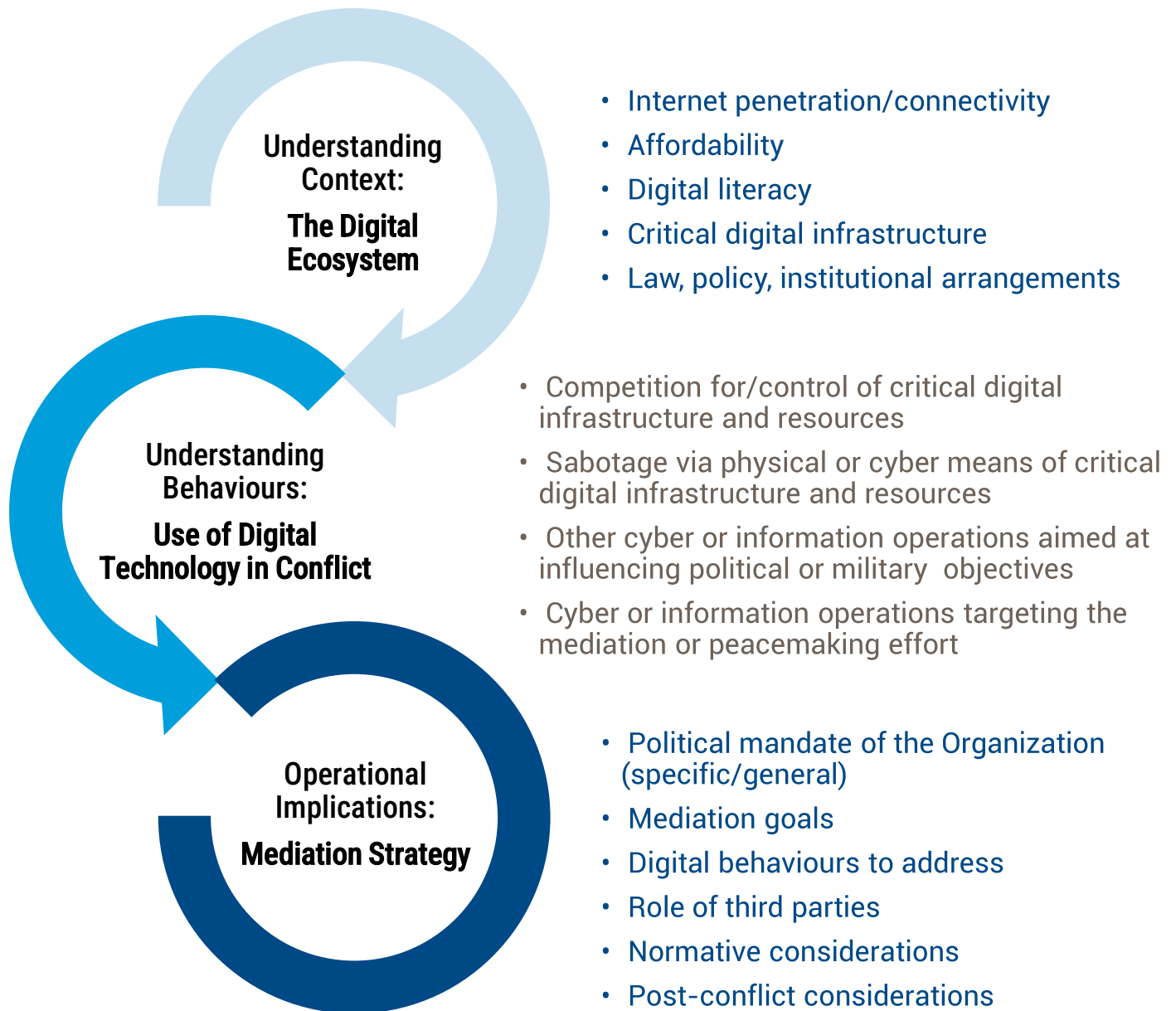


**DPPA
FRAMEWORK FOR
DIGITAL
TECHNOLOGY-
SENSITIVE
CONFLICT ANALYSIS**

Digital Technology-Sensitive Conflict Analysis



Background

The UN Guidance for Effective Mediation stresses the importance of preparation for mediation efforts to be effective and credible. This includes developing mediation strategies on the basis of comprehensive conflict analysis. There is a growing recognition of the need to better understand the role of digital technologies in the environments in which we work, including their use by conflict parties, the effects of such uses and their implications for efforts to inclusively manage and resolve conflict. This requires expanding our existing conflict analysis tools to ensure they properly capture new behaviours that can affect mediation and other peacemaking efforts, including when they are conducted online

It is expected that mediators will be increasingly dealing with digital technology-related issues as potential agenda items of peace processes. The following framework includes a non-exhaustive list of questions that can be used to enhance conflict analysis, ensuring it is sensitive to the digital technology-related behaviours of different actors in a given conflict situation. Not all questions will be relevant in all circumstances, and in making use of this framework mediation teams may wish to focus on specific aspects of the framework most relevant to the conflict context, issues raised by the parties and ultimate goals of the mediation process.

