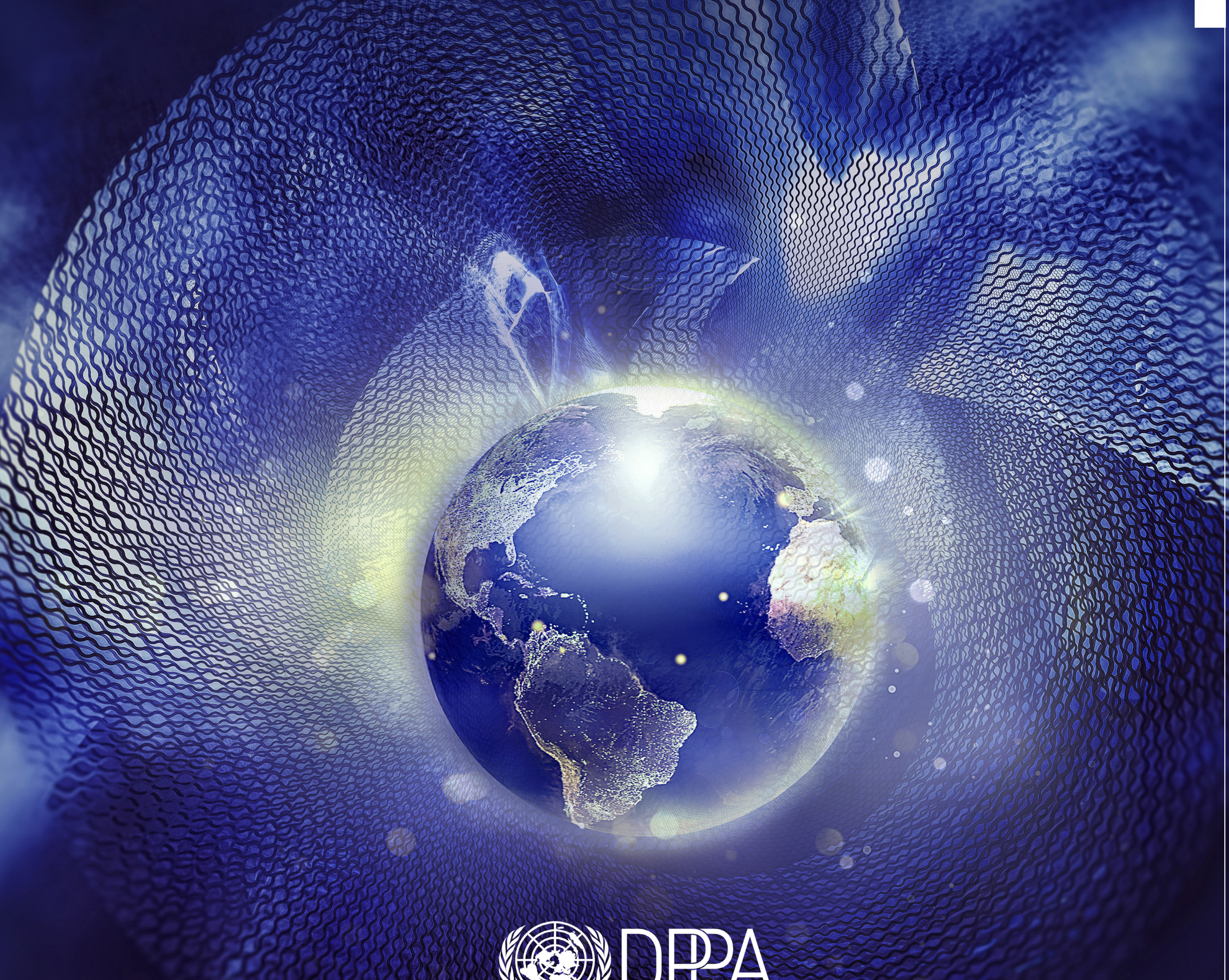
DPPA Practice Note: Addressing the Malicious Use of Information and Communications Technologies in Mediation Processes



DPPA

Preventing Conflict. Sustaining Peace

DPPA Practice Note: Addressing the Malicious Use of Information and Communications Technologies in Mediation Processes

Drafted by the Policy and Mediation Division, UN Department of Political and Peacebuilding Affairs. The Policy and Mediation Division is grateful to all who contributed valuable advice and comments throughout the process of this publication.

Table of contents

I. Introduction

The malicious use of information and communications technologies (ICTs) is a reality of contemporary armed conflict,[1] featuring regularly in international wars between States and in internal civil conflicts. UN Member States further share a common understanding that an increasing number of States are developing ICT capabilities for military purposes and that their use in future conflicts between States is becoming more likely.[2]

This Practice Note explores the implications of these trends for peace mediation efforts.[3] The malicious use of ICTs by conflict parties can have several effects, including the denial of access of an adversary to critical information and services, the degradation or disruption of an adversary's digital systems or networks, or even the destruction of such networks and critical infrastructure that relies upon them. To achieve these malicious effects, two primary ICT tactics deployed by conflict parties are: (1) offensive cyber operations,[4] and (2) Internet and telecommunications shutdowns.

