EUROPEAN UNION
Institute for
Security Studies

DIGITAL TECHNOLOGIES AND CIVIL CONFLICTS

BRIEF / 4
Feb 2021

Insights for peacemakers

by

Camino Kavanagh*
Visiting Senior Fellow, Department of War Studies, King's College London and Non-Resident Scholar, Carnegie Endowment for International Peace

CONFLICT
SERIES

INTRODUCTION

Most attention relating to digital technologies and conflict has focused on cyber or information operations between states.[1] Yet, it is civil conflicts that have increased in number and become more protracted over the past decade due to a number of factors, including their increasingly internationalised character.[2] Moreover, it is in these contexts that societies are more vulnerable and likely to be more affected by the misuse of digital technologies; and it is in these contexts that states show less restraint in their behaviour and can cause more harm to civilians. Mediating or facilitating a solution to civil conflicts, already an enormously difficult task, is compounded by the ways in which numerous actors use digital technologies to disrupt or delay conflict resolution efforts. For mediators and others engaged in peacemaking efforts, understanding these challenges is critical to designing already charged engagement strategies.

This Conflict Series Brief attempts to shed light on some of the risks associated with the use of digital technologies that can negatively impact mediation or negotiation efforts in civil conflicts, and examines

Summary

› Mediators and conflict resolution institutions now face greater challenges in peace processes as conflict parties rely on both online and offline means to recruit followers, finance activities, censor the vulnerable and control conflict narratives, and spy on or disrupt an opponent's digital systems.

› In this new context, mediators must develop a more sophisticated understanding of how such uses of digital technologies affect the dynamics of civil conflicts and disrupt peace processes.

› This includes understanding how the technologies are used in conflict situations, including support or services provided by third parties; understanding how international law, norms and other relevant measures can offer a framework for agreements or peace settlements; and identifying the range of actors with direct or indirect responsibilities in a particular conflict.

› The relative novelty of these issues for mediators underlies the urgent need for evidence-based research whose results might help mediators and other conflict management actors to respond more effectively to the challenges they present in peace processes.

The views expressed in this publication are solely those of the author(s) and do not necessarily reflect the views of the European Union.

how peacemakers might address them. Hence, rather than elaborating on the positive uses these technologies offer to mediators, which are already addressed by an emerging literature, we focus on clarifying the additional challenges conflict parties' use of digital technologies impose on peacemakers. Specifically, this Brief:

1. highlights how digital technologies can undermine peacemaking efforts;
2. summarises the international law, norms and other such measures applicable to the behaviours of the conflict parties in their uses of digital technologies; and
3. suggests a broader approach to stakeholder analysis.

On this basis, we illustrate and visualise an analytical framework (see page 4) suggesting how these three main aspects might be flexibly addressed depending upon the specific context. The final section offers some concluding remarks and recommendations.

DIGITAL TECHNOLOGY USES IN CIVIL CONFLICTS

Information technologies have always served parties to contemporary conflicts, with new uses constantly adapting alongside technological developments and levels of technological uptake in a given setting. An early example of such an adaptive innovation in intra-state conflicts can be traced back to the Angolan civil war and the mid- to late-1990s when external actors supported efforts by the National Union for the Total Independence of Angola (UNITA) to establish a domestic IT system and a global strategic communications network to influence the Angolan diaspora and foreign governments. This added to the myriad of obstacles preventing the resolution of the conflict.[3] External support provided UNITA access to the internet and email with web hosting and other IT support, allowing the group to "maintain an even higher profile than [it] had prior to the prohibition of its representational activities pursuant to SC resolution 1127 (1997)."[4] The UN team responsible for monitoring compliance with Security Council-imposed sanctions assessed a number of options for disrupting UNITA's communications,[5] eventually contacting the authorities of the state from which the IT support to UNITA was emanating. The situation resulted in a domestic investigation of the matter, while the Security Council called for further restrictions on UNITA, as well as greater attention to UNITA representatives' use of the internet.[6]

Offensive cyber tools and capabilities are also creeping into civil conflicts, often deployed in conjunction with information operations and other tactics and tools.

