



USAID
FROM THE AMERICAN PEOPLE



Photo: KC Nwakalor for USAID

DIGITAL ECOSYSTEM COUNTRY ASSESSMENT

Conflict and Violence Addendum



ACKNOWLEDGEMENTS

The Conflict and Violence Addendum was authored by Nicole Patierno, with notable technical contributions from Laura Sigelmann, Amy Malessa, and Craig Jolley.

Special thanks to Craig Jolley and Samantha Chen for their management and valuable insights. Additional thanks to colleagues from across the Bureau for Conflict Prevention and Stabilization; the Digital Sector Council; the Innovation, Technology, and Research Hub; the Center for Democracy, Human Rights, and Governance; and other operating units for reviews. Their contributions substantially improved and informed the final Addendum.

This publication was produced for the United States Agency for International Development by Digital Frontiers, with special thanks to Carlos Saavedra, and Priya Sethi.





Introduction

EXECUTIVE SUMMARY

The purpose of this document is to assist teams conducting [Digital Ecosystem Country Assessments](#) (DECAs) to incorporate conflict, violence, and peacebuilding considerations in their data collection, assessment, and recommendations for USAID Missions.

This guide addresses:

- How conflict and violence impact digital ecosystems;
- How digital ecosystems shape conflict and peace dynamics;
- How to analyze intersections between conflict, violence, peace, and digital ecosystems;
- Conflict-sensitive considerations for DECA assessment teams, and;
- What questions DECA teams can incorporate into data collection to address these considerations

BACKGROUND

The rapid development and adoption of digital technology are transforming industries, governments, economies, and societies. The global—although unequal—proliferation of digital technologies effectively means that digital systems are becoming more inherent for people and communities, particularly how they form networks and interact with each other and their environment.

Under the banner of USAID's [Digital Strategy](#), the Bureau for Development, Democracy, and Innovation, Innovation, Technology, and Research Hub, Technology Division (DDI/ITR/T) launched an innovative [framework](#) to assess country-level digital ecosystems, representing the 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. The Digital Ecosystem Framework investigates the complex, interactive dynamics across three pillars: digital infrastructure and adoption; digital society, rights, and governance; and the digital economy. Digital ecosystems impact—and are impacted by—overarching country environments, including the conflict and violence dynamics in country environments.

ABOUT THE CONFLICT, VIOLENCE, AND PEACE ADDENDUM TO THE DECA

This document presents core considerations for analyzing conflict, violence, and peace dynamics across the DECA's three pillars, and provides critical examples of digital risks and opportunities in conflict and crisis environments.

INTENDED AUDIENCE

This document is primarily designed for use by DECA Research Teams and for USAID Mission staff involved in commissioning DECA research. DECA Research Teams should review this Addendum **after** familiarizing themselves with the DECA Toolkit. This guide is designed to assist users in identifying where digital ecosystems intersect with conflict and violence in a given country or region, and where digital development provides opportunities to advance peace and security. The Addendum can also be used by USAID staff working in conflict and violence-affected environments, to better understand current trends and pressing considerations at the nexus of digital development, conflict, and violence.

HOW THIS DOCUMENT IS ORGANIZED



Section 1

Conflict and Violence Prevention and the DECA

Provides DECA Teams with a background on the ways in which conflict, violence, and peace dynamics impact the digital ecosystem, as well as ways in which the digital ecosystem can influence patterns of conflict, violence, and peace.



Section 2

Digital Ecosystem Across the Violence and Conflict Assessment Framework

Familiarizes DECA Teams with USAID's approach to analyzing conflict and violence, including key considerations and connections to the digital ecosystem.



Section 3

Considerations for Conducting DECA in Conflict and Violence-affected Environments


Highlights conflict sensitivity considerations for DECA planners and research teams to employ when designing and conducting assessments in conflict and violence-affected settings.



SECTION 1:

Conflict and Violence Prevention and the DECA





This section is intended to provide DECA planners and assessment teams with an understanding of USAID’s approaches to violence and conflict prevention and mitigation, and to highlight the dynamic interactions between digital ecosystems and conflict, violence, and peacebuilding.

Nearly 80 percent of countries where USAID operates have experienced significant violence, conflict, or humanitarian crisis during the past decade.¹ In 2019, the number of active armed conflicts reached its [highest point](#) since 1946, and the number of intrastate conflicts has steadily risen since 2010. Beyond the increasing prevalence of armed conflicts,² global violence³ is also on the rise. Casualties resulting from non-combat violence (including homicide, terrorism, domestic abuse, gender-based violence, disappearances, and kidnapping) outpace deaths associated with armed conflict by well over a [five-to-one margin](#). Beyond the direct threats that conflict and violence pose to human safety and well-being, these dynamics are considered ‘development in reverse,’ and capable of undoing and jeopardizing development investments across all sectors.

Societies that experience conflict, violence, and instability are often characterized by patterns of social exclusion, social fragmentation, and inequitable resource management due to ineffective and/or illegitimate governance. These issues are often compounded by corruption and inability to manage shocks or stresses.

USAID has dedicated strategies, policies, and programming to prevent conflict and violence and promote peace in the complex environments where we work. USAID’s conflict prevention efforts seek to interrupt pathways to the outbreak, escalation, and recurrence of violence and conflict and promote peaceful societies. This is achieved by addressing the underlying drivers of conflict, and working to strengthen factors that mitigate the likelihood, magnitude, and effects of conflict and violence.

[Leading conflict prevention research](#) identifies several structural prevention factors which enable societies to peacefully manage conflict and instability. These structural prevention factors include social cohesion and cooperation across groups, acceptance of the rights of others, inclusive economic and political regimes, diversified economies with equitable opportunity to generate high income, and a well-functioning government. USAID’s approaches to building peace take a variety of forms, but ultimately work to strengthen the legitimacy, inclusiveness, and effectiveness of institutions, build social cohesion and reconciliation between conflicting social groups, and support the ability of communities to manage conflict and the threat of violence through peaceful means.

This research also highlights the potential for digital technologies to support these structural prevention factors, particularly when digital ecosystems are used responsibly for effective service delivery or to help information flow horizontally between citizens. However, despite its potential as a force for empowerment and equality,

1 Most countries in which USAID works exhibit a significant degree of fragility: roughly 20 percent are in acute crisis, 20 percent are either recovering from or prone to crisis, and 40 percent experience or are at risk of smaller-scale shocks and stresses such as communal violence and rampant crime. [Responsible Development: A Note on Conflict Sensitivity from USAID’s Center for Conflict and Violence Prevention \(CVP\)](#).

2 **Armed Conflict:** An umbrella term for the systematic use of violence between two or more organized armed groups (i.e., any criminal cartel, army, militia, or other military organization, whether or not it is state-sponsored, excluding any group assembled solely for nonviolent political association). There are four primary types of armed conflict: (1) international armed conflict, (2) intrastate armed conflict/internationalized intrastate armed conflict, (3) criminal armed conflict, and (4) non-state armed conflict. Under the World Health Organization’s conceptualization of violence, Armed Conflict is a form of collective violence that is motivated by political, economic, and social drives.

3 **Violence:** The intentional use of physical force or power, threatened or actual, against another person or against a group or community that results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation. Krug, E., Mercy, J., Dahlberg, L., and Zwi, A. (2002) [“The World Report on Violence and Health”](#). The World Health Organization.

digitalization has also 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.

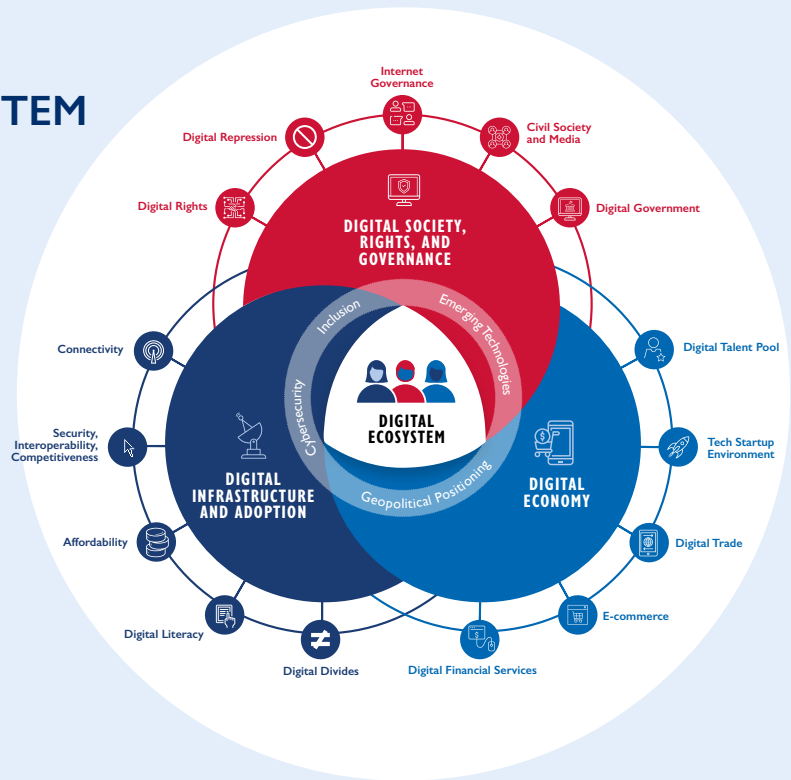
DECA planners and research teams can meaningfully assist USAID Missions to understand the risks associated with digital technologies, and to identify innovative digital pathways to more effective and equitable service delivery, and more peaceful, just, and inclusive societies. The following section introduces USAID’s approach to conflict and violence assessment and highlights key conflict, violence, and peace dynamics across the digital ecosystem.