Parties use cyber operations (or attacks) to gain unauthorized access to an adversary's digital services or networks. As has been widely documented since the Russian Federation's full-scale invasion of Ukraine in 2022, for example, both sides have conducted cyber campaigns.[5] Meanwhile, shutdowns involve actors using their control over national telecommunications networks to remove or restrict Internet and telecommunications access in internal conflict zones. In 2023 alone, governments or de facto authorities imposed Internet and telecommunications shutdowns in conflict zones on at least 74 instances across nine countries.[6]

Cyber operations and shutdowns are not the only ICT tactics used in conflict. Other methods include compromising ICT supply chains and hardware, either at the manufacturing stage or later along the supply chain, as was the case in Israel's pagers and walkie-talkies attacks in Lebanon in 2024. A more common use of ICTs involves information operations on social media platforms, which can shape the domestic and international narrative around a conflict.[7] Conflict actors also rely on commercial cyber intrusion capabilities (such as spyware) to monitor political opponents, armed opposition groups and civil society. These activities are beyond the scope of this Practice Note, which is focused on malicious ICT acts whose primary goal is to disrupt the normal functioning of digital networks and systems.[8]

As the malicious ICT conduct in conflict has grown, so have the calls for its inclusion among issues to be negotiated in peace processes. Demands for an end to "cyber attacks" featured in early diplomacy around the war between Ukraine and Russia,[9] and lifting the Internet shutdown in Tigray became part of the negotiations on a permanent cessation of hostilities in northern Ethiopia. By enhancing their preparedness in view of these dynamics, UN and other mediators may be able to respond more effectively when conflict parties, civil society organizations and humanitarian actors raise issues relating to these specific types of ICTs during peace negotiations.

Section II of this Practice Note introduces mediators to the malicious use of ICTs and shutdowns in conflict, highlighting their different possible effects. Section III focuses on the implications for mediation processes, mediator preparedness, and options for negotiating and monitoring agreements.

[1] International Committee of the Red Cross, "International humanitarian law and cyber operations during armed conflicts", 2019.

[2] *Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, A/79/214, 2024.

[3] This Practice Note is a result of collaboration between the Mediation Support Unit (MSU) of the United Nations Department of Political and Peacebuilding Affairs (DPPA), the Center for Security Studies at ETH Zurich and the Centre for Humanitarian Dialogue (HD). It includes insights from a workshop co-organized by ETH Zurich and MSU in 2022. The event brought together experts in mediation process design, ceasefires, cyber security and digital peacebuilding to discuss a paper by Sean Kane and Govinda Clayton, *Cyber Ceasefires: Incorporating Restraints on Offensive Cyber Operations in Agreements to Stop Armed Conflict*, 2021.

[4] General Assembly documents use "ICT operations" or "ICT attacks" rather than "cyber operations". Without prejudice to this terminology, this Practice Note employs the more informal "cyber operations" to enhance accessibility for readers who are not ICT experts (such as mediators). The Secretary-General has also used the term "cyber operations". See United Nations, "Secretary-General's remarks to the Security Council's High-Level Debate on 'Maintenance of international peace and security: addressing evolving threats in cyberspace'", 20 June 2024.

[5] See for example, CyberPeace Institute, "Timeline: How have cyberattacks and operations evolved over time since the military invasion of Ukraine", 2024.

[6] Access Now, *Shrinking Democracy, Growing Violence: Internet Shutdowns* in 2023, 2024.

[7] For further resources on social media and peace agreements see Govinda Clayton, Maude Morrison and Sean Kane, "Including digital technologies in peace agreements", in *Still Time to Talk: Adaptation and Innovation in Peace Mediation*, Accord 30, Teresa Whitfield, ed. (London, Conciliation Resources, 2024). See also Build Up, HD and DPPA MSU, "Monitoring social media provisions in peace agreements", 2024.

[8] Direct links may exist between different ICT acts, however. The denial of ICT access through cyber operations or Internet shutdowns, for example, may also be aimed at limiting the use of social media or media reporting.

[9] Russian Foreign Ministry, "Foreign Ministry statement on continued cyberattack by 'collective West'", 29 March 2022.

II. Potential consequences arising from the malicious use of ICTs in armed conflict

Integrating information and communications technologies into peace talks requires an understanding of the motivations for, and means of, using ICT tools for malicious purposes. This section provides an introduction for mediators, highlighting some potential consequences of the malicious use of ICTs in conflict.

Actors who exploit ICTs during conflict generally seek the following effects:[10]

- **Destruction:** long-term damage to a system or entity so that it cannot function or be restored to a useable condition. This approach may include permanently deleting data on a network or making it inaccessible, for example through malicious code known as "data wipers" (such as NotPetya, used in Ukraine in 2017). It may also involve manipulating industrial control systems to cause physical damage to the infrastructure they operate. In 2010, for example, the United States and Israel allegedly used the Stuxnet malicious computer worm to attack the Iranian nuclear programme.

- **Denial of service:** prevention of access to critical information, systems and services. This effect is often achieved through distributed denial-of-service (DDoS) attacks, such as those that succeeded in disconnecting Estonia from the Internet in 2007. A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming it with a flood of Internet traffic from multiple sources. Denial of service can also result from Internet and mobile phone shutdowns, such as those deployed in Myanmar, particularly since the 2021 military takeover.

- **Disruption:** a temporary break or interruption of the flow of critical information on a network, or of an adversary's access to systems or services. This effect is shorter in duration than a denial of service.

- **Degradation:** partial reduction of the operation of a network or communications system, or a limitation of an adversaries' access to networks. So-called bandwidth throttling is one example, as is blocking access to certain websites rather than a complete Internet shutdown.

Conflict parties can achieve these effects by exploiting ICT tools in two distinct ways: (1) by conducting offensive cyber operations, and (2) by using their control, administration and operation of telecommunications networks to enact shutdowns. Mediators are more likely to facilitate effective negotiations if they understand that these two approaches tend to differ with respect to the types of conflict in which they are adopted, the extent and permanence of their impact, and their implications for peace agreement design. A summary of the key distinctions between cyber operations and shutdowns elaborated in the remainder of this Section can be found in Annex I.

