USAID
FROM THE AMERICAN PEOPLE

DIGITAL ECOSYSTEM COUNTRY ASSESSMENT

Conflict and Violence Addendum

BRIEFER

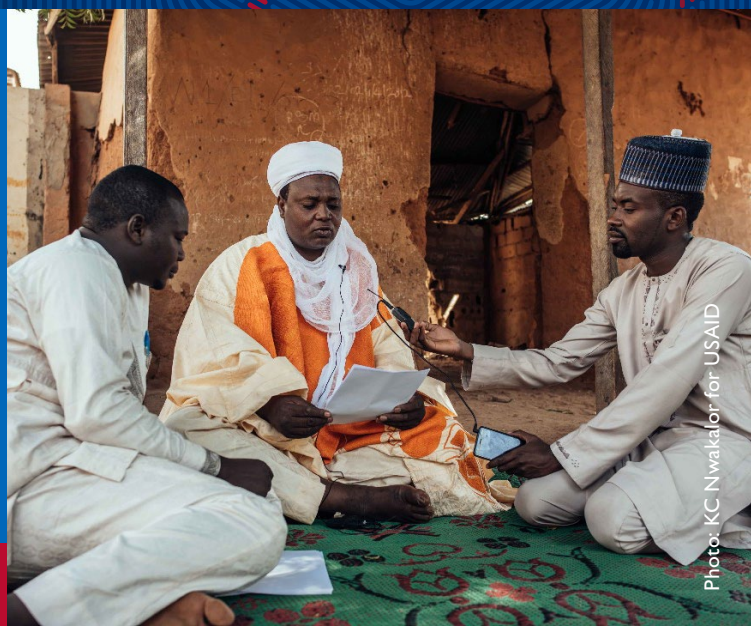

Photo: KC Nwakalor for USAID

The Conflict and Violence Addendum is designed to assist teams conducting Digital Ecosystem Country Assessments to incorporate conflict, violence, and peacebuilding considerations in their data collection, assessment, and recommendations for Missions. This Implementation Guide highlights the dynamic interactions between digital ecosystems and conflict, violence, and peacebuilding, and introduces analytical priorities covered by the Addendum.

While digital technologies have opened new avenues for conflict and violence prevention, they are also rapidly transforming the spaces in which conflicts are fought, and amplifying existing vulnerabilities and risks related to conflict and violence. These technologies have enabled new and scaling trends of repression, manipulation, surveillance, polarization, criminal or extremist expansion, gender-based violence, and the undermining of social cohesion and stability. Key dilemmas for DECA teams to investigate include:

- **Disruption of Prosocial Norms**. Digital devices and digital platforms have been shown to influence how people seek connection and resources, how they develop relationships and form communities, and how they see themselves in relation to others. In particular, digital technologies are capable of shifting individual behaviors that interact with feelings of trust, fear, belonging, and threat.
  - » While digital technologies have been used to support and enhance prosocial norms and values across the globe (social inclusion, financial assistance, gender equality, etc.), these have also contributed to the formation or escalation of extremist or hateful norms that disrupt social cohesion, or outrightly validate violent behavior.
  - » Digital risks and harms are strongly influenced by vulnerabilities and fractures already present in society offline, which are then compounded in unprotected or unsafe digital environments.