FIGURE 1: Conflict, Violence, and Peace Dynamics in the Digital Ecosystem

CONFLICT, VIOLENCE, AND PEACE DYNAMICS IN THE DIGITAL ECOSYSTEM

KEY CONFLICT AND VIOLENCE CONSIDERATIONS

- Inclusion versus exclusion of individuals and groups in society
- Social cohesion versus fragmentation and polarization between groups
- Illegitimate, ineffective, or repressive governance and resource management
- Shocks and stresses (man-made and natural)
- Individual vulnerabilities and pathways to conflict and violence



KEY CONFLICT AND VIOLENCE CONSIDERATIONS IN EACH DIGITAL ECOSYSTEM PILLAR

Digital Infrastructure and Adoption:

- Destruction of digital infrastructure and impacts of insecurity
- Inequitable digital development by geography or group
- Digital divides and patterns of marginalization along identity groups
- Lack of digital literacy and vulnerability to digital harm and exploitation
- Exploitation of available digital infrastructure to advance interests (recruit, promote narratives, mobilize, secure resources)
- Conflict and disaster early warning systems and access to information

Digital Society, Rights, & Governance:

- Digital repression (surveillance censorship, social manipulation, internet shutdowns, and targeted persecution of online users)
- Mis-, dis-, and hate speech and mobilization for violence
- Political, social, and economic polarization
- Legal and institutional protections of rights against online harm (cybercrime, cyber-bullying, technology-facilitated gender-based violence, etc.)
- Access to online services and support networks
- Use of digital platforms for civic participation and peaceful dispute resolution
- Robust and protected data landscape for evidence-based policy that advances peace and security

Digital Economy:

- Patterns of access or exclusion to digital financial services
- Use of digital market platforms for illicit economic activity

SECTION 2:

Digital Ecosystems across the Violence and Conflict Assessment Framework



This section is organized according to the Violence and Conflict Assessment Framework (VCAF) diagnostic pillars and elevates analytical considerations for understanding the connections between country context, conflict and violence dynamics, and the digital ecosystem.

To understand the causes and consequences of conflict and identify entry points for peacebuilding programming, USAID has launched an updated Violence and Conflict Assessment (VCA) framework. The ultimate purpose of the conflict assessment is to improve the effectiveness of USAID development and humanitarian assistance by providing Missions with a clear picture of 1) how and where their interventions interact with conflict and violence dynamics in order to adapt their programming, and 2) how a Mission’s development interventions and approaches can most effectively prevent, manage, and mitigate conflict and violence.

Where Missions have conducted a conflict assessment or violence and conflict assessment, DECA Research Teams should review the assessment as part of their preparation. However, not all Missions will have an up-to-date assessment. This section highlights how the various components of the framework can support DECA research to identify and understand dynamics of violence, conflict, and peace across the digital ecosystem.

FIGURE 2: Violence and Conflict Diagnostic Framework

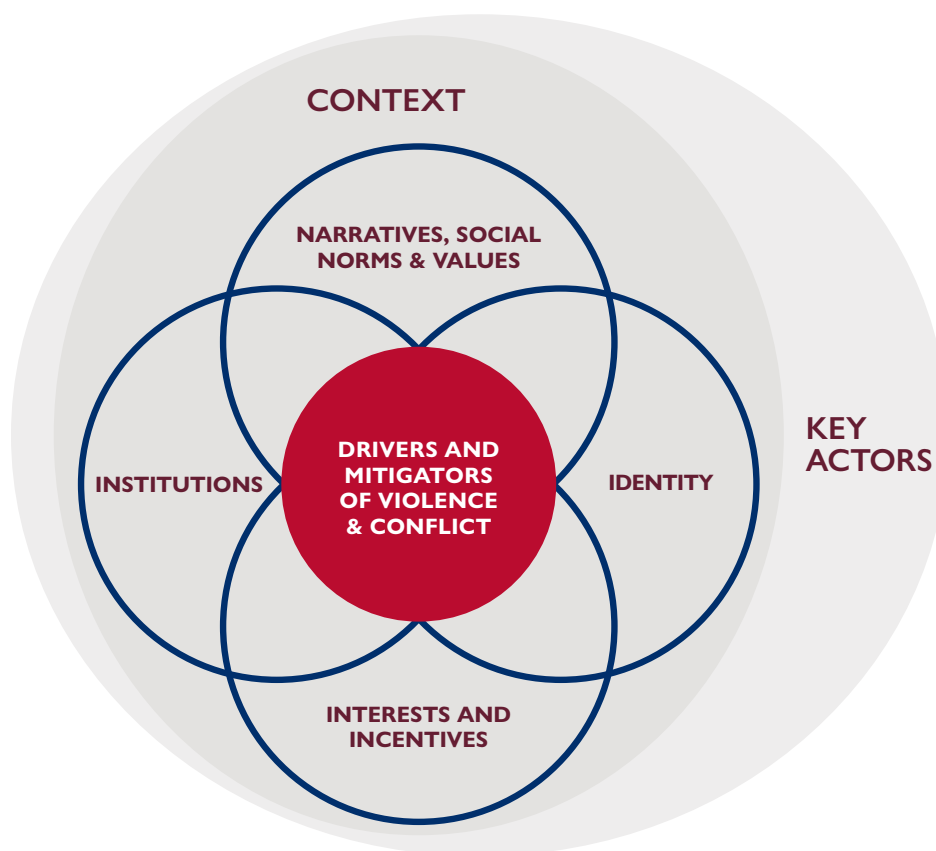


FIGURE 3: Overview of VCAF Framing and DECA Priority Questions

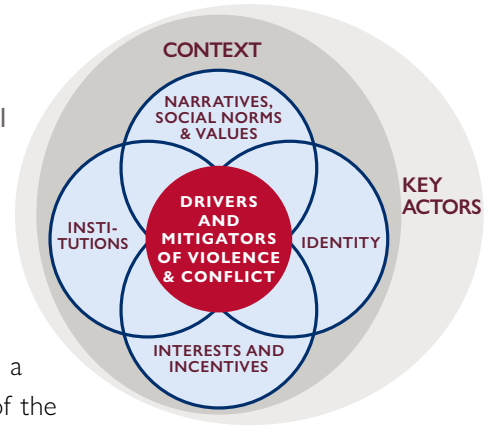
Violence and Conflict Assessment Framing	Considerations for the DECA Team
<p>CONTEXT</p> <p>Factors that may play a role in shaping conflict and violence dynamics, but that are “givens” in the context, changing slowly or not at all.</p>	<ul style="list-style-type: none"> • Are there historic or ongoing cases of armed conflict or outbreaks of violence? Between whom? • Have past conflicts destroyed or damaged digital infrastructure? Is digital infrastructure inaccessible or nonexistent due to insecurity? • To what degree is telecommunication infrastructure used for political or social control? • Do digital divides follow patterns of exclusion of groups that are party to existing social conflicts or active violence?
<p>IDENTITIES</p> <p>Salient markers of similarity, affinity, or distinction among groups of people.</p>	<ul style="list-style-type: none"> • How do people organize themselves in society? What are the salient characteristics that groups identify with? • Are these identities represented in the digital ecosystem? How? • Are certain identities more prone to being targets of digital harm and/or repression, or exclusion from digital services? • What are existing and emergent patterns of technology-facilitated gender-based violence?
<p>INTERESTS & INCENTIVES</p> <p>Motivations for engaging in violence or conflict for economic, political, or social gain.</p> <p>The decision is often a calculus, with people assessing complex and overlapping risks and opportunities (negative and positive incentives).</p>	<ul style="list-style-type: none"> • Is there active competition and contestation around resources? • Are there ideological or resource-based motivations driving actions in the information environment? • Is the digital ecosystem being used for contestation or the pursuit of a groups' interests? Recruitment? Illicit economies? Organized criminal activity? Electoral control?

