	Any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential, or unauthorized logical IT perimeter (Microsoft Digital Defense Report).
Censorship	Suppression of communications in any form.
Ciphertext	Data or information in its encrypted form used primarily by cryptology experts. Sometimes referred to as encrypted data (Microsoft Digital Defense Report).
Critical Infrastructure	Describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety (DHS). According to CISA, there are 16 critical infrastructure sectors in the United States.
Cybersecurity	The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. As the Cybersecurity Strategy of the U.S. Department of Homeland Security (DHS) emphasizes: "Cybersecurity is not an end unto itself, and efforts to mitigate cybersecurity risks must also support international commerce, strengthen international security, and foster free expression and innovation."
Cyber Attack	According to NIST, a cyber attack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."
Cybercrime	According to Interpol, cybercrime "refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user."

Term	Definition
Cybercrime-as-a-Service (CaaS)	According to *Info Security Magazine*, CaaS refers to the productizing of malware and the on-demand purchasing and selling of cybercrime services. This means that cybercriminals do not need to create their own malicious code but can buy it online. This makes it significantly easier to access, even to a layperson.
Cyber Insurance	According to Cisco, "cyber insurance is an insurance product designed to help businesses hedge against the potentially devastating effects of cybercrimes such as malware, ransomware, DDoS attacks, or any other method used to compromise a network and sensitive data." Demand for cyber insurance has grown rapidly in recent years.
Cyber Harms	According to Cyber Harms: Concepts, Taxonomy and Measurement, cyber harms are damaging consequences resulting from cyber incidents, which can originate from malicious, accidental, or natural phenomena, manifesting itself within or outside of the internet. They can impact individuals, organizations, or countries.
Cyber Hygiene	The practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.
Cyber Resiliency	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents (NIST).
Cyber Threat	According to NIST's Computer Security Resource Center, a cyber threat is "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability."
Cyber Vulnerability	According to NIST's NIST's Computer Security Resource Center, a cyber vulnerability is "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." See CISA's overview of cyber vulnerabilities for more details.
DarkNet	According to the FBI, the DarkNet is a subset of the deep web. DarkNet content is not indexed and consists of overlaying networks that use the public internet but require unique software, configuration, or authorization to access. This access is predominantly designed to hide the identity of the user. See the FBI's Primer on DarkNet Marketplaces.

Term	Definition
Dark Web	Dark web refers to websites on a DarkNet. The dark web includes pages on servers that cannot be accessed by a search engine (or indeed, a user) without an appropriately permissioned account. Large-scale illegal activities take place on the dark web.
Deep Web	According to the FBI, the deep web is the vast amount of web content on the internet that is available to the general public, but it is harder to find unless you have the exact URL (not indexed for search engines like Google). Examples of deep web sites include sites only accessible by password or gateway software.
Distributed Denial-of-Service (DDoS)	According to CloudFlare, a DDoS attack "is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic." CISA's denial of service attacks factsheet provides a good overview.
Digital Surveillance/ Surveillance Technology	Surveillance technology refers to the use of digital technology to monitor the behavior or movement of people in public and private places. Governments, private companies, and other organizations can use it to target, intimidate, or otherwise influence individuals or groups.
Doxing	The act of gathering, by licit or illicit means, and posting on the internet PII and other sensitive information about an individual, including for example, addresses, dates of birth, social security numbers, telephone numbers, e-mail addresses, credit information, employers, and details regarding the individual's family members.
Encryption	The process of transforming plaintext into ciphertext (Microsoft Digital Defense Report).
Human Error/ Confiscation	Revelation of sensitive material online (social media, forwarded emails) or through confiscation of devices.
Firewall	A capability to limit network traffic between networks and/or information systems (Microsoft Digital Defense Report).
Insecure Mobile Communications	Taps or intercepts of calls, texts, and files sent from a cellular phone.
Insecure Files/Data	Files or data that can be stolen through online or physical action.

Term	Definition
Internet of Things (IoT)	CISA explains IoT as "any object or device that sends and receives data automatically through the internet." Common IoT devices in 2020 include smart doorbells like Nest, fitness trackers like FitBit, and smart home security systems, etc. These devices pose a potential cybersecurity risk because they share a lot of information online and do not necessarily adhere to the highest levels of cybersecurity protections. For additional information, see this CDSE webinar on IoT.
Insider Threat	A person or group of persons within an organization who pose a potential risk through knowingly or unknowingly violating security policies (Microsoft Digital Defense Report).
Kill Chain	Developed by Lockheed Martin, the Cyber Kill Chain is a framework to identify and prevent cyber intrusions. The seven-step model identifies what the adversaries must complete in order to achieve their objective so as to strengthen a cyber analyst's understanding of an adversary's tactics, techniques, and procedures.
Lack of Privacy or Anonymity	The inability to keep online activities or identity from being revealed to others.
Machine Learning (ML)	According to USAID's Digital Strategy, ML is a set of methods that train computers to learn from data, where "learning" generally amounts to the detection of patterns or structures in data. ML approaches begin by finding patterns in a subset of existing data and use them to make predictions for new, unseen data.
Malware	According to CISA, malware is "malicious code that is designed to destroy data" and can "can threaten an organization's access to critical assets and data." For more information, see this FTC video.
Man-in-the-Middle (MITM) Attacks	According to Force Point, an MITM attack "is a form of cyber eavesdropping in which malicious actors insert themselves into a conversation between two parties and intercept data through a compromised but trusted system. The targets are often intellectual property or fiduciary information."
Multi-Factor Authentication (MFA)	According to National Cybersecurity Awareness Month in this how-to guide, MFA is "a security process that requires more than one method of authentication from independent sources to verify the user's identity." The FBI has more information in this video.
Phishing	According to CISA, "phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information." An ODNI factsheet has more information, as does this *Stop, Think, Connect* campaign video.