[10] Max Smeets, "The strategic promise of offensive cyber operations", *Strategic Studies Quarterly*, vol. 12, No. 3 (2018), pp. 90–113.

1. CYBER OPERATIONS

Cyber operations involve leveraging a combination of technological, human and organizational resources to gain unauthorized access to an adversary's digital services or networks and manipulating information stored on them.[11] In most cases, States are the perpetrators of cyber operations, since conducting them typically requires significant military, financial and technological capabilities. Cyber operations also have the greatest potential impact when directed against adversaries that operate substantial digital networks and systems themselves, such as other States. Cyber operations are therefore more prevalent in international conflicts between States or in "grey-zone" confrontations between adversarial States that are not formally at war.

States have explored both tactical and strategic uses of cyber operations during international conflict. As tactical tools, cyber operations can disrupt an opponent's access to critical infrastructure and network services, such as communications during battle. They can take secure government and military communications networks, anti-aircraft defence systems, or position, navigation and timing systems off-line. As strategic tools, they can directly attack and damage strategic military, dual-use or even civilian infrastructure in the opponent's territory.[12] Attacks have also been directed at financial and commercial targets, such as when data wipers caused significant economic losses in Ukraine.[13]

International wars such as those between Georgia and the Russian Federation (2008), Armenia and Azerbaijan (2020), and the Russian Federation and Ukraine have featured cyber operations in addition to conventional military operations.

Heavily internationalized civil wars have also seen ICT operations, including a reported cyber infiltration carried out by the United States in Syria that unintentionally took the country's Internet temporarily offline (2012).[14] Some non-state armed groups also possess sufficient capabilities to launch cyber attacks, as Hamas allegedly unsuccessfully attempted against a civilian target in Israel during their 2019 conflict.

The incidence of cyber operations in conflict is known to be increasing, yet the actual severity of their effects is uncertain.[15] Feared potential consequences of offensive cyber capacities, such as the destruction of critical infrastructure, have not yet occurred to any serious extent during armed conflicts. Conventional kinetic weapons remain more effective for producing strategic and long-lasting damage to an opponent's infrastructure and networks. Some cyber attacks have temporarily shut off electricity or communications networks, such as in Ukraine in 2016, but these impacts tend to be short-lived as manual controls can often be restored quickly.

While the impacts of individual attacks may be limited, however, the cumulative effect of sustained cyber campaigns can be significant. As of January 2024, the CyberPeace Institute had recorded 331 ICT incidents in the Russian Federation and 666 in Ukraine since the start of the war in 2022; of more than 20 targeted sectors, the public administration, financial and transport sectors were most affected.[16] The cumulative impact of type of disruption may be difficult to quantify, but it is certain to impinge on civilians' lives and social and psychological well-being.

[11] Florian Egloff and James Shires, "The better angels of our digital nature? Offensive cyber capabilities and State violence", *European Journal of International Security*, vol. 8, No. 1 (2023), pp. 130–149.
[12] Kane and Clayton, *Cyber Ceasefires*.
[13] The NotPetya data wiper attack, for instance, initially targeted Ukraine in 2017 and may have caused USD 10 billion in economic damages worldwide. See Joshua Stein, "Ukraine is on the front lines of global cyber security", Atlantic Council, 9 January 2024.
[14] Spencer Ackerman, "Snowden: NSA accidentally caused Syria's internet blackout in 2012", The Guardian, 13 August 2014.
[15] See, for example, Erik Gartzke, "The myth of cyberwar: Bringing war in cyberspace back down to earth", *International Security*, vol. 38, No. 2 (2013), pp. 41–73.
[16] CyberPeace Institute, "Timeline: How have cyberattacks and operations evolved over time since the military invasion of Ukraine".

2. INTERNET AND TELECOMMUNICATIONS SHUTDOWNS

In undertaking a shutdown, a government or de facto authority typically utilizes its ownership of, as well as its technical and administrative control over, national or local telecommunications networks to deny, disrupt or degrade an adversary's use of those networks and the Internet. Shutdowns differ from cyber operations in that they are most often undertaken as a tactic in intra-State civil wars.[17] Given that civil wars continue to account for most conflicts globally, this use of ICTs is of great relevance to mediators.

The act of restricting or shutting down network access in a specific geographic area can offer tactical advantages during armed conflict. It can limit an armed opposition group's ability to use ICTs for military purposes, such as to coordinate force deployment or access online geographic information systems to operate drones or to target mortars and rocket fire. It can also curtail a group's political organizing and financial activities, such as fundraising or the payment of salaries.

Outside situations of active armed conflict, governments and de facto authorities also implement shutdowns during domestic political crises, for example in response to mass protests or unrest related to contested moments during political transitions or electoral processes. Recent examples include shutdowns in Kenya, Myanmar, Sudan, Venezuela and, notably, Bangladesh, where protestors gave the Government a two-day "ultimatum" to restore the Internet as part of their demands during the July 2024 protests.[18]

Indeed, Internet and mobile shutdowns have become a common feature of domestic armed conflicts and political crises. Since the 2021 military takeover in Myanmar, for example, the State Administrative Council is reported to have ordered at least 275 shutdowns.[19] The reports of shutdowns were concentrated in states where the national military was engaged in armed conflict with ethnic armed organizations and opposition forces.