The list is broadly structured around the minimum elements suggested for the conflict analysis process in the [United Nations Conflict Analysis Practice Note](#) (2016). Section 1 provides a basis for assessing the general digital eco-system of a given country, or region within a country, an essential first step in any analysis; and for understanding the different legal and policy instruments that have been put in place (or not) relevant to digital technologies in a given setting, as well as associated institutional arrangements. This background information can provide a good indication of government capacities and capabilities and relevant checks and balances. Section 2 provides a basis for exploring how conflict parties use digital technologies as a means to attain their objectives and the potential harms associated with such uses. These uses often overlap and therefore should be assessed in conjunction with each other. Section 3, the analytical section, suggests a series of questions that aim to ascertain the implications of the digital technology-related behaviours identified for a negotiation process, and for UN mandate implementation.

UNDERSTANDING THE CONTEXT

1. THE DIGITAL ECOSYSTEM

ACCESS AND INFRASTRUCTURE

- 1.1 What is the internet penetration rate in the country? What is the smart phone usage rate in the country? Are there observable digital disparities within the country?
- 1.2 What is the cost of digital access (i.e., the cost of connectivity relative to local income)? Are there observable differences across the country?

- 1.3 What is the general level of digital literacy in the country?
- 1.4 Are there observable digital disparities in the country whereby gender, sexual orientation, ethnicity, education, economic situation, geography, language etc. influence a person or community's capacity to access and use the internet?
- 1.5 Which social media platforms are used the most in the country/region in question? Which languages are most predominantly used on the platforms? Are there any demographics that use certain platforms over others (in particular, young people or older people, women, men, and LGBTI people)?
- 1.6 What are the main telecommunications/digital infrastructure in the country (terrestrial/subsea)? Is the infrastructure privately, state owned or a mix of both? Which are the companies?

GOVERNANCE (LAW, POLICY AND INSTITUTIONAL ARRANGEMENTS)

- 1.7 Has specific legislation been adopted in the following areas:
 - Data protection/privacy
 - Cybercrime
 - Hate speech

In these and other pieces of legislation:

- Are individual rights relevant to privacy and data, including freedom of expression online, protections for women and girls from online violence and other such rights guaranteed in national legislation?
 - Is surveillance and censoring of online content or internet shutdowns permitted?
- 1.8 Has the government adopted a national cyber security and/or digital security legislation or relevant policy or strategy? Are these strategies gender sensitive, in particular, do they acknowledge gender-differentiated access and vulnerabilities and identify adequate risk mitigation measures?
 - 1.9 Has the government established a national cyber security agency? Have national CERT/CSIRT or other relevant emergency/incident response teams been established? What other cyber-related incident response/crisis management procedures are in place?
 - 1.10 Has the military published a cyber doctrine or strategy? Has a dedicated cyber command or similar been established?
 - 1.11 Has the government announced intentions with regard to developing offensive cyber capabilities? If so:

- Which is the responsible government entity?
- What oversight measures have been put in place to accompany the development and deployment of such operations?

1.12 With regard to the country's telecommunications/ICT sector?

- Which institution(s) is responsible for the telecommunications sector in the country?
- What are the main communications/digital infrastructure in the country? Is the infrastructure privately or state owned or a mix of both? Which are the companies?
- Has the government designated telecommunication and other such infrastructure and assets as critical? If so, has it made public this categorisation (e.g., in public policy or via a national security strategy)?

INTERNATIONAL NORMS AND COOPERATION

1.13 Has the government agreed to adopt other human rights or gender equality commitments on related issues (e.g., CEDAW - General Recommendation 35 on GBV against women, which addresses technology-mediated settings/environments and technology-mediated violence)?

1.14 Does the country actively participate in normative/ standard-setting processes relevant to digital technologies at the UN or regional/ sub-regional levels?

1.15 Has the government published its national view on how international law applies to the use of ICTs by States as per the recommendations of the UN Open-Ended Working Group (OEWG) and UN Group of Governmental Experts (GGE) on ICTs and international security?