Term	Definition
Ransomware	According to the *Stop, Think, Connect* campaign, ransomware is "a type of malware that accesses a victim's files, locks and encrypts them, and then demands the victim pay a ransom to get them back." For more information, see videos from the FBI and CDSE, and these factsheets from CISA, National Cybersecurity Alliance, DoJ/DHS/HHS, and the FBI's Cyber Division.
Rootkit	According to CISA, a rootkit is "a piece of software that can be installed and hidden on your computer without your knowledge."
Social Engineering	According to CISA, a social engineering attack is where "an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems." See this FBI video and this ODNI video for more information.
Spear Phishing	According to the National Cybersecurity Alliance, "spear phishing involves highly specialized attacks against specific targets or small groups of targets to collect information or gain access to systems." The FTC has more info here, in this ODNI video, and in this ODNI factsheet.
Spoofing	According to ForcePoint, "spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server."
Spyware	According to Avast, "Spyware is a type of malware that tries to keep itself hidden while it secretly records information and tracks your online activities on your computers or mobile devices. It can monitor and copy everything you enter, upload, download, and store. Some strains of spyware are also capable of activating cameras and microphones to watch and listen to you undetected."
Surface Web (or Clear Web)	According to the FBI, the surface or clear web contains content for the general public that is indexed by traditional search engines (like websites for news, e-commerce, marketing, collaboration, and social networking). It's estimated that only 4 percent of internet content is available on the surface; the remainder is only available on the deep web or darknet.
Threat Variant	New or modified strains of an existing virus or malware program; malware family (Microsoft Digital Defense Report).
Trojan (or Trojan Horse)	According to Norton, a Trojan "is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network."

Term	Definition
Virus	According to CISA, viruses are a type of malware that "have the ability to damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages." More information from Norton can be found here. This FBI video covers anti-virus software, patching, and firewalls.
Virtual Private Network (VPN)	According to the FBI, "A VPN creates a secure tunnel for your data to transit the internet, using a network of private servers... A VPN creates the appearance that your data is coming from the VPN server, not from your device. Therefore, it's harder for an attacker to identify you as the source of the data." See this FBI video for more information.
Watering Hole Attacks	According to the U.K. government's National Cyber Security Centre, a watering hole attack "works by identifying a website that's frequented by users within a targeted organization, or even an entire sector, such as defence, government, or health care. That website is then compromised to enable the distribution of malware."
Zero Day Attack or Exploit	According to FireEye, a zero day exploit is an advanced cyber attack that "happens once [a] flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability." FireEye has an associated video found here.

ANNEX II: CYBER ACTORS AND CYBERCRIME

CYBER ACTORS

"Cyber actors" is an umbrella term for the key players that engage in digital (cyber) activities. Therefore, any government, organization, business, or individual who uses digital technologies to advance their work is considered a cyber actor. The table below describes those actors who can pose a threat to a country's cybersecurity.

Cyber Actor	Description
Nation-State 	Nation-states often have the most advanced and agile tools to leverage cyber space for their foreign policy objectives. Digital technology is also used to create efficiency in government service delivery, including administration or maintenance of critical services.
Nation-State Sponsored Group 	Nation-states sponsor groups of cyber professionals to carry out cyber events, including, but not limited to, cyber attacks, cyber espionage, or disinformation campaigns.
Cybercriminals 	Individuals or organizations committing crime through the use of the internet. Cybercrime is defined as illegal attacks predominantly committed for monetary gain or business espionage, not political or other purposes.[57] Cybercrime constitutes the majority of cyber attacks.
Hacker 	An unauthorized individual who attempts to gain access or actually gains access to a computer network or information system.[58]
Hacktivists 	Individuals or organizations that participate in infiltration and disruption of a network or website to further political or social goals.[59] These are a small proportion of overall cyberattacks.
Cyber Terrorists 	Individuals or organizations who seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, or damage public morale and confidence for political or ideological motivations.[60]
Script Kiddies 	Individuals, typically young or inexperienced hackers, who use computer scripts and programs created by others and accessed online to launch attacks. Their goals are typically achievement, learning, small monetary gains, and showing off to build their reputation.