- **Surveillance and Repression**. The profit models, governance structures, and vulnerabilities of many prominent digital platforms are dramatically impacting conflict dynamics and rising insecurities. Platforms that offer users free access do so in exchange for collecting or extracting private information about users - their identities, preferences, beliefs, patterns, and more. Conflict actors can surveil and exploit the massive quantity of vulnerable personal data collected and stored through individuals' use of digital technologies. Personal data is increasingly used by conflict power-brokers to prey upon or proactively manipulate individual and group incentives and interests and achieve desired outcomes.
- **Information Control and Manipulation**. Digital platforms – which both fill gaps left by eroded trust in traditional institutions and sources of information, and infiltrate and influence mainstream media and narratives – have contributed to splintering and siloing of information, trust, and decision-making across contexts.
  - » Misinformation, disinformation, and hate speech is shared across digital platforms, where siloed information networks can create multiple, parallel "facts," narratives, and realities. The potential online echo-chamber effects of information-sharing can contribute to narratives of exclusion or deprivation, amplify perceptions of threat and vulnerability, increase the emotional salience of conflict, and importantly, influence off-line interactions. Where competing, irreconcilable narratives exist in society, there can be increased risk of conflict and violence.
  - » Digital media can magnify trigger events by quickly raising mass awareness of events or issues capable of mobilizing action. Digital media also enables remote users to influence on-the-ground events, and volatile environments are often ripe for information manipulation, contestation, and control. In addition to contributing to the escalation of triggers and transitional moments, research points to the role of ICTs in directly triggering and facilitating offline violence in contexts across the globe. Interacting within a constellation of offline and online context dynamics, digital media platforms are distinctly capable of amplifying and normalizing unverified, hateful, dangerous speech in fragile contexts.
- **Exclusion, Deprivation, and Grievances**. Digital development and associated resources can create new grievances when demands for access or control are not met, or can inflame existing narratives of grievance where digitally disadvantaged communities already experience other deprivations in society. Digital divides due to access issues or digital illiteracy can also contribute to existing societal divisions, deprivations, and exclusions. As digital technologies have become a critical – and sometimes primary – means for service provision and information management, digital infrastructure and access have become both an object and a driver of cooperation, competition, and conflict. These deprivations – deemed by UN Deputy Secretary General Amina Mohammed as the 'new face of inequality' – can enforce narratives of relative deprivation and frustrated expectations of groups who do not see themselves as benefiting fairly from country advancement.
- **Resilience**. Digital ecosystems can contribute to societal resiliencies when: Digital Infrastructure is interoperable, well managed and maintained, accessible, and well-protected; Digital Society, Rights, and Governance are created and upheld around the primacy of citizen security and protection; and Digital Economies provide opportunities and pathways for diversified and inclusive economic development.
  - » Digital literacy equips individuals and groups to access, manage, understand, integrate, communicate with, and evaluate digital technologies safely and appropriately for participation in economic, social, and political life. Digital literacy works to maximize the potential for digital development to reap equitable and sustainable results, and helps to mitigate the risks that digital technologies introduce or exacerbate; most prominently, risks pertaining to privacy, security, and information manipulation.

FRAMING QUESTIONS FOR RESEARCH ON DIGITAL ECOSYSTEMS, CONFLICT, AND VIOLENCE

- **General**. How are state or non-state actors using digital technologies to repress or control groups or deny access to services? What groups are targeted by online abuse, harassment, violence, or surveillance? Where? Who are the perpetrators?
- **Patterns of Inclusion/Exclusion**. How does the digital ecosystem reflect or reinforce patterns of inclusion or exclusion between groups or segments of society?
- **Patterns of Social Cohesion or Fragmentation**. How does the digital ecosystem reflect or reinforce patterns of social cohesion or fragmentation? How are digital technologies used to divide groups, spread hate, or to target or attack specific groups? How are they used for peacebuilding, dialogue, or civil society capacity building?
- **Effective and Legitimate Governance of the Digital Ecosystem**. How is delivery of digital services (government services, private services, public goods services) managed? To what extent is delivery and management equitable, effective, and legitimate – or corrupt? To what extent are digital government systems respecting individual rights pertaining to privacy and security?
- **Access to Free Flowing, Accurate Information**. What are the trusted sources of information used by different groups to understand conflicts or political issues? What information silos or polarized narratives exist? What, if any, digital technologies are being used to spread mid-dis/malinformation? How and to whom?
- **Shocks and Stresses**. How does the digital ecosystem help or harm the state and society's ability to effectively manage the impacts of man-made and natural shocks and stresses?
- **Vulnerability and Resilience to Conflict and Violence**. How do actions in the digital ecosystem impact the safety and well-being of individuals and groups? Are digital technologies utilized for criminal or extremist ends? How can the digital ecosystem protect individuals and groups from the adverse effects of conflict and violence?