CIVIL SOCIETY AND ACADEMIA

1.16 Do local/ global civil society groups actively engage on issues relevant to digital technologies in the country? If so, which groups and which topics? What is their perceived effect on public policy?

1.17 Do local or foreign academic institutions or think-tanks focus on any aspect of digital technologies and conflict as they pertain to the national context? What is their perceived effect on public policy/efforts to resolve the conflict?

IDENTIFYING AND UNDERSTANDING BEHAVIOURS

2. DIGITAL TECHNOLOGY USE IN THE CONFLICT (MEANS AND METHODS)

2.1 INFLUENCE AND MANIPULATION VIA SOCIAL MEDIA

2.1.1 What is the online social media presence of the conflict parties and other relevant actors?

- Which of the platforms identified in Section 1 above do they use? Do they use different social media accounts for different purposes?
- What is the size and make-up of their follower base?

2.1.2 Are there reports of the conflict parties, or affiliated actors, using social media, including encrypted messaging applications in conjunction with other internet enabled applications (e.g., GIS applications) to plan or conduct military operations?

2.1.3 Are there reports of the parties using social media for any of the following purposes: monitoring and surveillance; propaganda, disinformation/ misinformation; censorship and to control/influence domestic or international narratives; to organise mass gatherings (such as protests); to spread hate speech, incite violence, including sexual and gender-based violence against women and girls; to leak or disclose confidential information relevant to a political process or key political actors.

- Do these reported uses amount to what could be considered a targeted campaign or operation?
- Did any specifically target women (including women in politics, with political power, or women activists)?
- What are the reported effects of these online behaviours?
- Are third parties (e.g., States, hackers) reported to have supported or engaged in any of these activities? If so, which tools, techniques, procedures (TTPs) have they reportedly used?
- In your assessment, to what extent might they exacerbate existing tensions and serve as a threat multiplier?
- Have any of these behaviours been addressed in peace talks?
- Have any of these behaviours been referenced in official UN reports, including in briefings to the Security Council?

2.1.4 What are the themes of the messages/narratives that conflict parties typically disseminate on social media? Do these online narratives overlap with root causes, proximate causes, or triggers of conflict? What are the reported effects of these narratives on the conflict and efforts to manage or resolve it?

2.1.5 Do social media companies have content moderators/moderation processes in place? If so, do these cater to the languages spoken in the country?

- What is the process for flagging content that breaches the Terms or Conditions of Service of a social media site?
- Does your office/entity use an expedited process/trusted partner process?
- What other interactions does your office/entity have with relevant social media companies?

2.2 OTHER FORMS OF CENSORSHIP AND CONTROL

Are there reports of government authorities:

2.2.1 Using partial or country wide 'internet shutdowns' to blocks specific online services? Are these practices recurrent? Have they targeted specific regions/ communities? What was the reaction of the companies whose services were restricted?

2.2.2 Using spyware or security exploits for monitoring, surveillance or targeting of political opposition/rights/women's groups, parties involved in a peace mediation process, or of journalists covering the conflict?

With regard to points 2.2.1 - 2.2.2 above

- Are such behaviours permitted under national legislation? Do those affected have access to legal or other forms of recourse?
- What are the reported effects of such behaviours?
- Have any of these behaviours been addressed in peace talks?
- Have any of these behaviours been referenced in official UN reports, including in briefings to the Security Council?
- Can issues related to digital technology provide opportunities/ entry points for constructive engagements with the conflict parties?

2.3 OTHER BEHAVIOURS

Are there reports of conflict parties:

2.3.1 Competing for control of critical institutions (e.g., relevant ministries; state-run telecommunications/internet service providers; government websites; government CERT/CSIRT) or critical infrastructure?

- 2.3.2 Using physical, cyber or other means, to disrupt or sabotage critical digital/telecommunications infrastructure such as cell towers, fibre-optic cables (terrestrial, subsea), cable landing sites, telco facilities, data centres, satellite links.
- 2.3.3 Deploying cyber capabilities to sabotage or otherwise interfere with cyber-dependent infrastructure upon which the delivery of essential public services (e.g., water, energy, health, finance) is reliant.
- 2.3.4 Deploying cyber and other capabilities for monetary gain (e.g., ransomware attacks, cryptocurrency mining, theft).
- 2.3.5 Deploying cyber capabilities to exfiltrate confidential information or to undermine the integrity of information critical to an adversary's political/military strategy.
- 2.3.6 Deploying cyber capabilities to exfiltrate or undermine the integrity of information relevant to a mediation effort (positions/interests of the negotiating parties).