Violence and Conflict Assessment Framing	Considerations for the DECA Team
<p>NARRATIVES, SOCIAL NORMS, & VALUES</p> <p>Narratives: The stories that we tell and are offered to us (by institutions, media, etc.) to make meaning of our lives and condition.</p> <p>Social norms: Guide behavior and perceptions of others within societies and dictate how we behave to fit in.</p> <p>Values: Represent social standards for what is considered good, important, or worthwhile.</p>	<ul style="list-style-type: none"> • What issues or grievances commonly characterize or cause online discussions/debates/campaigns? • What narratives are different groups seeking to advance in the information environment? • Are these narratives being shaped by misinformation, disinformation, and hate speech? How are these narratives impacting levels of social cohesion, intergroup dynamics, or violence within the country? • How is information and communications technology (ICT) playing a role in how narratives are shaped? • Are digital norms contributing to violence against or vulnerability of any groups?
<p>INSTITUTIONS</p> <p>Formal or informal rules and practices governing human interaction.</p> <p>These include social and political structures, laws, policies, organizations, and other mechanisms for shaping human behavior.</p>	<ul style="list-style-type: none"> • What institutions play a role in shaping narratives? Do any exert disproportionate or total control of media influence? • What institutions are involved in promoting or implementing cybersecurity or content moderation? (Cybercrimes units, legislation, civil society organizations, private sector ICT and social media companies, etc.) • What legal infrastructure exists, particularly around protections against online harm? What mechanisms are available for reporting and remediation for privacy or security breaches, or censorship? • Are there conflict or disaster early warning systems? Who runs them and how do they work?
<p>DRIVERS OF CONFLICT AND VIOLENCE</p> <p>Interactions between institutions and identities that threaten individuals' and groups' ability to meet their needs or achieve their interests or influence their assessment of incentives for participating in violence or conflict.</p> <p>In social conflict, grievances occur when institutions behave ineffectively and/or illegitimately; leading to exclusion, elitism, corruption, unmet expectations, and consistently unmet needs.</p>	<ul style="list-style-type: none"> • Are groups excluded from the digital ecosystem or access to services based on identities? • What patterns of digital exclusion (literacy, access to digital markets, connectivity, education services) exist? • What patterns of social fragmentation exist online (hate speech, attacks, threats)? • Is the state using digital technology, tools, and governance to repress or control groups within society or deny access to justice or services? • How does the digital ecosystem influence perceptions of incentives and disincentives for participating in violence?

Violence and Conflict Assessment Framing	Considerations for the DECA Team
<p>MITIGATING FACTORS AND RESILIENCE TO CONFLICT & VIOLENCE</p> <p>Mitigating factors help prevent groups and individuals from turning to violence to meet their objectives.</p> <p>These factors occur as a result of interactions between institutions and identity groups; they are not always normatively positive.</p> <p>Sources of resilience to conflict and violence reduce the vulnerability of individuals and groups to the harmful effects of conflict and violence.</p>	<ul style="list-style-type: none"> • Are there legitimate and effective protections against digital harm? What actors play a role in promoting protections or accountability? • What institutions or organizations are engaged in digital literacy and/or media literacy efforts? • To what measure is digital infrastructure, economy, and digital society participatory, inclusive, transparent, and accountable? • Are actors using digital technology to improve government accountability? To monitor and document atrocities or acts of violence? • Is digital technology contributing to improved access to justice, civic participation, or service delivery? • Is the digital ecosystem enabling increased access to support networks for victims of online or offline harms? • What enterprises, organizations, or platforms exist that identify trends around hate speech, and/or risk factors and early warning signs for extremism? • To what extent do digital government platforms and services incorporate mechanisms for participatory service delivery (feedback loops)?
<p>KEY ACTORS (MOBILIZERS, ENABLERS, PERPETRATORS, & TARGETED GROUPS)</p> <p>Individuals or groups that have the potential to influence outcomes in conflict, violence, or peace, whether as mobilizers, enablers, perpetrators, or targeted groups.</p> <p>Actors are mobilizers if they have the means (resources) and motivations (interests) to recruit or galvanize action, but they may also play more supporting, but still influential, roles.</p>	<ul style="list-style-type: none"> • What stakeholders are looking to mitigate the use of technology for polarization, discrimination, harassment, violence, and/or conflict? • How is social media being used by conflict or pro-peace actors? Is it a medium for misinformation, disinformation, and hate speech? Are conflict actors using digital forums for advancing their interests, targeting groups, or mobilizing support? • What groups are targeted by online abuse, harassment, or surveillance? Who are the perpetrators? • What groups are targeted for offline violence due to online narratives (including those that are misinformation, disinformation, and hate speech)? • How are state, non-state, or geopolitical actors interacting with the digital ecosystem? What modes of repression exist and who is using them?
<p>TRAJECTORIES (TRENDS, TRIGGERS, WINDOWS OF OPPORTUNITY, & TRANSITIONAL MOMENTS)</p> <p>Possible alternative futures for a country and their potential impact on conflict and violence</p>	<ul style="list-style-type: none"> • What triggers and transitions is the country facing in the short to mid-term? • What are patterns of misinformation, disinformation, and hate speech during transitional moments (e.g., disinformation around elections)? • What are trends in media usage across groups? Is there evidence of increasing or eroding trust in institutions? Between groups?

CONTEXT

Context refers to the ‘given’ factors in an environment; physical and geographical characteristics, history, socio-economic and demographic characteristics, and existing institutions, as well as a history of conflict or violence. Contextual factors change slowly or not at all. While no single contextual factor is causal to conflict outbreak, certain contextual factors increase the risk for conflict.

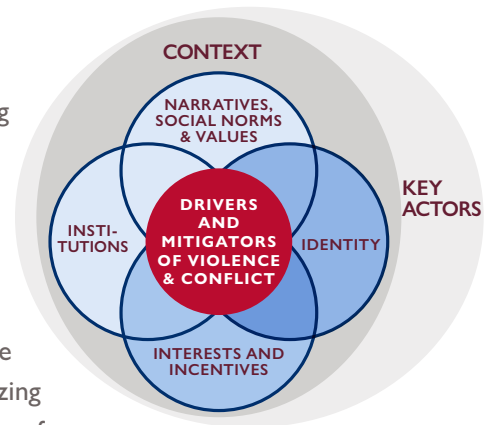


DECA Considerations For the purpose of the DECA Assessment, a country’s established digital infrastructure should be understood as part of the country’s context. In addition:

- DECA teams should be aware of conflict histories, what groups have historically been involved in conflict or engaged in violence, and whether there are current manifestations of historic conflicts.
- DECA teams should seek to identify to what extent violence may have damaged the country’s digital infrastructure, or where conflict and violence prevent free access and mobility. Teams should consider what, if any, parts of the country have less state presence and what areas are unreachable due to insecurity.

IDENTITIES, INTERESTS, AND INCENTIVES

Identities are salient, dynamic markers of similarity, affinity, or distinction among groups of people. Aspects of individual identities may be chosen, born into, or imputed, and may be stable or shifting. All individuals have multiple identities that impact an individual’s lived experience. Identity exists and is shaped at the individual, communal, group, and institutional levels. As identities become markers of similarity, distinction, or affinity to others, identities strongly influence ingroup and outgroup dynamics. Identities become more or less salient depending on the context; in certain conditions, identity can turn from a relatively neutral organizing principle into a powerful mechanism for enabling or even mobilizing violence. These often include identities that are political, geographic, cultural, religious, ethnic, and gendered, or age-, ability- or other affinity-related.



Individual and group **interests** reflect their underlying core needs, wants, fears, or concerns. **Incentives** refer to the real or perceived rewards attached to decision-making. Interests and incentives are often constructed through thoughtful (rational or intuitive) calculations of risk and rewards. Interests and incentives can be complex and overlapping across a range of economic, political, and psychosocial factors. In conflict and violence-affected contexts, people may engage in violence to amass wealth or political power, or to support or protect the basic needs of their family and community. Taken together, interests and incentives inform individual or group motivations for engaging in violence or conflict for economic, political, or social gain.

DECA Considerations Digital ecosystems intersect with identity formation, as well as with individual and group interests and incentives, in ways that alter and even drive conflict and violence.

- 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, and ultimately [impact identity construction](#). Technologies that are replacing or rapidly changing social and economic interactions not only impact identity formation, but are also altering incentive structures, and changing traditional inter-group exposure and interests.
- Digital media⁴ can encourage [selective exposure](#), [homogeneous echo-chambers](#), confirmation bias, and [hyper-sensory](#) environments. These components have been shown to reduce users' [capacity to evaluate information](#), harden ingroup and outgroup perceptions, and impact empathy development and emotional regulation.
- For-profit digital platforms are often [algorithmically designed](#) to promote emotive engagement in order to capture more users and spread more content. This profit model has contributed to the spread of extreme and polarizing information, as well as new patterns of engagement, and network formation. In conflict and violence affected environments—where certain group identities may be more salient—digital technologies can harmfully exacerbate in-group belonging and favoritism and out-group opposition. These environments present particular risks, where polarization can be escalated and stoked into violent conflict.
- 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. DECA Teams should seek to understand what groups are using technologies across the digital ecosystem in this way and to what end.
- **Digital Economy Spotlight:** Digital marketplaces can impact interests and incentives associated with participation in violence, creating opportunities for violent and criminal elements to extort and abuse individuals and groups and to also generate revenue.

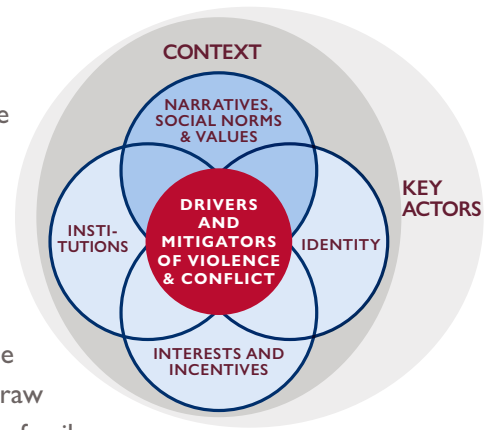
ONLINE-OFFLINE DYNAMICS

The relationship between online and offline interactions are dynamic and interconnected. Digital users bring digital goods (financial resources, information, social networks, skills) back to their in-person interactions with family, friends, and other peer networks, which both influence and are influenced by digital environments. Likewise, the relationship between online and offline violence is interlinked. **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.**

⁴ Digital media is defined as the media content and associated metadata exchanged through web-based information and communication technologies to enable the exchange of information, goods, or services; such as social media, messaging apps, search engines, news aggregators, websites, streaming services and mobile applications.