CYBERCRIME

Currently, sophisticated criminal groups and nation-states commit most cybercrimes, at times working together. Cyber criminal groups are formed explicitly to focus on cybercrime or are developed as a division of transnational criminal syndicates—the same organizations involved in global weapons trading, drug running, money laundering, human trafficking, sexual exploitation, extortion, fraud, and other illicit activities. Nation-states typically commit cybercrime by either teaming with criminal groups or sponsoring proxy groups to act on their behalf, providing them with arm's-length deniability of involvement. Their motives

can range from efforts to try to raise money or to steal intellectual property in order to improve economic competitiveness. North Korea, for example, is believed to be behind the theft of $81 million from a Bangladeshi bank in 2016 by hacking the SWIFT international payments network. The National Counterintelligence and Security Center has flagged China, Russia, and India as the biggest threats for stealing intellectual property from companies.[61]

Both criminal groups and nation-states recognize the high-reward, low-risk opportunity that cyber attacks offer and are investing heavily in building their capabilities. The larger criminal organizations function more like structured, well-resourced multinational companies. They know that digital skills will allow them to commit innovative new forms of theft, and in the case of diversified crime groups, facilitate their other existing activities. They can be very adept at testing new approaches and pivoting away from those that produce poor returns. They also know that by investing in new capabilities and staying ahead of law enforcement, which globally is moving slowly in this space, they can largely operate with impunity. Only a few countries have the means to effectively counter high-level cybercrime operations, and because resources and skills are limited, most governments choose to focus their efforts on national level security threats such as protecting core government systems and critical infrastructure like power grids and telecommunications networks.

The danger of cyber criminals should not be underestimated. Terrorist groups like Al-Qaeda and Daesh, known for their physical attacks with massive death tolls, actually have relatively low cyber capabilities, mostly employing social media for recruitment and propaganda, as well as some low-level hacking. Meanwhile, less well-known, non-state criminal groups with advanced cyber capabilities, such as Shadow Brokers, Anonymous, and some international criminal syndicates, which can conduct multilayer complex attacks and create advanced persistent threats (APTs), historically have had little interest in causing politically motivated physical damage or sparking interstate cyber conflict. However, new trends are likely to increase future threats. Tactics, techniques, and procedures are becoming commoditized and more widely available as a service, making advanced cyber weapons more and more available to less sophisticated actors. For example, script kiddies' actions are fairly innocuous, yet they are gaining access to ever more powerful tools and their numbers are growing quickly as more developing countries with large and underemployed youth populations expand their connectivity.[62] The growing availability of AI and 5G networks will also make it easier for actors looking to exploit digital tools for their objectives, while simultaneously making attribution of a cyber-attack more difficult. Given these dynamics, cyber capabilities of international terrorist groups, cyber criminals, unskilled hackers, or nation-state actors will continue to grow in reach and sophistication.

In addition to highly organized cyber criminal enterprises and cyber terrorist groups, individual hackers or cyber criminals can also commit cybercrimes with pernicious real-life consequences.

One clear-cut example is the rise of cybercrime as a way to perpetuate gender-based violence (GBV) and intimate-partner violence. Online GBV is not new, with the increased adoption and use of digital tools over the past two decades leading to the rapid growth of gender-based online harassment, doxxing, and revenge pornography. However, the use of malware and other hacking tools/cyber weapons to commit acts of GBV is a relatively new phenomenon. For example, stalkerware is "software, made available directly to individuals, that enables a remote user to monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user in a manner that may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence."[63] Stalkerware can track the victim's physical location, SMS messages, phone calls, and internet history—all without the victim's knowledge. While cybercriminal syndicates and cyber terrorist groups may cause greater societal disruption or affect a greater number of victims at one time, malware and other hacking tools can also be deployed at the individual level in an extremely negative and disruptive way.

ANNEX III: ADDITIONAL RESOURCES AND RECOMMENDED READINGS

QUICK READS, RESEARCH, AND THOUGHT LEADERSHIP

- **Center for Global Development**: The Technology and Development Program focuses on the macroeconomic implications of technology change as well as technological applications for specific development challenges.

- **Center for Strategic and International Studies (CSIS)**: The Technology Policy Program provides pragmatic, data-driven analysis, and recommendations on cybersecurity, privacy and surveillance, technology and innovation, and internet governance.

- **Council on Foreign Relations**: The Digital and Cyberspace Policy Program conducts research across several topic areas related to cybersecurity and international relations.

- **EU vs Disinformation**: EU vs Disinfo is the flagship project of the European External Action Service's East StratCom Task Force that was established in 2015 to better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns. The Studies and Reports section includes a range of studies, articles, and reports on the spread of pro-Kremlin disinformation.

- **Freedom House**:

  Technology and Democracy: Focuses on understanding how information and communications technologies have had an impact on democracy globally.

  Freedom on the Net: An annual study of internet freedom around the world.

- **New America**:

  Cybersecurity Initiative: Research across several topic areas related to cybersecurity and international relations.

  Ranking Digital Rights: A non-profit research initiative housed at New America's Open Technology Institute that works to promote freedom of expression and privacy online and assesses private sector companies' commitments and policies based on international human rights standards.

