USAID
FROM THE AMERICAN PEOPLE

Cybersecurity

DEMOCRACY, HUMAN RIGHTS, AND GOVERNANCE (DRG)

Photo credit: Maxime Fossat for USAID

Why Does Cybersecurity Matter for DRG?

DRG programs frequently work on politically sensitive topics, including elections, human rights, and information resilience. USAID's partners and beneficiaries—including human rights defenders, independent media, and civil society—are often targeted because of their sensitive work. Authoritarian governments and other malign actors regularly deploy digital surveillance techniques and cyber attacks to monitor and harm key DRG players, thus cybersecurity capacity building is quickly becoming a critical element of DRG programming. Even in open, democratic spaces, cybersecurity is crucial to effective DRG programming. Cyber attacks against elections technologies, government databases, and critical infrastructure can erode public trust in USAID's government partners.

What is cybersecurity, and why does it matter for international development?

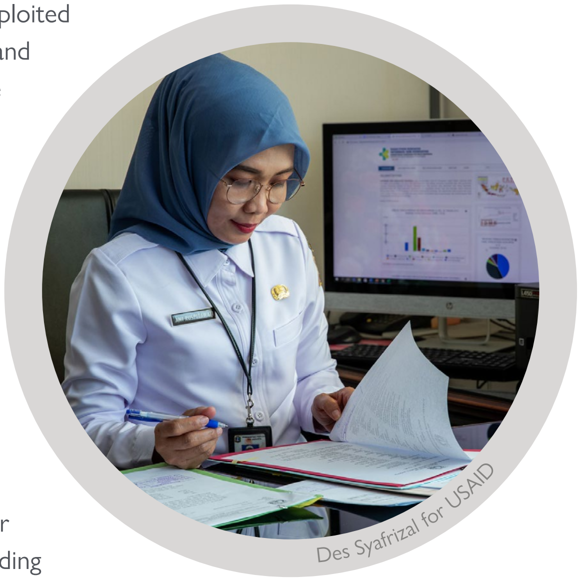
As noted in USAID's Cybersecurity Primer, USAID defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation." As USAID partner countries further their digital transformation and continue to adopt new digital tools and systems, cyber risks and vulnerabilities proliferate. Cybersecurity failures pose material threats to USAID partner countries and undermine partner country government legitimacy. USAID must protect its digital investments by ensuring that its digital programming addresses cyber harms and includes cybersecurity mitigation measures.

The Ukraine Responsive and Accountable Governance Program builds the cybersecurity capacity of Ukraine's Central Elections Commission

The Ukraine Responsive and Accountable Governance Program (URAP) promotes citizen-centered elections and political processes in Ukraine. To strengthen the cybersecurity capacity of Ukraine's Central Elections Commission (CEC), URAP first conducted an electoral cybersecurity needs assessment. With the findings of this assessment, it collaborated with government and cybersecurity actors to facilitate upgrades to Ukraine's electoral cybersecurity infrastructure. URAP subsequently trained more than 600 people involved in Ukrainian elections—including election commissioners, political party representatives, Parliament, and civil society members—on key cyber hygiene topics. As a result, the CEC successfully staved off cyber attacks during Ukraine's 2019 presidential and parliamentary elections, which built the public's confidence in the integrity of these elections.

Cybersecurity Trends in DRG

The proliferation of online personal data creates an opening for malign actors to run mis- and disinformation campaigns. The use of social media and messaging apps in many low- to middle-income countries (LMICs) has generated massive amounts of online personal data. Authoritarian governments and other malign actors can exploit these detailed user profiles to identify and exacerbate social divisions, create social and political instability, and influence the opinions of voters. LMICs with weak institutions and low social cohesion are particularly vulnerable to disinformation campaigns. These coordinated efforts—enabled by technology—seek to influence or exploit the opinions and actions of a group of people. In Burma, malicious actors exploited social media algorithms to spread propaganda in the wake of the 2021 coup and disinformation that led to serious human rights abuses against members of the Rohingya minority ethnic group. Though not all of these campaigns have a cyber element, so-called "hack-and-leak operations" allow malicious actors to control narratives by hacking networks, exfiltrating data, and using that data in information operations. We have yet to witness the impact of emerging technologies like artificial intelligence (AI) large language models on mis- and disinformation. Some AI companies have already forecast the risk of AI being used to develop disinformation narratives.