SOCIAL NORMS, VALUES, AND NARRATIVES

Social norms can be [defined](#) as “the mutual expectations within a group about the appropriate way to behave.” Social norms guide individual and group behavior by suggesting what group members do in a given situation, what they expect others to do, and how they anticipate others will react to a certain behavior. There are often powerful incentives for complying with norms, including the threat of marginalization and even violence, as well as rewards of social acceptance. Norms may be widely shared by people within a group or society, or may be deeply contested and shape fault lines across which societies polarize. Norms are powerful because they draw upon people’s deep-seated human desire to belong within social groups, especially in fragile environments where uncertainty and insecurity prevail and social connections are key to survival.



Similarly, **values** represent standards of what is or is not considered good, important, or worthwhile. Values are often transmitted by both formal and informal social institutions, including families, religious groups, and schools, as well as media and public culture. Healthy social norms and values, such as those that support rule of law, social mobility, freedom of expression, the forging of inclusive political coalitions, and expansive or pluralist notions of identity and nationhood, all play a role in bolstering resilience to violence. Social norms and values can protect against instability and enable resilience, but they can also support and encourage use of violence or violent conflict.

DECA Considerations Digital technologies have the capability to shift or disrupt established norms and values, simply due to their introduction, utilization, and mainstreaming in society. Digital technologies provide mechanisms for new norms and can persuade individuals to accept them.

- While digital technologies have supported and enhanced prosocial norms and values across the globe (social inclusion, financial assistance, 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 Economy Spotlight:** Monetary and social transactions of both formal and informal economies are steeped in historical context, culture, and norms. Digital technologies may [disrupt existing prosocial norms](#) (i.e., relationship-building across identity or affinity groups, or hierarchies) that meaningfully contribute to individual and community belonging as well as social cohesion and bridging across groups.

Narratives refer to the stories that individuals and groups tell to make sense and create meaning of their lived experiences through a coherent worldview. Narratives are both individually constructed and influenced by social groups, institutions, and media. Narratives dynamically impact individual and group perceptions, behaviors, and motivations, thereby shaping identity construction, norms and values, and group interactions. As narratives play a key role in creating meaning, forming belief systems, and influencing behavior, they are critical components of peace and stability, or conflict and violence.

Narratives can be used to encourage social interaction and political engagement to manage intergroup conflict, or they can be harnessed to increase polarization, weaken trust and social cohesion, and incite conflict, violence, and atrocities against specific groups. Group narratives circulate through a variety of domains, including traditional media, school curricula, official pronouncements, interpersonal communications, and community rumors. Control

of narratives and modes of dissemination are established arenas of social and political contest, and the spectrum of competing narratives in society often reflect fault lines of conflict.

DECA Considerations While narratives as drivers of peace or conflict predate the current digital era, digital technologies amplify narratives, which can generate opportunities for peace, or increase the risk of violence escalation.

- **Digital Infrastructure Spotlight:** [The Institute for Economics and Peace \(IEP\) Positive Peace framework](#) includes free flow of information as a critical pillar of peace and security; where free and independent media disseminates information in a way that leads to greater knowledge, informed decision-making, and improved human capital. Peacebuilding organizations and individuals are increasingly [mobilizing ICTs](#) to support social norms and narratives that build peace, including collecting and disseminating information on public security; crowdsourcing citizen experience; monitoring and mapping trends in conflict and violence; and strengthening citizen capabilities to [prevent and reduce violence](#).
- Media can impact individual narratives and behavior, as well as collective, group, and national narratives and identities. At the same time, identity and context frame how digital platform narratives are received, as offline social networks inform trust in digital media narratives.
- [New research](#) indicates that narratives promulgated through digital platforms are impacting conflict- and violence-affected environments in specific ways, particularly in shifting intragroup and intergroup perceptions and dynamics. 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 thrives across digital platforms, where siloed information networks [create multiple, parallel facts, narratives, and realities](#). The 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 [influence offline interactions](#). Where [competing, irreconcilable](#) narratives exist in society, there can be increased risk of conflict and violence.
- Upticks in extreme, polarized narratives and [digital hate speech](#) have been shown to reduce intergroup interactions and social cohesion, isolate already marginalized identity groups, and even contribute to offline violence, from interpersonal violence to mass violence and atrocities.
- **Digital Rights, Society, and Governance Spotlight:** Polarization within information spaces sows distrust, corrodes social cohesion, [erodes democratic values](#), and catalyzes [real-life unrest and outbreaks of violence](#). Under-regulated and under-governed online spaces enable weaponization of platforms for hateful or violent ideologies to reach wide pools of potential supporters. However, [in certain environments](#), regulatory responses to information-sharing have contributed to a shrinking civic space or even political repression and diminished freedom of expression.
- Digital civil society plays an increasingly critical role in strategically [countering misinformation and disinformation](#), upskilling communities for responsible use of digital platforms, utilizing emerging technology to document atrocities and hold perpetrators accountable, and defending digital spaces based on international norms and rights pertaining to freedom of expression, assembly, access to information, and the press.

DIFFERENT PLATFORMS, DIFFERENT NARRATIVES

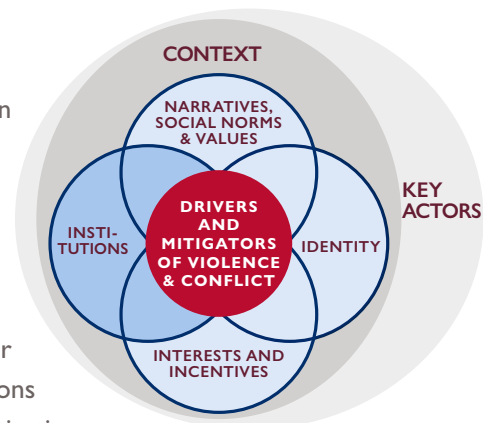
Authoritarian control and crackdowns as well as standardized regulatory controls on the information environment drive content and discourse to alternative, decentralized, or encrypted channels (Twitter, Whatsapp, Telegram, Signal, Reddit, Discord, etc.). There has been an [expansive growth](#) of encrypted messaging apps (EMAs)—where millions of users now rely on EMAs for interpersonal communication, commerce and financial transactions, organizing, [and, increasingly, for news](#) content. Non-state armed groups, criminal networks, and other malicious actors have been strengthened by tactical exploitation of different platforms, and strategic deployment of narratives and misinformation, disinformation, and hate speech to [disrupt or consolidate control, finance](#) and [operate](#) illicit and violent activities, and [recruit members](#). **Ordinary citizens seeking information, community, belonging, prestige, or opportunity may be vulnerable to compelling narratives, norms, and incentives established in digital spaces.**

What platforms are most used and how actors utilize them varies across countries. The Islamic State’s (IS) transnational footprint influences its digital strategy; IS’s advanced online strategy uses a wide range of digital platforms (Twitter, Telegram, WhatsApp, and YouTube) to reach and recruit from audiences across the globe. Boko Haram has used video-centric platforms (Facebook and Twitter) to publicize their attacks or arsenal and to dramatize their tactics and threat capabilities. Cartels in Mexico and the Northern Triangle similarly use image-based digital media (Facebook, TikTok, and Instagram) to promulgate narratives of prestige and profit, and harden self-serving offline social norms pertaining to violence, gender, and power.

INSTITUTIONS

The VCAF defines **institutions** as formal or informal rules and practices that govern human interaction. These include social and political structures, laws, policies, markets, organizations and other mechanisms for shaping human behavior. Formal and informal institutions operate at all levels of social life to influence interests, incentives, and behaviors. Institutional performance refers to the extent to which formal and informal institutions produce outcomes that individuals and groups perceive as effective and/or legitimate. Institutional performance can create or reinforce trends that contribute to societal resilience or grievances. When institutions perform in ways that groups consider to be legitimate and effective, then conflict-mitigating societal patterns likely emerge. In contrast, illegitimate and ineffective institutions can drive dysfunctional patterns of fragility and stress, which contribute to grievances and increase risks associated with conflict and violence outbreak.

As with individuals, systems and institutions are dominated by interests and incentives, and supply and demand for resources shape politics and public authority in ways that are transactional, exclusionary, and sometimes illicit and violent. In certain contexts, violence and criminality are utilized as governing strategies, where political and economic elites benefit at the expense of marginalized segments of the population. These environments are particularly unstable, as manifestations and cycles of violence and inequality spread by institutions are matched with escalating risk of violent resistance among the public. As noted, elitism, exclusion, chronic capacity deficits,



and corruption—all aspects of institutional performance—are among the most potent risk factors that give rise to grievance and violence.

DECA Considerations The [Digital Strategy](#) articulates USAID’s pursuit of advancing digital technologies to increase accountability and transparency in governance and improve service provision, including the ability of institutions to efficiently and effectively respond to citizens’ stated needs. DECA planners and assessment teams should examine the institutions that govern behavior and interaction in the digital ecosystem that have the potential to influence patterns of conflict, violence, or peace.