  Securing Digital Dividends: A paper that makes the case for mainstreaming cybersecurity in international development.

- **Politico's Cybersecurity Newsletter**: A weekly newsletter on cybersecurity in policy. Mostly focused on the United States but provides important analysis on international issues as well.

GENERAL CYBERSECURITY AWARENESS

- **The Global Forum on Cyber Expertise (GFCE)**: A global coordinating platform of countries, international organizations, and the private sector used to exchange best practices and expertise in cyber capacity building. The United States is a member of GFCE.

  Cybil is a GFCE-managed knowledge hub of international cyber capacity building, including tools, publications, overview of activities on cyber capacity building globally, upcoming events, and the GFCE Working Group outcomes.

- **International Computer Security Incident Response Teams (CSIRTs)**: Carnegie Mellon University maintains a list of international CSIRTs. A CSIRT with national responsibility (or "National CSIRT") is one that is designated by a country or economy to have specific responsibilities in cyber protection for the country or economy. A National CSIRT can be inside or outside of government but must be specifically recognized by the government as having responsibility in the country or economy.

- **MITRE**: A non-profit organization that works in the public interest across federal, state, and local governments, as well as industry and academia. One of their main competencies is cybersecurity, where through some initiatives they work with national governments to develop cybersecurity strategies or workforce capabilities.

- **National Cybersecurity Alliance (NCSA)**: Through public/private partnerships, NCSA creates and implements education and awareness efforts to empower users at home, work, and school with the information they need to keep themselves, their organizations, their systems, and their sensitive information safe and secure online and encourage a culture of cybersecurity.

  Tips for staying safe online for individuals

  Tips for staying safe online for businesses

  Security awareness videos

  STOP. THINK. CONNECT. Campaign: A global online safety awareness campaign to help all digital citizens stay safer and more secure online. Led by NCSA and the Anti-Phishing Working Group, the campaign was created in partnership with the U.S. government (through DHS) and includes a coalition of private companies, non-profits, and government organizations. Their website contains basic fact sheets, research, and campaigns about various aspects of cybersecurity intended for the general public.

CYBERSECURITY LEGISLATION

- **Data Protection and Privacy Legislation Worldwide**: The United Nations Conference on Trade and Development maintains a database of global cybercrime legislation.

MATURITY MODELS AND INDICES

- **Cybersecurity Capability Maturity Model (C2M2)**: C2M2 is a U.S. Department of Energy program enabling voluntary, consistent measurement of the maturity of an organization's cybersecurity capabilities. The C2M2 focuses on the implementation and management of cybersecurity practices associated with the information technology and operations technology assets and the environments in which they operate. The model can be used to: 1) strengthen organizations' cybersecurity capabilities; 2) enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities; 3) share knowledge, best practices, and relevant references across organizations as a means to improve cybersecurity capabilities; and 4) enable organizations to prioritize actions and investments to improve cybersecurity. The model is publicly available for download.

- **Global Cybersecurity Index**: Managed by the International Telecommunications Union, this index measures the commitment of countries to cybersecurity at a global level. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars—1) legal measures, 2) technical measures, 3) organizational measures, 4) capacity building, and 5) cooperation—and then aggregated into an overall score.

- **The Global Cyber Security Capacity Centre (GSCC) at Oxford University**: A research center focused on efficient and effective global cybersecurity capacity building initiatives. It has created a maturity model through which to review a country's cybersecurity maturity by assessing countries across five dimensions: policy and strategy; culture and society; education, training, and skills; legal and regulatory frameworks; and standards, organizations, and technologies.

  Cybersecurity Maturity Model (CMM): Created by GSCC, the CMM assesses a country's cybersecurity maturity along the five dimensions mentioned above. Each dimension includes specific factors for evaluation. To date, CMM has been deployed in 80 countries, and 110 have been reviewed. GCSSC is seeking to expand the number of countries using CMM through regional collaboration. Currently, GCSSC has two major partnerships: 1) Oceania Cyber Security Center in Australia and 2) the Cybersecurity Capacity Centre for Southern Africa.

- **National Cyber Security Index (NCSI)**: Managed by the e-Governance Academy Foundation in Estonia, this cybersecurity index measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cyber security capacity building. Rankings are based on public evidence, specifically: 1) legal acts, 2) official documents, and 3) official websites.

SECTOR-SPECIFIC RESOURCES

DRG:

- **Atlantic Council**: The Digital Forensics Research Lab operationalizes the study of disinformation by exposing falsehoods and fake news, documenting human rights abuses, and building digital resilience worldwide.

- **Center for Democracy and Technology**: A non-profit organization that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual.

- **CivicSpace.tech**: Funded through USAID's Strengthening Civil Society Globally (SCS Global) Program, CivicSpace.tech was created to help fill knowledge gaps among development practitioners on digital trends and threats around the world. It is intended to equip civil society, governmental, and other actors with information they need to participate in decision-making conversations about technology in development programming and to protect their interests in the quickly changing digital landscape.

