USAID
FROM THE AMERICAN PEOPLE

Cybersecurity
CONFLICT PREVENTION AND STABILIZATION

Photo Credit: ACCESS Development Services

Why does cybersecurity matter for conflict prevention and stabilization?

Cybersecurity and conflict prevention and stabilization are entwined in several ways. Most notably, as conflict increasingly takes place in the digital realm instead of on the physical battlefield, malicious cyber actors are waging more frequent cyber attacks to hack and disable critical infrastructure. Meanwhile, new cyber trends and technologies—including malware-as-a-service—have made it easier for nation-states, non-state actors, and other combatants to wage cyber attacks with fewer resources and at a lower cost. The highly destructive nature of these cyber attacks on critical digital infrastructure and information systems poses a direct threat to the security of a nation's civilians, civil society organizations, independent media, and government partners.

Beyond thwarting or preventing direct cyber attacks, strong and effective cybersecurity procedures are also crucial for conflict prevention and stabilization at a broader societal level. Cyber attacks against critical infrastructure and information ecosystems can damage citizens' confidence in public institutions, leading to instability and the erosion of social cohesion. And while many cyber attacks to date have been staged between states, necessitating robust national-level cybersecurity measures to protect against foreign cyberattacks, cybersecurity is also critical for internal stability and the mitigation of civil conflict. Authoritarian regimes can use digital technologies to suppress and surveil perceived enemies of the state within their own populations, including civil society groups, activists, and journalists. Furthermore, actors may perpetrate data theft from insecure datastreams that allow them to craft disinformation campaigns or spread hate speech designed to incite civil unrest and violence.

As conflict prevention and stabilization is closely linked to successful operations in the humanitarian sector, please also see the Humanitarian Assistance cybersecurity sectoral brief for additional relevant information.

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. Because 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.

Cybersecurity trends affecting conflict prevention and stabilization

Cyber attacks are increasingly aiding and displacing traditional conflict. Modern cyber warfare typically takes two forms: standalone cyber warfare attacks and hybrid warfare, in which cyber attacks are part of a larger physical conflict. One prominent early example of standalone cyber warfare occurred in 2007, when Russia launched cyber attacks (but no physical attacks) against Estonian government websites, banks, and other targets in retaliation for the Estonian government's relocation of a Soviet-era statue—the first known case of state-on-state cyber warfare. However, in the years since, Russia has increasingly waged hybrid warfare. To give itself a tactical advantage and weaken its opponents, Russia incorporated cyber tactics to supplement its physical attacks in Georgia in 2008, in Ukraine in 2014 to annex Crimea, and in its 2022 invasion of Ukraine. Cyber attacks are growing in prominence in conflicts in other regions as well. In the Middle East, Iran and Israel have engaged in a tit-for-tat cyber conflict for years, and a cyber group thought to be directed by Hezbollah's cyber unit has targeted Iran's other ideological enemies including Egypt, Jordan, the Palestinian Authority, the United Kingdom, and the United States since 2012.

Non-state actors are increasingly deploying cyber attacks. As cyber attack operations have a relatively low barrier to entry, cyber conflicts are no longer limited to use by nation-states: non-state actors are now leveraging cyber attacks to cause major damage. These range from online-only politically motivated hacktivist collectives to groups affiliated with major terrorist organizations like ISIS. For example, Egyptian hacktivists targeted Ethiopian government websites in 2020 as online fury grew over Ethiopia's construction of a new dam over the Nile River. Politically and economically motivated cyber criminal groups have also waded into international politics and conflict. For example, the prominent ransomware group Conti declared its support for Russia's 2022 invasion of Ukraine and threatened retaliatory attacks against U.S. targets should the United States strike against Russian infrastructure. In other cases, the lines between state and non-state actors are blurred. A hacktivist collective called CyberBerkut—which has carried out attacks against Ukrainian and NATO-related targets—is suspected to be affiliated with Russian military intelligence. Similarly, Ukraine's IT Army, while not formally part of Ukraine's military infrastructure, carries out cyber attacks in collaboration with the Ukrainian government. The enmeshment of state and non-state actors in the cyber realm will continue to have profound implications for current and future conflicts.