- **Digital Society, Rights, and Governance Spotlight:** Governments can build trust, legitimacy, and effectiveness—critical components of peace and security—by utilizing [digital technology and data for public good](#). Digital technologies have become increasingly critical—and sometimes primary—means for service provision, and governments can effectively improve performance through digital technology adoption. [Good digital government](#) (or e-government) is often characterized by [visible constraints to misuse by adopting and enforcing data governance policies and ethical guidelines](#); transparent procurement and delivery mechanisms; and open consultation with stakeholder communities for participatory governance in a digital world.
- Varied formal and informal institutions may be involved in protective structures against online harm, gender-based violence, or cybersecurity attacks. Computer Security Incident Response Teams, civil society organizations (CSOs), ICT companies, legislative bodies, and police units may play a role in the creation and implementation of legal protections.
- Countries experiencing conflict and violence may participate in regional, national, or subnational early warning systems, such as the [Conflict Early Warning and Response Mechanism](#) in the Horn of Africa. Early warning systems may be maintained by regional governance bodies, the state, or civil society, and often rely on varying degrees of digital infrastructure for operation. DECA teams should explore what barriers or support structures exist to inhibit or encourage early warning effectiveness.
- Alternately, governments can abuse power and exert control over digital infrastructure, tools, and governance in order to strengthen dominance over citizens. In 2021, [global digital rights watchdogs documented](#) at least 182 internet shutdowns in 34 countries; [intentional Internet restrictions](#), largely attributed to government campaigns to control or censor information, curtail media and civil society efforts, suppress opposition views, or to conceal [repressive or military tactics](#). According to [Freedom on the Net 2021](#), it is increasingly common for governments around the globe to assert control over telecommunications platforms to comply with censorship and surveillance. Internet and digital media surveillance technology has facilitated mass data harvesting, analysis, and targeting capability. In 2019, the Carnegie Endowment for International Peace found [47 countries used AI-based surveillance technology](#); with those figures expected to increase rapidly as technology systems proliferate and mature.
- An institution’s inability to enforce rules of protection and competition has been shown to contribute to opportunistic violence, where individuals and groups view violence as necessary, effective means to achieve security, stability, or opportunity. Conflict actors who compete with state control over resources or [information](#) have increasingly sought to control or [destroy digital infrastructure](#). Non-state armed group insurgencies across contexts destroy connectivity infrastructure to undermine security intelligence, public situational awareness, and [trust in central governance](#). Malicious actors infiltrate connectivity infrastructure for targeted information manipulation campaigns in order to access critical, private, or sensitive information, to [enable or advance their own conflict operations](#), or to degrade or disrupt critical service provision.

DECA CROSS-CUTTING TOPIC: CYBERSECURITY

Cyberattacks resulting in harmful surveillance, data harvesting, targeting capabilities, and cybercrimes are [on the rise globally](#) and often linked to trends in rapidly emerging [digital technologies](#). The rising proliferation of offensive cyber capabilities among state and non-state actors threatens peace and security at local, national, and international levels. Malign actors have used digital technology (e.g., malware, spyware, phishing, distributed denial-of-service attacks) to control or destabilize conflict and security dynamics in many varied ways, including by manipulating outcomes of national elections, geolocating individuals to surgically target opposition voices, controlling access to information, and shutting down critical infrastructure. Disinformation and propaganda campaigns are [often supported by malicious cyber operations](#) (false accounts, troll farms, and bots), which manipulate opinion, disrupt constructive dialogue, and escalate division, and even catalyze violence.

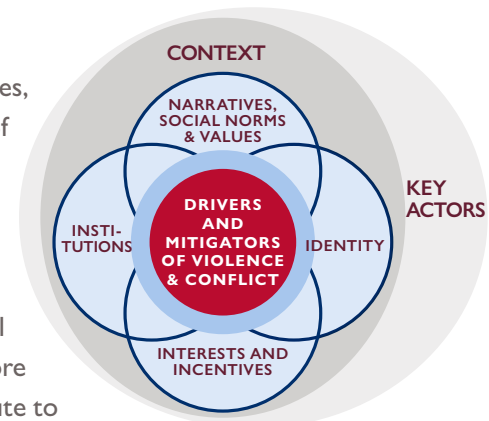
As digitalization expands, cyber spaces become more prominent arenas to exploit vulnerabilities and even wage conflict. In particular, countries with weak administrative capacities to protect key institutions and infrastructure from offensive cyber operations present growing opportunities to both non-state and foreign-state actors to surveil, capture, and disrupt critical digital infrastructure. Cybersecurity encompasses all the ways in which people, systems, and technology protect information kept in digital devices from being taken, damaged, modified, or exploited. See: [USAID Cybersecurity Primer](#) for more.

DRIVERS OF CONFLICT AND VIOLENCE

Drivers of conflict and violence emerge when the interactions between identities, institutions, narratives, social norms, values, and interests generate deep feelings of dissatisfaction (grievances). Often these grievances manifest over disparities in how society is organized and how this impacts citizens' lives and hope for the future. Grievances arise from the perception (objective or imagined) that an individual or groups' needs are not met, or that their interests or values are threatened by other groups or institutions. Grievances can be propagated by explicit, rational arguments and positions, or they can be sustained and transmitted through more symbolic or emotive ways in memory, narratives, and culture. Grievances contribute to individual or group belief that violence or violent conflict are necessary or effective means of achieving political, economic, or social needs or desires.

Drivers of conflict and violence also emerge when interactions between identities and institutions create **incentives** for participating in violence or armed conflict, as a means of advancing individual or group circumstances. Both grievances and interest-based conflict and violence are often most potent when they are attached to persistent societal patterns or trends.

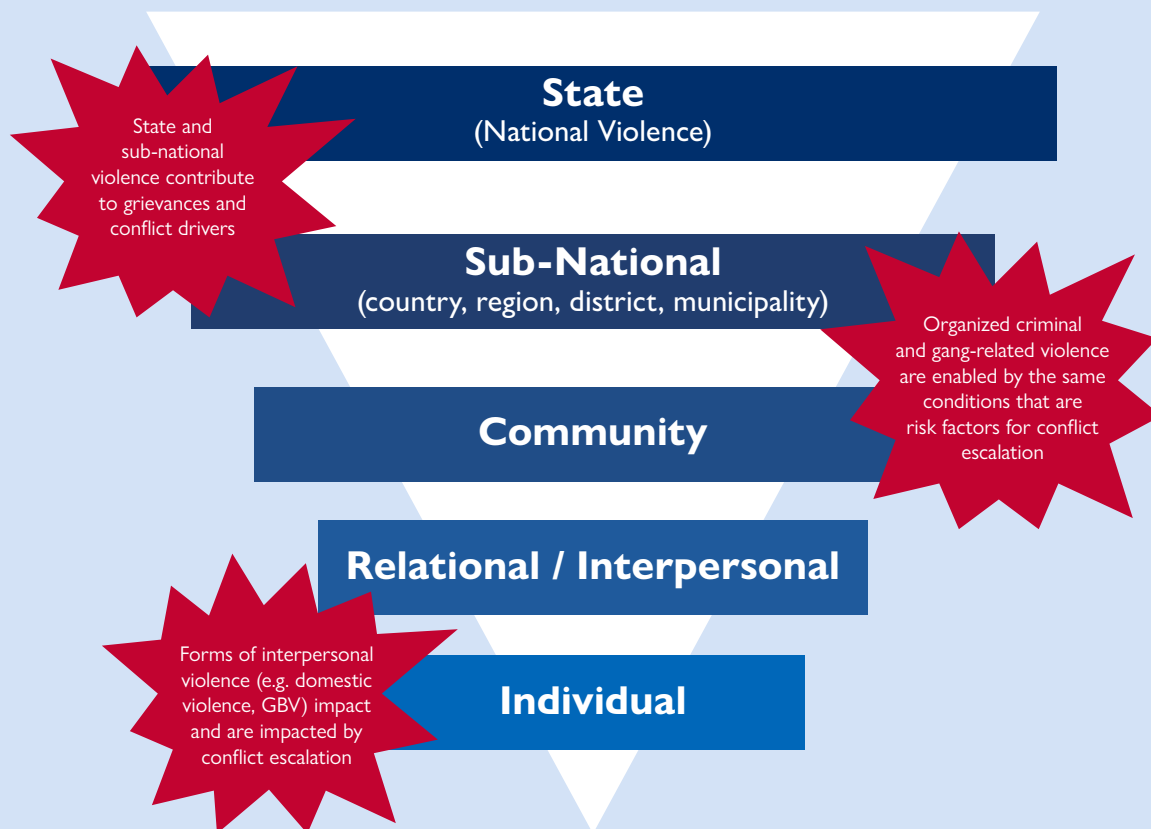
Societal trends are systematic and repetitive forms of interaction and transaction across individuals, groups, and institutions that either mitigate or drive conflict and violence. Elitism, exclusion, chronic capacity deficits, unmet expectations following transitions, and corruption are all examples of societal trends that frequently give rise to grievances and generate risk of conflict and violence. Likewise, some of the most common risk factors associated with individual violent behavior are entrenched trends of exclusion, economic inequality, unemployment, lack of opportunities, inadequate protection, erosion of social controls, and presence of criminal and violent organizations.



A NOTE ON NON-CONFLICT VIOLENCE

Understanding the dynamics of violence is crucial to USAID's efforts to promote peaceful and prosperous societies. When left unchecked, violence constitutes a major threat to the well-being of countries and their citizens. Today, violence is responsible for more fatalities than armed conflict and terrorism combined, with [homicides surpassing armed conflict deaths](#) by an estimated five-to-one margin.