In contrast to cyber attacks, whose impacts to date have been largely temporary, shutdowns often have long-lasting effects. For example, civilians in conflict zones in the north-western and south-western regions of Cameroon (January to April 2017) and northern Ethiopia (2020-2022) have endured extended Internet and mobile phone shutdowns. The shutdowns in Cameroon even led to the creation of so-called "Internet refugee camps" as civilians and businesses moved around the country to avoid the Internet blackout.[20]

As the foregoing suggests, Internet and mobile shutdowns are blunt tools that affect not just armed groups or protestors, but also the entire population in a targeted geographic area. The UN General Assembly and Office of the High Commissioner for Human Rights recently detailed the dramatic and often underappreciated impacts of long-lasting shutdowns on civilians.[21] In situations of acute fighting, shutdowns can hinder civilians' ability to obtain life-saving information about troop movements and humanitarian corridors, as well as to communicate or request aid or medical assistance. As the Secretary-General has also indicated, "telecommunications blackouts" prevent humanitarian workers from seeking out the safest roads, coordinating aid distribution and tracking the movements of displaced people who need assistance.[22]

Over the longer term, shutdowns sharply curtail freedom of speech, economic livelihoods and access to banking services needed to obtain cash for necessities. Initial evidence indicates

[17] While less common, shutdowns have also been alleged in inter-State war. See, for example, Reuters, "Ukrainian officials report 'shutdown of all communications' in Kherson region", 31 May 2022.
[18] Deutsche Welle, "Bangladesh student group halts protests for 48 hours", 22 July 2024.
[19] Myanmar Internet Project, "No end in sight: situation of Internet shutdown and infrastructure damage in Myanmar", 16 July 2024.
[20] Moki Kindzeka, "Cameroonians march to demand internet", Deutsche Welle, 17 April 2017.
[21] United Nations Office of the High Commissioner for Human Rights, "Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights", 23 June 2022.
[22] United Nations, "Secretary-General's remarks at press stakeout", 15 January 2024.

that shutdowns harm women in particular, by denying them crucial economic and educational opportunities, exacerbating existing inequalities, and affecting their physical and mental health.[23]

Responding to these developments, civil society organizations have played an active role in reporting on the humanitarian, social and economic impact of shutdowns, as well as in lobbying conflict parties to restore services. In November 2022, for example, civil society groups called on the African Union to address the long-running Internet shutdown in northern Ethiopia as part of its mediation of the peace talks between the Government of Ethiopia and the Tigray People's Liberation Front.[24] In Sudan, organized pressure campaigns and legal challenges have led to court rulings aimed at restoring Internet coverage, at times with greater effect (such as in 2019)[25] than at others (such as in 2021).[26]

Barriers to addressing shutdowns during peace negotiations include the position held by some governments that shutdowns of Internet and telecommunications services are legitimate national security decisions under national regulatory frameworks. Through a series of intergovernmental processes, beginning with groups of governmental experts in 2015 and followed by fully inclusive open-ended working groups, States have consistently affirmed the applicability of international law to State use of ICTs and cyber operations. There is less clarity however with respect to shutdowns, as these working groups have also held that "States exercise jurisdiction over the ICT infrastructure within their territory by, inter alia, setting policy and law".[27]

The Global Digital Compact, a comprehensive intergovernmental agreement on digital technology adopted as an Annex of the Pact for the Future in September 2024, is notable in that it includes for the first time a commitment by States to "refrain from Internet shutdowns and measures that target Internet access".[28] Early drafts of the Compact contained language on the compliance of Internet shutdowns with international law.[29] However, as Member States' negotiating positions differed as to whether international law or national legislation should be included in the text, neither was referenced in the final version.

[23] Access Now, "Why Internet shutdowns are even worse for women", 8 March 2022.
[24] Access Now, "Two years of Internet shutdowns: people in Tigray, Ethiopia, deserve better", 4 November 2022.
[25] Reuters, "Some Internet service restored in Sudan after court ruling", 9 July 2019.
[26] Reuters, "Sudan court orders restoral of Internet, but no sign of services returning", 9 November 2021.
[27] A/79/214.
[28] United Nations, *Pact for the Future, Global Digital Compact and Declaration on Future Generations*, 2024.
[29] See Paragraph 28(d) of United Nations, "Draft Global Digital Compact", rev. 3, 2024.

III. Implications for mediators

Mediators can enhance their ability to facilitate negotiations on the malicious uses of ICTs in conflict by adopting a context-specific approach that is tailored to the specificities of a conflict and the needs of a mediation process. As most mediators have a relatively limited understanding of the ICT domain, this section discusses options for (1) enhancing mediator preparedness, and (2) negotiating and monitoring agreements on restricting malicious ICT uses. Wherever relevant, it highlights approaches that might be more appropriate for either cyber operations or shutdowns.

1. ENHANCING MEDIATOR PREPAREDNESS

Prior to any engagement, mediators can take steps to better prepare their team and the conflict parties to engage on digital issues. In this context, two elements are key: digital technology-sensitive conflict analysis and the integration of technical expertise into mediation teams.

i. Digital technology-sensitive conflict analysis

Conflict analysis is a crucial component of mediation. It helps mediators to understand the underlying issues, dynamics and interests of the conflict parties, and to develop an approach that meets the specific needs and challenges of the context. The UN's Framework for Digital Technology-Sensitive Conflict Analysis encourages mediators to undertake routine assessments of the "digital ecosystem", explore how conflict parties use ICTs as a means to obtain their objectives, and ascertain the implications of potentially malicious behaviours for a negotiation process and the implementation of their mediation mandate.[30]

Through conflict analysis, mediators can understand whether cyber operations, Internet and telecommunications shutdowns, or both are being deployed in a conflict. Distinguishing between ICT tactics may not be straightforward at first, since cyber operations and telecommunications shutdowns can produce similar effects, such as denial, disruption, or degradation of network services. However, a familiarity with the distinctions between these methods is vital for developing effective responses during a peace process.