Photo Credit: Digital Empowerment Foundation (DEF)

Cyber attacks can have wide-reaching impacts on conflict dynamics outside of their immediate objectives. Even when cyber attackers are not ideologically motivated, their attacks can impact local conflict dynamics by reducing confidence in public institutions and eroding social cohesion. One recent study in the Journal of Information Technology & Politics suggests that cyber attacks can quantifiably diminish public confidence in government, leading citizens to not trust authorities to keep them safe. This study found that "intensifying cyber attacks can cause severe social damage," even when that is not the intended outcome of the attack. However, the study also found that individuals who became more familiar with the specifics of a cyber attack did not lose as much confidence in their governments. This suggests that USAID partner countries can counter the negative effects of cyber attacks by increasing transparency and awareness of cybersecurity before and after attacks and boosting support for independent media that cover the attacks. Cyber attacks are also used in conjunction with information manipulation campaigns to further erode public confidence in government and stoke fear. For example, a month before Russia's invasion of Ukraine, a cyber attack brought down multiple Ukrainian government websites, replacing them with a screen warning Ukrainian citizens that their personal information was compromised and to "be afraid and wait for the worst."

Cybercrime intersects with conflict in a number of ways—it can flourish in conflict settings, and in some cases it finances both state and non-state belligerents. While cyber threat actors are usually thought of as either cyber criminal groups or state actors with geopolitical goals, the lines between these groups are often blurred in conflict settings. For example, both the People's Republic of China (PRC) and Russia are known to recruit cybercrime groups to support their political goals; in 2022, the U.S. Secret Service reported that hackers linked to the PRC government stole COVID-19 relief funds, while in Ukraine, suspected Russian state-sponsored cyber attacks match the same techniques previously used by a known ransomware group, suggesting that experienced cybercriminals are now working directly with Russian security forces to target Ukraine. At the same time, Russia's war in Ukraine has severely disrupted the international cybercrime marketplace, fracturing once-powerful eastern European ransomware outfits as various actors choose sides in the conflict. Finally, both state and non-state groups have used cybercrime to fund their military operations. Laundering donations through cryptocurrency has become a tool for terrorist financing, and North Korea has used the ransomware operations of state-sponsored Lazarus Group cybercrime group to fund its nuclear weapons program.

Use of digital repression tools—including spyware—and information manipulation campaigns can increase social instability. The use of digital repression tools—including Internet shutdowns, firewalls that limit Internet browsing activity, punitive cyber laws, and spyware like the Pegasus software—can heavily restrict freedom of expression and the activities of the digital press. In addition, these tools can potentially escalate conflicts and lead to greater social instability. According to an analysis of governmental digital repression in over a dozen African countries, while authoritarian leaders might justify the use of such tools as imperative to safety and security, evidence suggests that "digital repression serves as an amplifier rather than mitigator of [political instability]." Tracking governments' use of digital repression tools, tactics, and legal instruments is increasingly essential to conflict prevention and stabilization efforts. Importantly, digital repression is not just a characteristic of U.S. adversaries—U.S. allies and friends are also known to use tools of digital repression in ways that can impact stability and citizens' rights. Similarly, information manipulation by malicious actors can greatly increase social instability by spreading unfounded rumors about political, ethnic, or religious groups. In Burma, a coordinated information manipulation campaign by the country's military precipitated a genocide against the Rohingya ethnic group.

Theoretical norms around cyber conflict prevention are slowly emerging. As calls grow for a new "digital Geneva Convention," key international organizations—especially the United Nations—are shaping new norms for cyber conflict. In 2021, representatives from 150 UN countries endorsed a cybersecurity report that laid out initial norms and recommendations for international cybersecurity standards. This report complements the European Union's development of a Cyber Diplomacy Toolbox in 2017 and ongoing work by other regional organizations like the African Union to enact cyber capacity-building measures. However, it is not yet clear if these proposed norms will translate into adopted or enforced standards.