When conducting research in conflict and violence-affected environments, it is important to assess both **conflict and non-conflict violence**, acknowledge the complex interactions between these, and seek to understand how these relationships exacerbate cycles of harm. In addition to overt conflict violence, research should include assessment of violence that takes place in the context of interpersonal relationships, families, communities, organized crime, and the state use of violent force. This frame is meant to assist users in integrating a more holistic understanding of violence and conflict, and does not replace existing USAID frameworks for assessing gender-based violence, gang violence, organized crime, citizen security, or violent extremism.



As noted throughout this guide, digital ecosystems impact both conflict and non-conflict violence. Digital repression tools enable sub-national and state-based political violence against civilians. Digital media and financing technologies are effectively wielded by criminal, extremist, and gang elements to multiply their operations. Digital media is playing an increasingly common and harmful role in cultivating [gender-based violence](#) and [violence against children and youth](#). Tactical targeting and victimization, as well as harmful narratives and [norms](#) distributed through digital media, can feed directly into individual and group motivations or vulnerabilities to participating in violence and violent conflict.

DECA Considerations . Digital development has the potential to play a positive role in promoting equity and peace, but it can also widen economic, social, and political gaps or deprivations and drive exclusion.

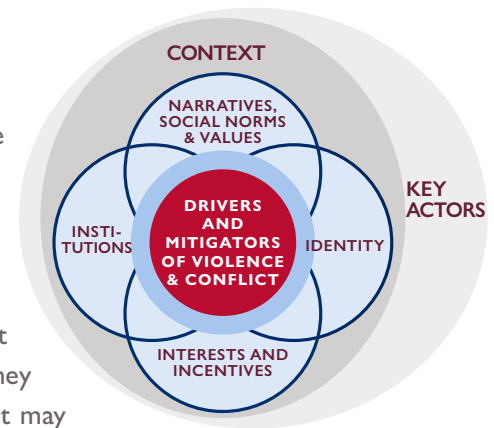
- Already marginalized communities are often left further behind by inequities in digital development, and often face greater risk of digital harms. These deprivations—deemed by UN Deputy Secretary General Amina Mohammed as the ‘[new face of inequality](#)’—can enforce narratives of relative deprivation and frustrated expectations of groups who do not see themselves as benefiting fairly from country advancement. In certain environments, long-term digital underinvestment in specific geographic areas can signal intentional deprivations towards specific populations. 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.
- Ineffective and inequitable governance—or governments that lack legitimacy across groups—feed narratives of grievance and exclusion. These deficiencies create fertile ground for mis-, dis-, or hate speech and further polarization of identity groups.
- **Digital Economy Spotlight:** Lack of economic growth and development is both a cause and a consequence of conflict and violence. Identity group-based inequality and patterns of exclusions from formal and informal economies are compounding risk factors for instability and violence. The [2021 Global Findex Report](#) estimated around 1.4 billion people lacked access to a formal financial system; the majority of unbanked persons live in developing countries, with conflict-affected countries showing the lowest levels of financial inclusion.
- Digital infrastructure and marketplaces can impact individual interests and incentives, creating opportunities for violent and criminal elements to extort and abuse individuals and groups, and generate revenue.

DECA CROSS-CUTTING TOPIC: INCLUSION

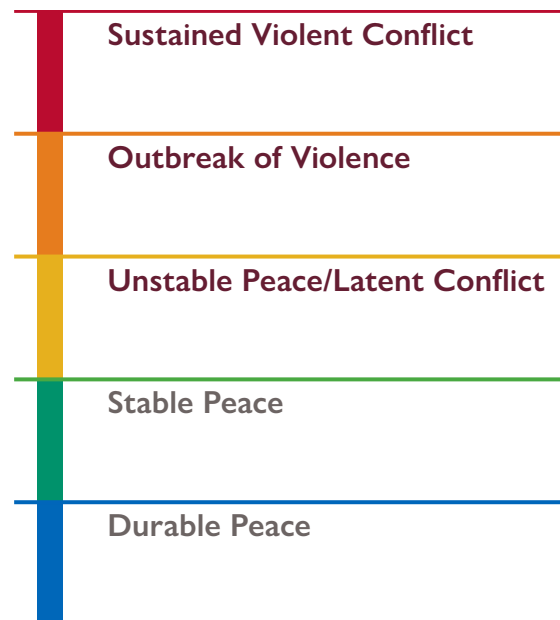
Marginalization and discrimination are among the most powerful grievances that reinforce conflict dynamics and exacerbate security concerns. [Research](#) on global digital ecosystems indicates that oftentimes populations who are more likely to suffer from other forms of exclusion are also digitally disadvantaged. Exclusions from digital spaces are often promulgated through social norms and inequities in access, literacy, or income. Depending on the local context, people may be excluded based on factors such as gender, race, age, ethnicity, disability, economic status, geography, sexual orientation, language, and refugee status. Involuntary exclusion from digital society and digital economies exacerbates societal divides and marginalization, harms social cohesion, and is an increasingly expanding barrier to individuals’ full participation in their communities and societies. Marginalized communities can also experience increased risk of exposure to digital harm as they are often not included in digital technology design, and are not being equipped to understand, utilize, and contribute to safeguards and protective measures. Recognizing exclusions and inequalities during the DECA research phase is an essential step to understanding how components of digital ecosystems interact with harmful conflict and crisis environment dynamics. See: [USAID Gender Digital Divide Primer](#), [Desk Review](#), [Gender Analysis Toolkit](#), and [Risk Mitigation Technical Note](#) for more.

MITIGATING FACTORS & RESILIENCE TO CONFLICT AND VIOLENCE

Whether and how armed conflict and violence erupts depends, in part, on the ability of institutions, identities, social norms, and other structures to provide means to suppress or resolve conflict through non-violent means. Most societies have mechanisms for organizing social competition and resolving disputes without recourse to violence, but these can function with varying degrees of effectiveness and legitimacy. For the VCAF, **mitigating factors** are the mechanisms that limit the outbreak, escalation, or recurrence of violence and escalation of conflict. They are not normatively positive, as disincentives for participating in violent conflict may also increase the intensity of latent conflict, which may manifest more intensely once those disincentives are removed. Examples of mitigating factors include reliable access to legitimate and effective local justice or dispute resolution mechanisms (positive) or firm control and regulation of a neighborhood's violent crime levels by a gang (negative).



Resilience to conflict and violence refers to the ability of individuals or groups to effectively manage and respond to active manifestations of violence and conflict. Resilience to conflict and violence is more focused on managing the harmful effects of conflict and violence on groups exposed to its effects. It includes a constellation of factors that contribute to individual or groups' ability to withstand and adapt to negative circumstances, including coping capacities, survival strategies, and other protective factors. Factors which strengthen resilience to conflict and violence are locally derived, but often include components of strong executive skills and sense of agency (or access to psychosocial support), social capital or connection to community, self-protection strategies, and the accompanying financial freedom to employ them.



DECA Considerations The digital ecosystem can both mitigate the likelihood of conflict and violence, as well as contribute to resilience to conflict and violence among those likely to be exposed to its effects. Some of these factors include ways for the digital ecosystem to help reduce wider social harms, while others specifically speak to how the digital ecosystem can address those harms that uniquely manifest in the digital space. **Digital ecosystems can contribute to societal resilience when digital infrastructure is interoperable, well managed and maintained, accessible, and well-protected; digital society, rights, and governance are built and operated around the primacy of citizen security and protection, and citizens are included in governance itself; and digital economies provide opportunities and pathways for diversified and inclusive economic development.** Some specific examples of how the digital ecosystem can mitigate conflict or violence and contribute to resilience to conflict and violence include:

- **Digital Infrastructure and Adoption Spotlight:** [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.
- USAID’s commitment to global digital ecosystems includes prioritizing opportunities to train the ‘workforce of tomorrow’ and build digital literacy within our partner countries. To be effective and equitable, USAID’s approach to digital programming must extend beyond access to physical devices and infrastructure and ensure that users possess a nuanced set of skills to meaningfully, responsibly, and safely participate in their digital ecosystem.
- Digital literacy efforts focused on reducing susceptibility to misinformation, disinformation, and hate speech are particularly important as both a mitigating factor and source of resilience to conflict and violence.
- **Digital Society, Rights, and Governance Spotlight:** Civil society can act as an effective buffer against the risk of violence, as CSOs can build relationships across social groups, promote social norms and other protections that discourage violence, and help maintain stability during crises. Civil society actors and organizations can curtail digital repression, serve as watchdogs in the face of declining online freedoms, promote [inclusive, participatory use of digital technologies](#) for public good, facilitate online activism and organizing, and [improve service delivery, peacebuilding](#) and humanitarian responses. CSOs are increasingly utilizing digital infrastructure to empower conflict and violence-affected communities—making development and stabilization efforts more inclusive, and equipping local voices with ‘digital agency’ and power over decision-making in peacebuilding and stabilization efforts.
- Increased access to online support services (e.g., psychosocial support for victims of violence) and informal support networks can strengthen individual resilience to violence and conflict.
- **Digital Economy Spotlight:** The expanding digital economy can be an important driver of democratic and economic development, opening up new market channels for local business, promoting inclusive trade, boosting revenue for governments, and increasing access to essential services. Though far from a silver bullet, digital financial technologies and environments have already reaped promising gains toward financial inclusion. In the wake of conflict and violence outbreak, functioning financial systems play critical roles; as mechanisms of stable governance and institutions, and as enablers of household resilience. A household strategy that uses multiple financial tools or systems is [more likely to be successful in mitigating the risks](#) and destabilizing impacts of shocks from conflict and crisis. In particular, [research](#) has shown that remittances and cash transfers have important multiplier effects on economic activity and recovery, and that digital financial services and mobile technologies can improve efficiencies, decrease leakage, and provide additional security and convenience to individuals using these funds. Access to diverse digital financial services and tech-enabled economies can support individual’s dignity, autonomy, and choice in how they manage their livelihoods, their survival, and/or their recovery, as these can put financial resources in the hands of crisis-affected people.