- **Digital Self-Defense Meta-Guide**: An extensive compilation of digital security guides and toolkits included based on relevance, practical advice, accessible language, and clear organization that can be put to work both by experts and non-experts. While the project ended in October 2019, the resources are still highly relevant and useful.

- **Electronic Frontier Foundation**: A leading non-profit organization defending civil liberties in the digital world.

Finance:

- **Addressing Cyber Security Risks in Emerging Financial Sectors**: Resources compiled from a November 2019 CGAP workshop that assessed why cybersecurity matters for advancing financial inclusion in emerging and developing countries and discussed how to support the financial sector in addressing and managing cyber risks.

- **Cybersecurity for Financial Inclusion: Framework & Risk Guide**: Developed by the Alliance for Financial Inclusion, this guide includes key principles and best practices to assist regulatory and supervisory authorities in devising tools for the financial sector to deal with cybersecurity risks. The guide is also useful for financial service providers to help them strengthen their cyber-risk management in the provision of financial services that target the last-mile, underserved consumers at the bottom of the pyramid.

Energy:

- **Digitalization and Cybersecurity Webinars** conducted under the Business Innovation Partnership initiative of the Energy Utility Partnership Program.

- National Association of Regulatory Utility Commissioners Publications:

  Black Sea Cybersecurity Strategy Development Guide (2017): This guide was developed to provide information and lessons learned to support Black Sea regulators, and others, in developing their own commissions' cybersecurity strategies. Drawing from experiences and best practices from U.S. state-level regulatory commissions and elsewhere, the document has been designed to cover the important issues and questions that regulators should address as they begin the process of developing their unique cybersecurity strategies.

  Cybersecurity Evaluative Framework for Black Sea Regulators (2017): This evaluative framework is an easy-to-use tool for regulators to evaluate utilities' cybersecurity preparedness. It is designed to provide a structured way for regulators to assess what level of cyber-preparedness utilities have reached and identify areas for improvement.

  The Utility Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards (2020): This guide was initially developed for regulators in Europe and Eurasia to reinforce their knowledge of practical

cybersecurity solutions in the face of ongoing threats within the energy sector. However, the questions of how to evaluate risks, assess mitigation measures, and select standards are relevant for regulators around the world.

Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators (2020): These guidelines were developed to assist regulators in ensuring that investments made in the name of cybersecurity are reasonable, prudent, and effective. They are intended to assist regulators in defining tariffs by establishing a regulatory approach to enhance the cybersecurity stance of their power systems and are based on literature and current practices.

SELECTED BOOKS

- *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* by Shoshana Zuboff
- *The Hacked World Order* by Adam Segal
- *The Perfect Weapon* by David Sanger
- *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* by Andy Greenberg

ANNEX IV: KEY USG CYBERSECURITY ACTORS

DEPARTMENT OF STATE, OFFICE OF THE COORDINATOR FOR CYBER ISSUES

- The State Department leads the U.S. Government's efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.

- The Office of the Coordinator for Cyber Issues (S/CCI) integrates the diplomatic efforts across the full range of international cyber policy issues that affect U.S. foreign policy, national security, human rights, and economic imperatives. S/CCI convenes interagency working groups on a range of cybersecurity issues, as well as regular meetings of State Cyber Officers or those State Foreign Service Officers that cover cyber issues as part of their portfolio. .

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

- The Cybersecurity and Infrastructure Agency (CISA) leads the United States' strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services. CISA works with the federal government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.

- CISA houses the United States Computer Emergency Readiness Team (US-CERT), responsible for analyzing and reducing cyber threats, and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

- CISA manages the Critical Infrastructure Cyber Community (C3) Voluntary Program, an innovative public-private partnership launched in February 2014 to help align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the NIST voluntary Cybersecurity Framework and manage their cyber risks.

DEPARTMENT OF COMMERCE

- **National Institute of Standards and Technology (NIST)** supports U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST's cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the ability to address current and future computer and information security challenges. NIST Cybersecurity Framework (CSF) is the prime tool, developed in partnership with stakeholders, that helps organizations understand their cybersecurity risks

(threats, vulnerabilities, and impacts), how to reduce these risks with customized measures, and respond to and recover from cybersecurity incidents. The CSF is the foundation for operation of systems by U.S. Federal Government agencies and is broadly used by the private sector.

- **National Telecommunications and Information Administration (NTIA)** is the Executive Branch agency principally responsible for advising the President on telecommunications and information policy issues. NTIA cybersecurity focuses on issues such as: 1) addressing cybersecurity concerns related to the IoT, including but not limited to connected devices, patchability, and upgradability; and 2) increasing collaboration between software developers and security researchers to find and patch cybersecurity vulnerabilities across digital tools and services.

DEPARTMENT OF JUSTICE, COMPUTER CRIME, AND INTELLECTUAL PROPERTY SECTION

- The Computer Crime and Intellectual Property Section (CCIPS) implements the DOJ's national strategies in combating computer and intellectual property crimes. This includes preventing, investigating, and prosecuting cybercrimes.