The peacekeeping community increasingly views the key goals of cyber-specific peacekeeping programs and measures to be the mitigation and de-escalation of cyber conflicts. Because norms governing the use of cyber actions in conflict have only recently begun to emerge, the cyber peacekeeping field is very new. Despite its nascent status, the mitigation and de-escalation of cyber conflicts is a key focus area for professionals in this field. They endeavor to disincentivize potential malicious cyber actors and to build the cyber resilience of civilians, public institutions, and other potential targets so that they are prepared for—and can withstand the effects of—such attacks. According to a proposal from the NYU Center on International Cooperation, "cyber peacekeepers" will eventually be necessary to "[prevent] cyber attacks, minimize the damage to infrastructure, rebuild infrastructure after conflict, and increase trust and security in cyberspace." Emerging cyber peacekeeping models include the UN's Digital Blue Helmets (DBH) initiative, which seeks to coordinate the UN's work on cybersecurity and the Cyber Peace Institute's CyberPeace Builders Program, which links humanitarian non-governmental organizations with free cybersecurity support.

Key considerations for cybersecurity activities in conflict prevention and stabilization

The following considerations present entry points for incorporating cybersecurity into conflict prevention and stabilization programming:

» Understand partner country policies, strategies, laws, and regulations around cybersecurity, data privacy, communications infrastructure, independent media, and digitalization.

  ○ USAID Missions and Bureaus need to understand the cybersecurity ecosystems they are operating in *before* designing and implementing new activities. Digital Ecosystem Country Assessments (DECAs) are one mechanism for better understanding these dynamics. If your Mission does not already have a DECA, consider commissioning one.

  ○ When planning or conducting your DECA, be sure to read the Conflict and Violence Addendum, which guides Missions to incorporate conflict, violence, and peacebuilding considerations into DECA development.

» Embed cybersecurity considerations, resources, responsibility designations, and management tools into every USAID-funded conflict prevention and stabilization program and project.

» Coordinate with other donors and implementing partners to identify areas of alignment in cybersecurity and conflict prevention and stabilization.

» Consider contracting a local cybersecurity or digital security firm to identify local risks, threats, and mitigation efforts and build the capacity and resilience of local partners.

» Identify cyber tools and resources that can be localized and used by partners, including the Cyber Peace Institute's CyberPeace Builders Program.

» Encourage the development of local processes or frameworks for non-governmental actors—e.g., civil society organizations, non-governmental organizations, and private-sector entities—to share information on observed cyber attacks or cyber warfare activities in a country or region. This will allow for pooling of resources and proactive cyber attack mitigation.

  ○ For example, USAID has partnered with nonprofit collective NetHope and cloud management software provider Okta to develop an Information Sharing and Analysis Center (ISAC) for the humanitarian sector. ISACs, which provide a platform for organizations within a sector to share information on and coordinate collective responses to cyber threats, are one model for encouraging information sharing on cybersecurity.

» Have a clear and agreed-upon plan for how a program will respond to a cyber attack or significant data breach or compromise. Recognizing that the leakage of data in a conflict context can be especially dangerous for the communities where USAID works, USAID program managers should consider including cybersecurity check-ins during regular meetings with implementing partners and grantees.

» Consult with USAID's Cybersecurity Team (cybersecurity.itr@usaid.gov) to learn more about how to incorporate cybersecurity into your programming.

» Contact the Office of Civilian Military Cooperation (cps.cmc.Task@usaid.gov) to be connected with USAID staff at Department of Defense combatant commands or the Pentagon. Information and analytics produced by these entities can shed light on trends in malicious cyber operations affecting different regions, and give USAID insights to coordinate capacity-building efforts with host country partners.

FOR FURTHER INSIGHTS into the cybersecurity in USAID CPS programming, please reach out to USAID's Cybersecurity Team at cybersecurity.itr@usaid.gov.