Des Syafrizal for USAID

Journalists, human rights defenders (HRDs), and civil society organizations (CSOs) are particularly vulnerable to cyber attacks and surveillance technology. Cyber attacks and cyber threats against members of the media and prominent members of civil society are increasing. The number of calls to AccessNow's Digital Security Helpline for civil society members (including journalists and HRDs) increased from 152 in 2013 to more than 2,000 in 2020. This steep increase demonstrates an urgent demand for cybersecurity services among these groups. Cybersecurity company Cloudflare estimated that media and journalism websites protected under its Project Galileo initiative experienced around 53 million cyber attacks per day between August 2020 and March 2021, five times higher than the number of cyber attacks during this period in the previous year. These attacks not only imperil the free flow of information by knocking websites offline, but they also pose a serious threat to the physical security of activists, journalists, and civil society leaders by revealing their personal information, such as their addresses. The rapid growth of surveillance technology enables malign actors or non-permissive governments to target and intimidate civil society members. Most prominently, the NSO Group's Pegasus spyware has targeted at least 450 people—including activists and journalists—in at least 18 countries.

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. It typically includes digital monitoring via cameras with AI-enabled facial recognition software; software covertly installed on mobile phones; monitoring of social media and messaging apps; and tracking of digital financial transactions.

Cyber attacks threaten the integrity of elections. Countries around the world are increasingly using digital tools—such as digital voter rolls and election results, biometric voter registration, and electronic voting machines—to conduct and publicize the results of their elections. This new technology can make elections more efficient and hasten the tabulation of final results, but it also creates new cyber risks that threaten the foundations of democracy. The Cybersecurity and Infrastructure Security Agency (CISA) breaks cyber threats against election infrastructure into three categories: confidentiality attacks (such as breaching online voter registration information), integrity attacks (such as electronically altering vote totals), and availability attacks (such as taking vote tabulation websites offline). This categorization demonstrates the myriad ways in which electoral processes are vulnerable to attack. To illustrate the severity of the issue, 2020 research from the Australian Strategic Policy Institute's International Cyber Policy Center found more than 25 instances of state-backed cyber operations in elections and referenda from 2010 through 2020, including in USAID partner countries such as Cambodia, Colombia, Indonesia, Malaysia, and Ukraine.

USAID's DRG team is investing in cybersecurity capacity building resources. USAID's DRG team is working actively to counter cyber threats across its portfolio. Cybersecurity is increasingly built into DRG policy documents, technical briefs, and tools, such as USAID's DRG Strategy, the Digital Government Model, and the Electoral Assessment Framework. USAID's Democratic Elections and Political Processes (DEPP) Team recently supported the International Foundation for Electoral Systems (IFES) in developing a five-part electoral cybersecurity briefing series, which includes the following publications: Electoral Cybersecurity Primer; Reference Document on Electoral Cybersecurity; Cybersecurity of Voter Registration; Cybersecurity of Election Results Management; and an Electoral Cybersecurity Donor Program Development Guide.

At the programming level, USAID is working directly with partner countries like Ukraine and Timor-Leste and with other partner organizations to draft cybersecurity policies and strengthen cybersecurity capabilities. The Agency provides robust support to USAID partner governments to shore up their election-related cyber defenses, including providing technical assistance to election management bodies on cyber hygiene and supporting post-election cybersecurity assessments. A key component of USAID's new Defending Democratic Elections Fund is fostering solutions that address electoral cybersecurity. On the civil society side, USAID is rapidly increasing its cybersecurity support to journalists, CSOs, and HRDs and other activists. Projects like Digital Apex and Greater Internet Freedom (GIF) are working directly with these groups to enhance their digital safety and build their cybersecurity capabilities. GIF developed a toolkit for journalists on digital hygiene best practices and evading digital surveillance.

Riaz Jahanpour for USAID / Digital Development Communications

Key Considerations for Cybersecurity Activities in DRG

- Understand partner country policies, strategies, and regulations around cybersecurity, data privacy, elections, and governance. Digital Ecosystem Country Assessments (DECAs) are one mechanism for better understanding these dynamics. If your Mission does not have a DECA, consider commissioning one.
- Identify areas of alignment with existing USAID or USG strategies, partnerships, and initiatives.
- Engage with interagency partners on local cybersecurity needs and existing USG programming.
- Embed cybersecurity considerations, resources, responsibilities, and management tools into every DRG project and activity.
- Anticipate that any DRG program or activity's digital systems will be subject to cyber attacks and develop a response plan to meet the possibility of a successful cyber attack or data loss.
- Review or conduct an assessment of potential risks associated with proposed digital solutions on DRG programs or activities.
- Support the development of a cyber-resilient civil society that monitors digital trends in a given country; advocates for open, secure, and interoperable digital systems; and educates the population on cyberthreats and security.
- Consider partnering with Digital APEX and leveraging GIF's resources and networks to improve the cybersecurity capabilities and resilience of human rights groups, activists, and other USAID civil society partners.

TO LEARN MORE about cybersecurity and USAID programming, please reach out to USAID's Cybersecurity Team at cybersecurity.itr@usaid.gov and the DRG digital team ddi.drg_gov@usaid.gov.