Analysis can also help to determine whether addressing the malicious use of ICTs by the conflict parties is necessary to achieve the political mandate of the mediation process or if it could be a distraction from more fundamental issues.

Mediators should further ensure that the conflict analysis process involves input not only from belligerent parties, but also from other stakeholders and affected communities. Inclusive conflict analysis contributes to the design of similarly inclusive negotiation processes. Evidence indicates that wider inclusion increases the likelihood that the issues discussed within a mediation reflect the needs of civilians, particularly women and youth groups. In the longer term, inclusivity can contribute to the success and durability of agreements.[31]

As noted above, initial evidence from organizations such as Access Now shows that women are particularly harmed by Internet and mobile phone shutdowns. Therefore, women's full, equal and meaningful participation in the mediation process may create incentives and pressure on conflict parties to restrict malicious uses of ICTs that harm civilians or impede humanitarian assistance. Civil society organizations – which have been advocates for monitoring and calling for an end to Internet shutdowns – could also play concrete roles in negotiations, for instance by illustrating the humanitarian impacts of shutdowns or monitoring subsequent agreements to lift them.

[30] DPPA, "Framework for digital technology-sensitive conflict analysis", 2023.
[31] DPPA, "Guidance on Gender and Inclusive Mediation Strategies", 2017.

ii. Integrating technical expertise into the mediation process

If mediation teams and conflict parties' delegations decide to explore the malicious use of ICTs and its potential effects in a negotiation process, they are likely to need additional technical expertise. Conventional military personnel, political representatives and mediation experts will likely lack the knowledge required to negotiate and implement provisions regulating malicious ICT activities. Technical advisers and ICT experts may help to fill the gap (see Box 1).

The inclusion of such expertise generally increases the likelihood of addressing technical details comprehensively, thereby improving the chances of successful implementation. In particular, negotiations regarding ICT-related components of agreements may benefit from the participation of military commands involved in cyber operations, intelligence agencies active in offensive cyber operations and national computer emergency response teams. Similarly, addressing shutdowns may necessitate roles for ministries of communications, telecommunications companies and other types of network operators, some of which might be private-sector entities.

The inclusion of expertise is not without risks. Introducing technical elements that require additional resource people can complicate the negotiation process and potentially slow efforts to reach agreements on addressing other urgent political or security-related issues. Moreover, relevant actors and intelligence agencies may be unwilling to acknowledge their cyber activities or formally participate in the talks; they could also refuse to share full information in response to concerns about alleged malicious ICT use, thereby undermining or potentially even derailing proposed talks on these issues.

In addition, significant disparities in the parties' ICT knowledge and capabilities may need to be addressed to help enable a constructive exchange. In any peace process that involves a complex technical subject, non-state armed opposition groups tend to have access to far fewer technical resources and may thus require technical experts to be deployed or embedded in their delegations. Due to the potential impact on their perceived impartiality, however, mediators may wish to avoid direct engagement in some of these types of capacity-building efforts for individual conflict parties. They may instead opt to arrange joint technical workshops or coordinate with specialized organizations that can provide direct technical support to individual parties in need of greater assistance.

Ultimately, mediators should carefully discuss with the parties as to what roles might be necessary for technical actors to achieve their goals for the negotiations and the implementation of any resulting agreements. Such goals may involve cyber incident response or achieving the technical restoration of Internet or mobile services.

BOX I: RESOURCES AND SUPPORT

In order to help mediation teams address technical challenges, the DPPA Mediation Support Unit (MSU) has developed and made available a number of tools and resources related to ICTs on its UN Peacemaker Website.[32] MSU is also adding experts in digital technologies to the DPPA Standby Team of Senior Mediation Advisors Mechanism.[33] These resources are available to UN mediators and external partners upon request.

[32] See the Digital Technologies page on DPPA's Peacemaker website, https://peacemaker.un.org/thematic-areas/digital-technologies.
[33] See the Standby Team of Senior Mediation Advisers page on DPPA's Peacemaker website, https://peacemaker.un.org/mediation-support-unit/standby-team-of-senior-mediation-advisers.

2. OPTIONS FOR NEGOTIATING AND MONITORING AGREEMENTS

Conflict parties that are willing to discuss the malicious uses of ICTs are faced with a choice of how best to negotiate and structure the substance of an agreement. Mediators can play a central role in helping parties agree on an approach. In broad terms, parties can opt to incorporate principles or constraints through a specific agreement, protocol or annex, or as clauses in a broader ceasefire arrangement, peace agreement or international treaty.

Dedicated ICT agreements allow for greater detail and the opportunity to address a wider range of malicious behaviours. To date, none specifically address the use of cyber operations or shutdowns in armed conflict. Notwithstanding this, attempts have been made to address harmful uses of social media via dedicated agreements, facilitated by the Centre for Humanitarian Dialogue in Bosnia and Herzegovina, Indonesia, Kosovo, Nigeria and Thailand.[34] Stand-alone agreements risk marginalizing ICT issues and commitments, however, particularly if party leaders do not fully understand or support the resulting agreement or see it as peripheral to what they perceive as core conflict issues.