DEPARTMENT OF ENERGY, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC)

- NERC develops and enforces reliability standards, including from the integration of Smart Grid, monitors the bulk power systems, and educates, trains, and certifies industry personnel.

FEDERAL ENERGY REGULATORY COMMISSION (FERC)

- FERC oversees the power grid of the United States, which includes the authority to approve mandatory cybersecurity reliability standards. FERC and NIST together coordinate the development and adoption of smart grid guidelines and standards.

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

- The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. Just as the FBI transformed itself to better address the terrorist threat after the 9/11 attacks, it is undertaking a similar transformation to address the pervasive and evolving cyber threat. This means enhancing the Cyber Division's investigative capacity to sharpen its focus on intrusions into government and private computer networks.

- The FBI's Protected Voices initiative provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations and cybersecurity threats, such as practical how-to video guides.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

- The National Counterintelligence and Security Center (NCSC) is the nation's premier source for counterintelligence and security expertise. Foreign intelligence entities, including foreign governments, corporations, and their proxies, actively target information, assets, and technologies that are vital to both U.S. national security and our global competitiveness. The NCSC is dedicated to raising awareness among government employees and private industry about these foreign intelligence threats, the risks they pose, and the defensive measures necessary for individuals and organizations to safeguard that which has been entrusted to their protection. ODNI plays a primary role in the National Defense Authorization Act (NDAA) Section 889 waiver process for Federal agencies.

- The Know the Risk Raise Your Shield campaign enables the layperson to better understand counterintelligence threats online and provide guidance and tips for protecting the sensitive information, assets, technologies, and networks to which employees have access. Contains a cyber training series, short videos, and travel tips.

ANNEX V: USAID'S FOCUS ON CYBERSECURITY REFLECTS BROADER USG POLICY GOALS

By promoting an open, secure, reliable, and interoperable internet, USAID promotes U.S. values and supports the USG policy goals of national security and economic prosperity. Improved cybersecurity protections within USAID Missions, USAID IPs, and in the countries where USAID works aligns with USG policy documents and frameworks:

- **U.S. National Security Strategy** – "As we bolster our scientific and technological base, we will make cybersecurity a top priority, strengthening our capability, readiness, and resilience in cyberspace. We will elevate cybersecurity as an imperative across the government."

- **U.S. National Cyber Strategy** – "The United States is committed to ensuring the protection and promotion of an open, interoperable, reliable, and secure internet that represents and safeguards the online exercise of human rights and fundamental freedoms—such as freedom of expression, association, religion, and peaceful assembly."

- **National Strategy for Counterterrorism** – "We will incorporate two of the most potent tools in the information environment: cyber operations and strategic communications. These tools are an integral part of our counterterrorism activities, and we will continue to incorporate them when appropriate to maximize their effects."

- **2018–2022 State-USAID Joint Strategic Plan** – Mandates international cooperation to "secure an open, interoperable, reliable, and stable cyberspace and strengthen the capacity of the United States and partner nations to detect, deter, rapidly mitigate, and respond to international cyber threats and incidents."

- **Cyberspace Solarium Commission Report** – "We must get faster and smarter, improving the government's ability to organize concurrent, continuous, and collaborative efforts to build resilience, respond to cyber threats, and preserve military options that signal a capability and willingness to impose costs on adversaries."

ENDNOTES

1 Hackett, Robert. "Ransomware attack on a hospital may be first ever to cause a death." Fortune.com. September 18, 2020. https://fortune.com/2020/09/18/ransomware-police-investigating-hospital-cyber-attack-death/.

2 Chi, Leisha. "Philippines elections hack 'leaks voter data'." BBC.co.uk. April 11, 2016. https://www.bbc.com/news/technology-36013713.

3 Baraniuk, Chris. "Millions of Mexican voter records 'were accessible online'." BBC.co.uk. April 25, 2016. https://www.bbc.com/news/technology-36128745.

4 "US Embassy Condemns Cyber Attack on Ministry of Health, Lugar Lab." Agenda.ge, September 4, 2020. https://agenda.ge/en/news/2020/2734.

5 California's recently passed data privacy law seeks to regulate this industry: Lazarus, David. "Column: Shadowy data brokers make the most of their invisibility cloak." November 5, 2019. https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

6 D. L. Pipkin, Information security. Prentice Hall PTR, 2000; E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures. Springer, 2010, pp. 25–44.

7 Abomhara, Mohamed and Geir M. Køien. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility. January 2015. https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4#sec2.2.1.

8 Ibid.

9 ITU. "Measuring digital development: Facts and figures 2020." International Telecommunication Union. 2020. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx#:~:text=ITU's%20Measuring%20digital%20development%3A%20Facts,wide%20urban%2Drural%20connectivity%20gap.

10 Brook, Chris. "What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More." Digital Guardian. October 6, 2020. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more#:~:text=Cyber%20hygiene%20is%20a%20reference,could%20be%20stolen%20or%20corrupted.