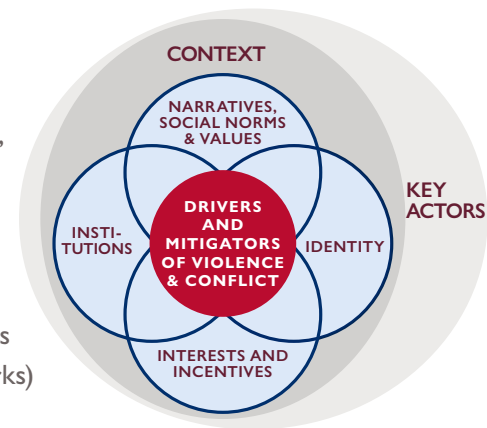
COPING AND ADAPTING AMIDST CONFLICT AND INSTABILITY

Somalia is [fast becoming a cashless society](#); an estimated 90 percent of adult Somalis own a mobile phone, while 73 percent use mobile money. This transition happened largely in response to chronic conflict impacts, contributing to the absence of an effective formal banking sector and lack of faith in the Somali shilling. In 2021, the Somali Central Bank formalized digital payments systems. Digital financial services are now a critical, unavoidable component of humanitarian support and long-term economic development and stability.

Following the Taliban takeover of Afghanistan in August 2021, [digital financial infrastructure](#) allowed citizens fleeing the Taliban to take their assets with them without risk; allowed humanitarian agencies to bypass banks and discreetly avoid the Taliban and provide cash directly to those in need; and assisted development donors to avoid unreliable intermediaries, with aid being given directly through a digital transaction.

KEY ACTORS

Key actors are individuals or groups that have the ability to influence conflict, violence, or peacebuilding outcomes, whether as mobilizers, enablers, perpetrators, or groups experiencing conflict. The ability of key actors to influence public outcomes varies. Conflict analyses often prioritize identifying mobilizers, or those who have the means and motivations to recruit, encourage, or mobilize others to engage in conflict, violence, or peacebuilding. Mobilizers may have a range of aims (ideology, political power, economic gain) and resources (financial, social networks) to draw upon to organize collective action.



Conflict dynamics are shaped by how key actors mobilize groups around communal identities, social norms, values, incentives, grievances, and resiliencies. Whether group disputes result in violence or armed conflict depends in large part on the motives and interests of those who stand to gain or lose substantially from violence. Key actors' interests most often involve some mixture of both public and private interests, and their stated aims and objectives may not be the same as their actual motivations and goals.

DECA Considerations While digital technologies have empowered key actors pursuing peace and stability with new tools to mobilize and advance peacebuilding operations, they have also catalyzed increased weaponization of digital space for political, economic, or social purposes by a wider pool of influential actors.

- Digital media platforms are often designed to accommodate low barriers to entry, relative anonymity, wide geographic reach, and vastly accelerated information creation and cascades (or, volume, reach, and speed). These dynamics have introduced or empowered floods of key actors and mobilizers to reach new constituencies and potentially contribute to conflict and violence escalation.
- Digital media can introduce not just *more* key actors, but *more polarized* actors; as even neutral actors are pushed into increasingly rigid and extreme positions. This vulnerability is exploited by malicious key actors who deploy strategic communication—including misinformation, disinformation, and hate speech—to amplify narratives of grievance and escalate polarization, chaos, instability, and conflict. DECA teams should pay particular attention to what actors are generating and

distributing misinformation, disinformation, and hate speech, and what communities are being impacted by information environment dynamics that cause harm.

ARTIFICIAL ACTORS AND MEANS OF MANIPULATION




There are a variety of online tactics that can be used to impersonate actors and manipulate conversations related to conflict dynamics, at both the local level and at scale. Those tactics include, but are not limited to, the ability to:

- Set up fake or automated personas to impersonate influential actors
- Manipulate audiovisual (e.g., image, video) content to change its origin or meaning
- Deploy artificial intelligence and machine learning to flood conversations with content
- Use bot or troll farms to artificially amplify or drown out content and harass individual users
- Purchase rapidly increasing private sector talent and capabilities (e.g., scaling disinformation services ‘for hire’)
- Distributed denial-of-service attacks
- ‘Deepfakes’ (text, picture, video, or audio manipulation using artificial intelligence)

All of these tactics can be deployed against opponents, dissidents, and marginalized communities who have limited means of redress and can suffer severe damages. Creating and scaling artificial actors—or artificial support for actors—has [manipulated public opinion](#) and resulted in [significant online and offline harms](#).

- Digital technologies have rapidly transformed the spaces in which conflicts are fought, as key mobilizers can utilize digital tools to surveil and suppress populations, manipulate public opinion, persecute opponents, stoke tension, and undermine social cohesion. DECA Teams should explore what entities and tactics (see below) are involved in these practices.
- Governments may use state resources and digital technologies to [spread propaganda or false information](#) against opposition parties to influence elections, justify violence, or control conflict narratives.
- Foreign governments, non-state actors, conflict stakeholders, and other financially or politically motivated actors can also adopt efforts to distort information environments; to shape public perceptions, subvert scrutiny and verification, and target and harm opposition parties.
- Data-driven technologies are becoming increasingly ubiquitous and more sophisticated (e.g., ‘deep learning’), which increases various actors’ ability to surveil populations in order to maintain or gain power. This is particularly troubling in contexts with weak legal and regulatory frameworks for data protection, including weak enforcement and oversight capacity. Conflict actors can surveil and exploit the massive quantity of vulnerable personal data collected and stored through individuals’ use of digital ecosystem technology to target, harass, and attack their opponents. DECA Teams should seek to understand what groups are using the digital ecosystem in this way and to what end.

FIGURE 4: Learning from DECA Research: Common Tactics and Outcomes

	Definition	Outcomes
CONTENT AMPLIFICATION	Using networks of covert or fake social media accounts to post and share content across multiple social media spaces. Amplified content may originally have been authentic, but is made to appear more popular or mainstream than it is.	 <ul style="list-style-type: none"> • Narrative Control: Biased or misleading information that serves to promote the political or military interests of a specific threat actor.
HASHTAG LAUNDERING	The use of media organizations to promote and legitimize hashtags that have been initiated or amplified in an inorganic manner.	
HASHTAG HIJACKING	This occurs when users take advantage of a trending hashtag to promote content substantially different from its intent.	 <ul style="list-style-type: none"> • Targeted Political Attacks: Direct attacks on politically exposed individuals. These often employ hate speech or disinformation.
NARRATIVE FABRICATION	The use of fabricated information typically as a means of engendering a strong response in the target audience and heightening division and polarization.	
NARRATIVE LAUNDERING	The initiation of a typically misleading or polarizing narrative that is recycled through well-established media outlets to lend the information legitimacy.	
HATE SPEECH	Abusive or threatening speech targeting a specific group or individual.	 <ul style="list-style-type: none"> • Incitement to Violence: Speech that encourages a target audience to commit acts of violence against a specific group or individual.

DECA CROSS-CUTTING TOPIC: GEOPOLITICAL POSITIONING

The varied forms of violent conflict often involve both strategic and spillover effects that cross national borders. Populations displaced by conflict and crisis spill beyond borders, insecurity and lawlessness allows armed groups to seize cross-border territories, and geopolitical competition fuels transnational flows of fighters, commercial assets, and information operations. USAID is committed to tracking and understanding the influence of authoritarian states—including but not limited to the People’s Republic of China (PRC) and the Russian Federation—which are actively working to shape the global digital space. Digital authoritarianism exported in different ways by PRC and Russia has created vulnerabilities not only in the security environment of partner states, but also in the ability of civil society and governing bodies to effectively manage conflicts and moderate civil discourse with transparency and accountability. Digital technologies developed within democratic and [allied states](#) have also been used toward geopolitical interests or malicious purposes, including international surveillance and cyberattacks. It is important for USAID Missions to understand how global dynamics impact the countries where they work, how global technology rivalries can affect development, information, markets, conflict, and crisis, and how geopolitical actors operate within country-specific digital ecosystems.

For example, during the Syrian civil war, USAID supported the Syrian Civil Defense, aka the “White Helmets,” a volunteer organization providing emergency assistance and relief to Syrians targeted by attacks. As they received more international support and media coverage, the White Helmets became the target of a [sophisticated and coordinated disinformation campaign](#). This disinformation campaign sought to sow suspicion about the credibility of White Helmets as a humanitarian organization, undermine their documentation of the Assad regime and Russian attacks (e.g., chemical weapons), diminish foreign political support, and erode their resources. In addition, the disinformation campaign provided cover to the Assad regime and Russia to deliberately target White Helmet centers and volunteers on-the-ground.