Alternatively, integrating or mainstreaming digital clauses into broader agreements offers the advantage of placing malicious ICT behaviours on an equal footing with other issues. In northern Ethiopia, for example, a broader cessation of hostilities agreement included the Internet and telecommunications among other essential services to be restored in Tigray (see Box II). A potential drawback of this approach is that the format can limit the amount of detail and that the agreement may therefore not cover the full range of problematic ICT behaviours. Provisions can also be vague and may lack the level of specificity needed for effective implementation, in particular monitoring.

As ever, the needs of the negotiating context should be the determining factor. If the parties have the limited objective of improving the humanitarian and economic situation in a specific region by restoring Internet and telecommunications services, the most appropriate way forward may be a stand-alone agreement specifying the timing of the restoration of services, guarantee of safe passage for technicians and basic monitoring. By contrast, if the parties are negotiating a comprehensive peace agreement and wish to limit the potential for cyber operations to disrupt agreement implementation, they may choose to include an ICT lens in a wider set of prohibited activities, as well as to establish communication and dispute resolution mechanisms.

The remainder of this section explores the negotiation of progressively more ambitious types of ICT agreements. The discussion begins with confidence-building measures, continues to specific prohibitions and constraints in formal peace, ceasefire and treaty agreements, and finally explores the monitoring of ICT commitments.

These different types of agreement are not mutually exclusive; rather, they are options that could potentially be elaborated over time. Mediation best practice typically prioritizes the establishment of functional relationships between conflict parties, with the aim of building confidence and trust before introducing more ambitious commitments as the parties move towards comprehensive agreements. Such an incremental approach may be particularly appropriate in relation to the unfamiliar terrain of ICTs. It could also help to avoid putting in place restraints that are unrealistic or that risk going unimplemented, which could undermine confidence in the wider peace process.

[34] For more details on these cases, see Annex I of Build Up, HD and DPPA MSU, "Monitoring Social Media Provisions".

i. Confidence-building measures

Confidence-building measures (CBMs) are actions taken to foster trust, cooperation, transparency and predictability between parties with the goal of promoting stability and reducing the risk of misunderstanding, escalation and (further) conflict.[35]

For example, conflict parties can agree to acknowledge – verbally or in written agreements – that cyber operations or shutdowns are taking place. They may also decide to incorporate the issues into the negotiating agenda. Simply acknowledging the digital dimension signals a willingness to shift behaviour, while avoiding the complexities of detailed prohibitions. Parties might also declare a general intention to cease future ICT activities, for instance by pledging not to interfere with Internet and mobile services. Such commitments can be monitored informally, so long as malicious ICT acts are easily detectable.

Going beyond general declarations of intent, parties might aim to agree on or reaffirm legal obligations, rights or emerging norms related to the responsible use of ICTs. Such steps can include commitments to honour existing obligations under international law relating to cyber operations, as well as the agreed voluntary norms of responsible State behaviour developed by General Assembly-mandated open ended working groups.[36] Parties can also recognize Internet and telecommunications access as a key enabler of other political, economic and social rights.[37] These types of affirmations would not necessarily require agreement on specific actions or monitoring provisions.

Other common CBMs in the digital space focus on agreements to improve communication and coordination between parties, or to provide an opportunity for information sharing, ICT incident response and management. Such measures may help to prevent ICT outages that are due to genuine technical issues or minor ICT incidents from escalating in the digital space or leading to offline hostilities.

ii. Constraints, prohibitions and commitments

Parties could also agree to include formal prohibitions of specifically defined malicious uses of ICTs in ceasefire arrangements, peace agreements or international treaties.

Ceasefires and related security agreements seek to limit, manage, stop and ultimately end conflict violence. Given their focus on limiting violent behaviour, ceasefires could address malicious ICT acts that have the potential to produce violent effects. Ceasefire prohibitions could include ICT activities that are expected to injure or claim the lives of civilians, damage civilian infrastructure, or threaten civilian organizations. Prohibitions might also address activities that undermine essential public and government services, such as the public Internet, communications networks, government civilian functions and essential public services. Detailed norms developed by inclusive UN open-ended working groups on the protection of critical infrastructure could be a useful starting point for the development of such provisions.[38]

Ceasefire agreements that seek a durable suspension of violence tend to go into considerable detail on prohibitions, as precision and clarity make it easier for the parties to implement an agreement and determine when it has been breached. Detailed restraints on ICT actions that lead to malicious effects would be akin to best practices relating to the management of traditional military weapon systems and technologies in a ceasefire agreement.

Given the pressing need for ceasefires in violent conflicts, mediators are justifiably reluctant to address issues that are not of clear importance to the process. In this respect, ceasefire provisions on the use of ICTs are only likely appropriate in cases when their effects cause serious harm to civilians, impede life-saving humanitarian activities or have a significant impact on conflict dynamics.

[35] See, for example, A/79/214. Annex B contains an initial list of eight voluntary global ICT confidence-building measures.
[36] A/79/214. Annex A contains practical checklists to assist with the implementation of these voluntary norms.
[37] Clayton et al, “Including digital technologies in peace agreements”.
[38] See A/79/214, in particular norms f, g and h in Annex A.

Prior to negotiating such prohibitions, mediators and technical experts could help to assess their technical and political feasibility. Specific restrictions on shutdowns are potentially easier to monitor than those on cyber operations (see below) and thus may be more technically feasible to include in ceasefires. On the other hand, Governments may see the restoration of telecommunications services as a sovereign decision to be taken through existing domestic legal mechanisms rather than in peace talks. It cannot therefore be assumed that it will be straightforward to reach political consensus among the parties on concrete prohibitions and constraints.