11 NIST. "Password Guidance from NIST." NIST. September 5, 2017. https://www.nist.gov/video/password-guidance-nist-0.

12 Adelmann, Frank, et al. "Cyber Risk and Financial Stability: It's a Small World After All." IMF. December 7, 2020. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622.

13 Interpol. "COVID-19 Cybercrime Analysis Report - August 2020." Interpol. August 4, 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

14 Mungadze, Samuel. "Life Healthcare Group hit by cyber attack amid COVID-19." IT Web, June 9, 2020.

15 Eva Ignatuschtschenko, Taylor Roberts, and Paul Cornish, "Cyber Harm: Concepts, Taxonomy and Measurement." SSRN Electronic Journal (January 2016).

16 Ibid.

17 "Life Healthcare expects R2.3-billion COVID-19 knock." News24. November 10, 2020.

18 Council of Europe. "Information Disorder." https://www.coe.int/en/web/freedom-expression/information-disorder.

19 Bradshaw, Samantha, and Philip N. Howard. "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation." Computational Propaganda Research Project. Oxford Internet Institute, Oxford University, September 2019.

20 The 2018 DRG BAA "Advancing Integrity in Media (AIM)" demonstrates USAID's recognition of this trend: "Given the expanding scope and shifting nature of the problem with technological advances and potential innovation in terms of the tools and techniques for disinformation and the threat they pose to democracy, and given the limits on USAID's knowledge of effective development interventions to combat these tools, USAID seeks to develop strategies and tactics that will be dynamic and adaptable to different contexts and technological advancements, and respectful of the essential norms necessary for informed political participation."

21 Flynn, Paul. "What Brexit should have taught us about voter manipulation." The Guardian April 17, 2017. https://www.theguardian.com/commentisfree/2017/apr/17/brexit-voter-manipulation-eu-referendum-social-media.

22 Cerulus, Laurens. "How Ukraine became a test bed for cyberweaponry." Politico, February 20, 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

23 Frankel, Sheer. "Facebook to Remove Misinformation That Leads to Violence." The New York Times, July 18, 2018. https://www.nytimes.com/2018/07/18/technology/facebook-to-remove-misinformation-that-leads-to-violence.html.

24 Arce, Alberto. "In frightened Mexico town, a mob kills 2 young pollsters." San Diego Tribune, October 22, 2015. https://www.sandiegouniontribune.com/sdut-in-frightened-mexico-town-a-mob-kills-2-young-2015oct22-story.html.

25 Guidance for implementing partners on embedding cybersecurity in USAID-funded programs is forthcoming in collaboration with M/OAA.

26 KPMG. "Digital Trust." KPMG. 2015. https://assets.kpmg/content/dam/kpmg/pdf/2015/12/digital-trust.pdf.

27 USAID Digital Strategy 2020-2024.

28 CISA. Critical Infrastructure Sectors. (Last updated March 24, 2020). https://www.cisa.gov/critical-infrastructure-sectors.

29 Chellel, Kit. "The Hacker Who Took Down a Country." Bloomberg Businessweek, December 20, 2019. https://www.bloomberg.com/news/features/2019-12-20/spiderman-hacker-daniel-kaye-took-down-liberia-s-internet#:~:text=The%20Hacker%20Who%20Took%20Down,tough%20but%20corporate%20espionage%20easy.

30 GSMA. "How 5G is Changing the Global Mobile Landscape." GSMA.com. October 2, 2019. https://www.gsma.com/membership/resources/how-5g-is-changing-the-global-mobile-landscape/.

31 Youyou, Wu, Michal Kosinski, and David Stillwell. "Computer-Based Personality Judgments Are More Accurate than Those Made by Humans." Proceedings of the National Academy of Sciences 112, no. 4 (January 27, 2015): 1036–40.

32 Carvin, Andy. "DFRLab uncovers Tunisia-based political influence operation on Facebook." Atlantic Council, June 2020. https://medium.com/dfrlab/dfrlab-uncovers-tunisia-based-political-influence-operation-on-facebook-8c4d16b90744.

33 Reuters. "Vietnam jails three more activists in crackdown on Facebook posts." Reuters, November 28, 2019. https://www.reuters.com/article/us-vietnam-security-trials/vietnam-jails-three-more-activists-in-crackdown-on-facebook-posts-idUSKBN1Y20J3.

34 De Yonge, John. "EY CEO Imperative Study 2019: For CEOs, Are the Days of Sidelining Global Challenges Numbered?" Ernst & Young, July 8, 2019. https://www.ey.com/en_us/growth/ceo-imperative-global-challenges.

35 Botting, Alexander and Daniel Vazquez. On Firm Foundations: Cybersecurity and Digital Development Strategies Post COVID-19. MarketLinks, July 7, 2020. https://www.marketlinks.org/post/firm-foundations-cybersecurity-and-digital-development-strategies-post-covid-19.

36 RBS. "When the Going Gets Tough, Cybercrime Gets Going." Risk Based Security (RBS), March 30, 2020. https://www.riskbasedsecurity.com/2020/03/30/when-the-going-gets-tough-cybercrime-gets-going/.