TRAJECTORIES

Trajectories refer to the likely paths a country is expected to face or continue facing. For the purpose of the VCAF assessment, trajectories encapsulate ongoing trends and patterns, as well as emergent events such as triggers, transitional moments, and windows of opportunity.

Trends and patterns (as discussed above) shape conflict and violence dynamics over extended periods of time. **Triggers** are immediate, usually observable actions or events that can provoke acts of violence, suppression, or conflict, including mass atrocities (e.g., disputed elections, sensitive or contested commemorations, assassinations, natural disasters). Triggering events or actions may amplify violence or create windows of opportunity for non-violent reforms or conflict mitigation. **Transitional moments** emerge following a crisis or dramatic change in a society’s structure. Transitional moments are often characterized by an “expectations gap” between what citizens expect and what the state delivers.

DECA Considerations Digital ecosystems—and the technologies they enable—are capable of contributing to sustained trends and impacting triggering events and transitional moments in distinct ways.

- Actors (including states, political parties, armed groups, etc.) have utilized digitally enabled political manipulation tactics, seeking to influence the outcome of political events by disabling digital infrastructure during elections or mass protests, or leveraging digital media to [propagate their position](#), manipulate voters, or [defame and silence opponents](#) and critics.
- Conflict and violence-affected environments already characterized by extreme polarization and/or potent patterns or narratives of grievances are at higher risk of trigger events precipitating instability and violence. The profit model of digital platforms often actively contributes to polarization and radicalization towards extremes.
- Digital media can magnify trigger events by quickly spreading mass awareness of events or issues capable of mobilizing action. Digital media also enables remote users to influence on-the-ground events, making volatile environments ripe for digital ecosystem contestation, platform control, and information manipulation. 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 false, hateful, dangerous speech in fragile contexts.

DECA CROSS-CUTTING TOPIC: EMERGING TECHNOLOGIES

The explosive growth of digital devices coupled with exponential advancements in emerging technologies have contributed to human progress and created exciting opportunities for effective international development. **Emerging hardware and software technologies** are opening new doors for early warning and civilian protection in conflict zones. Crowdsourcing applications are allowing for more effective organization of civil society, and increased accountability of government service provision and human rights protection. Artificial intelligence is being used to assess complex social and behavioral phenomena, from human trafficking and transnational crime, to violence perpetration and vulnerability to extremist actors.


While the pace and scale of innovation and mainstreaming of new technologies have clearly equipped development actors' reach and potential for impact, these also come with **significant ethical and human rights considerations and risks**. All digital technologies entail some level of data collection and storage. As such, they enable access to information—including information related to conflict dynamics, politically sensitive issues, or private information about citizens. In particular, the deployment of emerging technologies in crisis response—e.g., use of biometrics to identify refugee populations, or use of mobile cash or smartcards in cash transfer programs—highlight the complex balance between technology-enabled solutions and the need to protect individuals' rights to privacy, integrity, and dignity. In the absence of economic incentives for technology companies to reform their revenue models, technologists struggle to [embed democratic values and respect for human rights](#) in the development and design of algorithms, machine learning models, and software systems.

DECA research should investigate the prevalence of emerging technologies within digital ecosystems and should interrogate the potential use of emerging technologies for good or for harm.

SECTION 3:

Considerations for Conducting DECA in Conflict and Violence- affected Environments





This section provides operational recommendations for implementing DECA research in settings affected by conflict and violence. The recommendations include conflict-sensitive risk analysis and mitigation measures, as well as planning and management considerations for staffing, coordination, and data collection.

Research in conflict and violence affected environments inherently presents risks, including that a research team's approach to data collection and management may inadvertently exacerbate tensions, increase risk to respondents or the assessment team, or lead to adverse reputational or operational impacts for USAID and its partners. The team should conduct context-specific risk analysis and create mitigation plans and operating standards prior to commencing data collection. DECA Research Teams should consult local team members and Mission staff about risks and appropriate precautions. It is recommended that the DECA Research Teams take the following considerations into account as they begin the assessment process:

PLANNING AND MANAGEMENT CONSIDERATIONS

Consider how use of digital technology for engagement or data collection and management can be exploited: directly through targeted, malicious access; or indirectly through profiling algorithms. Exploitation or leakage related to data collection or management may result in harm.

- Ensure that personally identifiable and demographically identifiable information is *protected* in accordance with [USAID Data Policy and Governance](#) and considerations for [Using Data Responsibly](#), particularly if DECA consultants are using personal computers for data collection.
- Work with the Mission-based Regional Security Officer (RSO), Partner Liaison Security Officer (PLSO), and Democracy and Governance Officers to understand both *traditional surveillance* and *digital surveillance* capabilities and tactics of actors operating within the country context; tailor data protection and communication methodologies appropriately to mitigate risk.
 - » Identify which groups may be most vulnerable to surveillance and repression and ensure data collection approaches are designed to reflect and mitigate this increased risk.
 - » Identify any social or identity groups that may require specific logistical or cultural accommodations or protections in terms of team engagement.
- Be familiar with [trauma-aware data collection approaches](#) to avoid re-traumatizing respondents who are at increased likelihood of exposure to trauma in conflict and crisis affected areas.

Staffing. DECA planners should seek to staff teams with consultants and analysts with experience in conflict and violence-affected environments, deep knowledge of the country, and an understanding of local conflict dynamics. DECA consultants should be skilled in facilitating/leading group discussions in ways that are sensitive to biases, and experienced in collecting and reporting on data from interviews and discussions with transparency about potential limitations. When staffing the team, consider how the identities of the core team members may affect how the team is perceived in-country, how the team interprets the data it collects, and how the team operates internally. DECA research teams should aim for inclusion and diversity in team make-up and roles.

Coordination. Prior to commencing data collection, DECA planning and implementation teams should consult with USAID regional conflict experts with the supported Mission, Bureau for Conflict Prevention and Stabilization’s Center for Conflict and Violence Prevention, Office of Transition Initiatives, and Office of Civil-Military Cooperation, and/or Regional Bureau conflict experts to identify key conflict dynamics that should be factored into DECA data collection planning and relevant programming and learning.

The purpose of this consultation is to ensure DECA teams enter the conflict or crisis affected context with an understanding of key identity groups, conflict actors, data sources (violence observatories, early warning platforms, or peacebuilding activities utilizing digital approaches), as well as leads on potential key informants to consider engaging in the course of DECA data collection.

Data Collection Planning and Management. The following potential sources reflect both secondary and primary data collection approaches and considerations for DECA teams to include in their baseline and fieldwork.

Secondary Data Collection

- **Past Conflict Assessments, Violence and Conflict Assessments, or other related research** that may have been commissioned by the Mission.
- **Open Source Conflict and Violence Data Providers** can be used for supplemental conflict analysis, conflict and violence monitoring, and for deep dives into niche areas of interest. Some specific resources to consider include:
 - » [Armed Conflict Location & Event Data Project \(ACLED\)](#)
 - » [Uppsala Conflict Data Program \(UCDP\)](#)
 - » [Positive Peace Index](#)
 - » [Fragile States Index, Fund For Peace](#)
 - » [PVE Research Portal](#)
 - » [Digital Society Project](#)

Primary Data Collection

- **Key informant interviews.** Ensure respondents reflect populations with diverse perspectives and relationships with the conflict, particularly to understand patterns of inclusion and exclusion. Local conflict experts with the USAID Mission or local organizations can identify groups and facilitate contact. While all interviewees and research interlocutors provide an opportunity for learning, it is critical to remember that all stakeholders hold subjective opinions about conflict dynamics. It is important to consider the source of the information, what their relationship to conflict dynamics and biases might be, and to balance interviews and reporting with diverse perspectives. Interview questions should be vetted by local partner interlocutors for cultural and linguistic appropriateness and for highlighting potential sensitivities. Perceptions and attitudes are critical components of conflict dynamics. The assessment team should seek to understand why people feel the way they do, or what aspects of the conflict dynamics shape the feelings of the communities, which may or may not correspond to widely observed facts.
 - » Connect with the Mission Democracy and Governance Office for guidance on security postures and associated approaches to accessing difficult-to-reach areas and populations. Where appropriate, consider asking Democracy and Governance Officers for introductions to active local implementing partners for similar guidance.
- In addition to the core interviewees recommended in the DECA Research Guide, specific types of respondents to consider including in primary data collection include:
 - » State entities or other units responsible for investigating and prosecuting digital violence or cybercrimes (where they exist);
 - » State units or civil society groups who provide conflict or crisis early warning and/or manage disaster risk management systems; and
 - » Local or regional conflict and violence observatories.
- **Online research or content analysis via specialized digital platforms.** Digital platform analysis can be used for a variety of objectives, to include monitoring conflict dynamics and key events, sentiment or narrative analysis, assessing online opinions, behaviors, narratives, and identities, and mapping key actors and networks in a given context. If DECA teams are equipped to engage in specialized social media analysis, team members should respect the privacy and security of users by utilizing *public* content, anonymizing reports, and adhering to the guidelines for third parties laid out in platforms' Terms of Service.
 - » For practical tools and guidance on platform selection, data availability, use, and application for conflict and violence analysis, see [Social Media Analysis Toolkit for Mediators and Peacebuilders](#).



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