With regard to points 2.3.1 - 2.3.6 above:

- What are the reported effects of such behaviours? Are they reported to have spilled over into other countries?
- Have they been publicly attributed to a specific threat actor or group? If so, who attributed the incident, and through which means? Were any normative commitments alluded to in the attribution statement?
- Are third parties reported to have been involved? (e.g., proxies acting on behalf of one or other conflict party; governments; defence contractors providing material support to one or other conflict party)?
- Have any of these behaviours been addressed in peace talks?
- Have any of these behaviours been referenced in official UN reports, including in briefings to the Security Council?

OPERATIONAL IMPLICATIONS

3. MEDIATION STRATEGY AND PROCESS DESIGN

A comprehensive conflict analysis and stakeholder mapping that is sensitive to how conflict parties use digital technologies can provide a solid basis for designing effective mediation strategies in contemporary conflicts. In particular, it will be essential when mediators intend to: a) include digital technology-related issues on the agenda for negotiations, including on ceasefires negotiations (e.g., re-establishment of essential services including the internet, behavior of the parties on social media etc.); b) use digital tools themselves to advance the mediation process.

Once your analysis of sections 1 and 2 above is completed, the set of questions below can provide concrete ideas on how to 'operationalize' it.

3.1 DIGITAL TECHNOLOGY-RELATED ISSUES ON THE AGENDA OF THE PEACE PROCESS

3.1.1 What is the goal of the mediation process (potentially defined in a formal mandate from the mediator's organization and/or the nature of the request received from the conflict parties for assistance)?

Based on your analysis (Sections 1 and 2) and question 3.1.1 above:

3.1.2 What part of the mediation strategy and operations need to take into account the digital aspects of the conflict, including the behaviours of the conflict parties vis-a-vis the technologies?

3.1.3 Should some of the behaviours identified in your analysis be addressed in the talks so that the broader goals of the process can be met?

3.1.4 Might it be of value to promote integration of certain digital technology-related issues, including normative considerations into longer-term peacebuilding work? If so, how?

3.2 ONLINE MEDIATION ACTIVITIES

The [Toolkit on Digital Technologies and Mediation](#) and the [Digital Risk Management E-Learning Platform for Mediators](#) provide useful insights and practical suggestions for using digital technologies in mediation and for managing associated risks. Together with the analysis developed in Sections 1 and 2 above, these resources can help addressing questions such as:

3.2.1 Can digital technologies help achieve specific objectives of the mediation?

3.2.2 Can digital technologies (e.g., digital platforms for hosting online consultations) contribute to promoting inclusion, in particular of women, youth and hard to reach groups in the mediation effort?

3.2.3 What are the risks associated with using digital technologies in the mediation process?

RECOMMENDED RESOURCES

- ✓ National cyber/digital security strategies (see ITU Repository; [UNIDIR Cyber Policy Portal](#))
- ✓ National defence strategies, whitepapers
- ✓ In-country national cyber security agency reports
- ✓ National CERT/CSIRT reports
- ✓ National defence strategies, whitepapers.
- ✓ National critical infrastructure guidance/documentation
- ✓ National legislative resources (vis legislation etc.)
- ✓ Telecommunications companies/ internet service providers operating locally.
- ✓ Local business associations
- ✓ Social media platforms
- ✓ Local and international news organisations
- ✓ NGOs/CSOs, including specialised INGOs and women's groups
- ✓ Threat intelligence company reports
- ✓ Cyber operations trackers
- ✓ Internet traffic trackers (e.g., Netblocks, AccessNow)
- ✓ UNIDIR and other relevant academic and research institutions
- ✓ [Paper on Social Media and Peace Mediation](#)
- ✓ [DPPA Social Media Checklist](#)
- ✓ Sparrow [platform](#) for Twitter monitoring
- ✓ Digital risk management e-learning [platform](#) for mediators (UNDPPA, CMI, CPI)

OTHER RELEVANT RESOURCE MATERIAL

- ✓ [Report and Toolkit on Digital Technologies and Mediation in Armed Conflict](#)
- ✓ [UN SG's Hate Speech Strategy](#)
- ✓ [UN SG's Strategy on New Technologies](#)
- ✓ [Reports of the United Nations Rapporteur on Freedom of Opinion and Expression](#)
- ✓ [Reports of the United Nations Groups of Governmental Experts and Open-Ended Working Groups on ICTs and International Security](#)
- ✓ [Human Rights Resolutions](#)
- ✓ [Annual reports of the OHCHR](#)