BOX II: CEASEFIRE AGREEMENTS

Local telecommunications shutdowns have begun to feature in the negotiation of ceasefire agreements. Most notably, under the November 2022 Permanent Cessation of Hostilities between the Government of Ethiopia and the Tigray People's Liberation Front, the Government committed to "expedite and coordinate the restoration of essential services in the Tigray region within agreed timeframes".[39] In early January 2023, State-owned Ethio Telecom announced that it had restored service to 27 towns and cities in Tigray following the ceasefire, a step that marked one of the first measures to be implemented under the agreement.[40]

In other ceasefire contexts, the effects of continuing Internet and telecommunications shutdowns have impacted the negotiation of ceasefire agreements. For example, facilitators of the December 2022 informal temporary ceasefire in Myanmar's Rakhine state reported that an ongoing shutdown complicated talks on the ceasefire. In particular, the shutdown limited the ability of the leadership of the Arakan Army, an ethnic armed group involved in the negotiations, to communicate with field commanders on the terms of the truce.[41]

Peace agreements seek to resolve underlying political issues and drivers of conflict between parties. With respect to ICTs, peace agreements might focus on measures to transition from conflict to cooperation in the digital domain. Such measures could include commitments to remove malicious software implanted in an adversary's networks or to engage in coordinated disclosure of hardware and software vulnerabilities used in cyber operations. Similarly, provisions might focus on re-establishing Internet or telecommunications coverage, rebuilding and restoring damaged or degraded infrastructure, dedicating the necessary financial resources needed for such reconstruction, and guaranteeing the safety of technical actors carrying out these tasks.

The parties might also agree to investigate the effects of ICT acts during a recent conflict or political crisis. Such an investigation could be undertaken with a view to establishing accountability and identifying possible policy and legislative changes to prevent the recurrence of ICT misuse (see Box III).

BOX III: REFORM AND ACCOUNTABILITY IN BANGLADESH

In Bangladesh, the interim Government prioritized investigating the Internet shutdown enacted during the July 2024 mass protests. The investigation, led by a newly formed committee under the interim Government's ICT adviser, revealed that the shutdown was undertaken by the Bangladesh Telecommunication Regulatory Commission and the National Telecommunication Monitoring Centre on direct orders from the former State Minister for Posts, Telecommunications and Information Technology. As of this writing, the probe had resulted in the removal of senior officials from national telecommunications regulatory bodies and reform of the legal framework surrounding the shutdown was under review.[42]

[39] Agreement for Lasting Peace through a Permanent Cessation of Hostilities between the Government of the Federal Democratic Republic of Ethiopia and the Tigray People's Liberation Front (TPLF), November 2022.
[40] Burkitt-Gray, "Ethio Telecom 'restores service to 27 towns' after ceasefire".
[41] Meeting with the Sasakawa Peace Foundation, whose staff brokered the informal ceasefire, 23 September 2024.
[42] Mamun Abdullah, "Probe reveals deliberate Internet blackout to suppress quota reform movement", Dhaka Tribute, 24 August 2024.

International peace treaties are written agreements between belligerent States that bring to an end the formal state of war between them. Given the relative rarity of inter-State conflict, contemporary examples of international peace treaties are limited. However, formal memorandums of understanding and bilateral agreements between States are more common, and several such instruments establish liaison mechanisms for managing cyber incidents (see Box IV). Since cyber operations are becoming a more common feature of inter-State war, future international peace treaties could be used to address malicious use of ICTs.

One candidate is the attempted draft treaty that was the topic of negotiations between Ukraine and the Russian Federation in March and April 2022, which reportedly includes mechanisms for the signatories to engage in consultations on urgent issues, exchange security threat assessments, establish emergency "hotlines" and put in place other confidence-building measures.[43] While the parties probably considered a wide set of security challenges in developing the provisions, these mechanisms could be well suited to restrict the malicious use of ICTs between the two countries, should peace negotiations one day resume and a treaty agreement be reached.

iii. Monitoring and verification

Monitoring and verification activities are often crucial for increasing the predictability and sustainability of ceasefires, peace agreements and international treaties. Agreements typically include provisions for creating new monitoring bodies or assigning functions to existing ones to manage and support implementation. Monitoring activities may play a key role in preventing the escalation of accidents and low-level ICT-related violations, as well as in increasing the sustainability and effectiveness of agreements.

BOX IV: INTERNATIONAL AGREEMENTS

In bilateral agreements between States, liaison and communication mechanisms are the most common types of arrangements for managing cyber incidents. Three such pacts are notable:

- The 2013 ICT security cooperation agreement between the Russian Federation and the United States, which establishes dedicated communication mechanisms for managing cyber incidents at the technical, military and presidential administration levels.[44]

- The 2015 cyber agreement between China and the United States, where the two countries commit to producing timely responses to requests for information, providing assistance in response to malicious cyber activities and establishing a high-level joint dialogue mechanism.[45]

- The 2015 agreement on cooperation between China and the Russian Federation which contains cyber non-aggression and mutual assistance provisions.[46]

In addition, the United Nations, the Organization for Security and Co-operation in Europe (OSCE), and coalitions of private-sector and non-governmental actors have developed voluntary norms of responsible behaviour in the State use of ICTs, as well as confidence-building measures for States that could serve as inspiration for liaison and communication provisions in future peace treaties.[47]

[43] On 15 June 2024, *The New York Times* published drafts of the joint agreement being negotiated between the Russian Federation and Ukraine. See, in particular, Article 4 of the draft dated 15 April 2022, Treaty on Permanent Neutrality and Security Guarantees for Ukraine.