37 CISA. Financial Services Sector.

38 Kagan, Julia. "Financial Technology – Fintech." Investopedia, updated on Aug 28, 2020. https://www.investopedia.com/terms/f/fintech.asp; BCBS. "Cyber-Resilience: Range of Practices." December 2018. https://www.bis.org/bcbs/publ/d454.htm.

39 Reaves, Bradley, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. 2015. "Mo(Bile) Money, Mo(Bile) Problems: Analysis of Branchless Banking Applications in the Developing World." In Proceedings of the 24th USENIX Security Symposium, 17. Washington, DC.

40 Microsoft Asia News Center. "Fear of cyberattacks slows down the progress of digital transformation in financial services companies in Asia Pacific." Microsoft, November 15, 2018. https://news.microsoft.com/apac/2018/11/15/fear-of-cyberattacks-slows-down-the-progress-of-digital-transformation-in-financial-services-companies-in-asia-pacific/.

41 Friday, Catherine. "Cyber threats to education sector jeopardise valuable research." Ernst and Young, January 22, 2020. https://www.ey.com/en_au/risk/cyber-security-risks-education-trends-and-cybersecurity-program-implementation-strategy.

42 RSI Security. "Cybersecurity in Education: What you Need to Know." RSI Security. November 12, 2019. https://blog.rsisecurity.com/cyber-security-in-education-what-you-need-to-know/#:~:text=Common%20Educational%20Cyber%20Attacks&text=If%20a%20school%20is%20known,other%20tools%20used%20while%20teaching.

43 Muncaster, Phil. "Over 1,000 U.S. Schools Hit by Ransomware in 2019." Infosecurity Group, December 18, 2019. https://www.infosecurity-magazine.com/news/over-1000-us-schools-hit-by/.

44 Emsisoft Malware Lab. "The State of Ransomware in the U.S.: Report and Statistics 2019." Emsisoft, December 12, 2019. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

45 Fripp, Charlie. "Hacker defaces University of Limpopo website again." HyperText, July 18, 2016. https://www.htxt.co.za/2016/07/18/university-website-defaced-hacker/.

46 Siemens and the Ponemon Institute. "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?" October 2019. https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1599074232/siemens-cybersecurity.pdf.

47 Liberty International Underwriters. "Cyber: The Overlooked Environmental Threat." Risk & Insurance, August 3, 2016. https://riskandinsurance.com/cyber-overlooked-environmental-threat/.

48 ITWeb. "City Power Hit by Ransomware Attack." IT Web, July 25, 2019. https://www.itweb.co.za/content/GxwQDq1AnVWqlPVo.

49 Shahbaz, Adrian. "Freedom on the Net 2018." Freedom House, November 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

50 Feldstein, Steven. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, September 2019. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

51 Newly available and inexpensive satellite imagery from private start-ups like Planet is already being used to do this. Data from precision agriculture will serve to further bolster analysis and provide ever more accurate assessments.

52 Mutschler, Pete. "Threats to Precision Agriculture." 2018 Public-Private Analytic Exchange Program. ASIS International, 2018. https://www.dhs.gov/sites/default/files/publications/2018 AEP_Threats_to_Precision_Agriculture.pdf.

53 The WannaCry virus was linked to North Korean government-affiliated hackers.

54 Mungadze, Samuel. "Life Healthcare Group hit by cyber attack amid COVID-19." IT Web, June 9, 2020. https://www.itweb.co.za/content/JBwErvnBK4av6Db2.

55 Much of this section is based on analysis provided in the following report by the World Economic Forum. Its findings are strongly consistent with numerous other reports, including from the Cyberspace Solarium Commission and various prominent cyber firms. For more information, see: Creese, et al. "Cybersecurity, Emerging Technology and Systemic Risk." Future Series. World Economic Forum, November 2020.

56 Critical internet infrastructure includes the internet backbone networks, DNS servers, Internet Exchange Points (IXPs), and top-level domain (TLD) registries and registrars.

57 Council of Europe. Convention on Cybercrime. November 23, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

58 NIST. "Hacker." NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/hacker.

59 CISA. "Cyber Threat Source Descriptions." Cybersecurity and Infrastructure Security Agency (CISA). https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions#nat.

60 Ibid.

61 NCSC Newsroom. "National Counterintelligence and Security Center Launches Campaign to Help Private Industry Guard Against Threats from Nation State Actors." Office of the Director of National Security, January 7, 2019. https://www.dni.gov/index.php/ncsc-newsroom/item/1938-national-counterintelligence-and-security-center-launches-campaign-to-help-private-industry-guard-against-threats-from-nation-state-actors.

62 According to CISA, script kiddies are a not-insignificant portion of these. Cybercrime rookies will graduate to higher ranks and create new challenges in the coming years.

63 Stopstalkerware.org. "What is Stalkerware?" Coalition Against Stalkerware. Accessed January 2021. https://stopstalkerware.org/what-is-stalkerware/.

FOR MORE INFORMATION ► digitaldevelopment@usaid.gov

USAID
FROM THE AMERICAN PEOPLE