[44] White House, "US-Russia Cooperation Fact Sheet", 17 June 2013.

[45] White House, "Fact Sheet: President Xi Jinping's State visit to the United States", 25 September 2015.

[46] Russian Federation, "Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security", 30 April 2015.

[47] See A/79/214 on the establishment of directories of technical and diplomatic points of contact to manage incidents. See also A/70/174, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 2015; OSCE, "Permanent Council Decision No. 1106", 3 December 2013; OSCE, "Permanent Council Decision No. 1202", 10 March 2016.

Attributing responsibility for ICT incidents that cause harm to civilians, digital networks and critical infrastructure, especially in connection with cyber operations, is notoriously difficult. As a result, the potential for negotiating detailed and specific restrictions on cyber operations may be limited. While technical capacities for identifying the sources of cyber attacks are improving among governments and private sector companies, the process of identifying the source of an incident, the actors involved and the extent of their independence remains challenging, complicating efforts to design, implement and monitor cyber components of peace or ceasefire agreements.

The main purpose of monitoring, however, is not necessarily to attribute responsibility and sanction violators. Rather, it is to manage incidents and prevent escalation. As DPPA's Guidance on the Mediation of Ceasefires notes, "in settings where elaborate monitoring and verification is not feasible, [ceasefires can instead] stipulate procedures for basic coordination, dispute resolution and de-escalation among the parties".[48] Monitoring and verification activities can be designed to take an incremental approach and evolve over time in terms of scope, detail and structure.

As mentioned above, shutdowns may be easier to monitor than cyber operations. They are generally carried out at the behest of a government or de facto authority that controls the targeted territory and associated telecommunications infrastructure. This makes attribution issues less challenging as compared to cyber operations. Tracking the lifting of shutdowns is also more straightforward than monitoring the cessation of cyber operations. Non-governmental Organizations such as NetBlocks and Cloudflare are demonstrating that open-source monitoring of Internet and mobile traffic is feasible.

[48] DPPA, Guidance on the Mediation of Ceasefires.

IV. Conclusion

The malicious use of ICTs in international and intra-State civil conflict is increasingly common. Cyber operations and Internet and telecommunications shutdowns are two common means through which conflict actors achieve effects, such as destruction, disruption, degradation and denial of access to digital networks and services.

Mediators can respond to this evolving landscape by considering the ICT dimension in peace negotiations. They can do so by adapting how mediation teams and conflict parties prepare for their processes, select issues for inclusion in negotiations and monitor agreement implementation. There is no one-size-fits-all approach with respect to the malicious use of ICTs. Negotiations must be fit for the purpose of the conflict context and the interests and technical capacities of the negotiating parties.

For mediators, a first step is understanding the distinction between cyber operations and shutdowns, whose key differences are summarized in Annex I. To manage both cyber operations and shutdowns, mediators can initially propose confidence-building measures that encourage parties to acknowledge ICT-related incidents and make statements of principles to adhere to principles based on international law and agreed norms. More concretely addressing the different characteristics of malicious ICT uses may require discrete mediation approaches and types of agreements, however. Mediators involved in domestic ceasefire or peace processes may find it possible to negotiate and monitor specific prohibitions and constraints related to shutdowns, if potential national security objections by governments can be overcome. In contrast, communication and liaison mechanisms may be more appropriate for addressing cyber operations and are more likely to be found in international peace treaties or agreements.

By understanding and addressing these distinctions while continuously adapting to the evolving ICT landscape, mediators can enhance the effectiveness and sustainability of peace agreements in the digital age.

Annex I: Key distinctions between cyber operations and shutdowns

	CYBER OPERATIONS	INTERNET AND TELECOMMUNICATIONS SHUTDOWNS
ICT tactic and intended effects	Gaining unauthorized access to an adversary's digital and communications systems and networks to disrupt, degrade or deny access to them or to damage these networks and the infrastructure that they operate.	Using control, administration and operation of national telecommunications networks to deny, disrupt or degrade an adversary's access to those networks and the Internet.
Relation to international law	Member States have affirmed that relevant international law and in particular the Charter of the United Nations applies to the ICT environment (A/70/174 and A/RES/70/237, and most recently in A/79/214).	As part of the Global Digital Compact, Member States committed to refrain from Internet shutdowns and measures that target Internet access (A/RES/79/1). As national law also regulates management of the telecommunications sector, some governments may see shutdowns as a national security matter that overrides international law.
Type of armed conflict	Mostly carried out by States against other States in international armed conflict or by adversarial States in "grey zone" confrontations.	Mainly enacted by governments or de facto authorities in internal armed conflicts or political crises, including to disrupt activities of non-state armed groups.
Duration of effects	Individual cyber operations tend to produce temporary effects on the functioning of an adversary's networks, conferring a tactical military advantage and causing economic losses but limited strategic damage to critical infrastructure. Extended cyber campaigns are likely to produce a cumulative impact on civilian well-being.	The duration can vary widely, from short-term shutdowns in moments of political crisis to multi-year shutdowns in protracted internal conflicts, with significant impacts on civilian populations and key human rights.
Monitoring and verification	Difficult, in view of the technical and political challenges involved in attributing responsibility for cyber operations.	Potentially feasible, given that attribution is relatively straightforward and that open-source monitoring of Internet and mobile traffic is technically possible.

DPPA

Preventing Conflict. **Sustaining Peace**