Some 30 years later, the relevance of digital technologies to civil conflicts has grown in tandem with the growth of digital-dependent global economic, social and political structures and the explosion of internet usage across the globe. The most obvious change has been the evolution of social media platforms, easily accessible technologies for communications and propaganda by all parties to a conflict, which in turn has driven states to develop tactics to censor or block messaging by opponents and control the internet and other communications technologies for their own purposes. Increasingly evident, too, is the degree to which offensive cyber tools and capabilities – once restricted to technologically-sophisticated states – are also creeping into civil conflicts, often deployed in conjunction with information operations and other tactics and tools. These uses of information technologies create new and complex power dynamics among the conflict parties, dynamics that peacemakers need to understand and consider in their engagement strategies.

Social media and information operations

Across the globe, social media platforms have provided significant opportunities for groups and individuals. They often represent the principal channel to communicate in real-time and mobilise support in times of political or social turmoil. These platforms make coordination and participation in decision-making much more immediate, effective and, at times, inclusive. They often allow members of a group engaged in peace negotiations, yet separated by significant distance and geographical obstacles, to maintain direct contact with their bases, which in turn can immediately mobilise support for or opposition to developments within the process. At the same time, such immediacy can be disadvantageous to a peace negotiation process since it removes the advantages of the protected (and 'noise'-free) space that distance often provides and in which conflict parties can agree to difficult compromises free of outside interference.[7]

Conflict parties often use social media to gauge or manipulate public opinion both domestically and internationally, which in turn can be used to legitimise critical decisions during conflict, such as whether to shift strategy, continue fighting or engage in settlement talks.[8] They also rely heavily on cross-platform and cross-medium tactics to amplify their stories, seeding them in blogs or on social media platforms.[9] From the Zapatistas in Chiapas to the FARC in Colombia such tactics have served to shed light on the plight of their group and garner sympathy and support for their cause.[10] Evidently, government actors, radical groups and others can counter these tactics.[11] They can use social media and other digital surveillance tools to monitor and disrupt or silence dissent and collective action.[12] Or they can rely on information operations, spreading hate speech and disinformation across social media channels to challenge the legitimacy of specific groups. In contexts such as Myanmar/Burma where social media (Facebook) is the only news or information source for a large swathe of the population, the implications have been significant.

Conflict parties can also use social media to monitor and identify potential targets. For instance, several women were assassinated in Iraq and Syria for comments made on social media following the withdrawal of the Islamic State (ISIS); in Turkey, Syrian nationals have been assassinated following comments made on social media against ISIS; individuals posting online commentary regarding the splits in al-Qaeda have met a similar fate.[13] In the context of a peace process or similar, conflict parties or their external backers can also use social media to monitor or silence the activity of international actors seeking to prevent or mediate a solution to the conflict.[14] Indeed, in current civil conflicts, there is growing evidence of conflict parties using social media to identify people within or beyond their own ranks who make comments online about compromise or dialogue with rivals on settlement issues.[15] Worryingly, there is increasing evidence of third parties, including States, engaging in coordinated information campaigns at the behest of or in support of one or other conflict party or to undermine the very legitimacy of a dialogue or mediation effort.[16]

These examples of single or cross-platform social media tactics, counter-tactics and operations involving multiple parties will likely increase in tandem with developments in technology and as more people come online across the globe. They constitute significant risks to any peace process, making it even more difficult for the parties involved to maintain a united delegation, facilitate or reach compromise positions, and ensure the security of their members. For peacemakers, they make it increasingly difficult to make sense of what is happening on the ground. They also render more complex the task of ensuring the integrity, security and confidentiality of peace negotiations and guaranteeing safe spaces for engaging the parties. Therefore mediators must find ways to work with conflict parties to agree on frameworks or protocols that moderate or even proscribe certain social media behaviours at different phases of a process. As for social media platforms, they need to step up their game in identifying and taking down accounts, including those of third parties, that have the direct intention of undermining peace efforts. This requires greater coordination of effort between peacemakers and the platforms, as well as with civil society actors, researchers and journalists on the ground.

Censorship and control

Several studies have demonstrated the different tactics used by states to silence dissent or control the information environment and critical information infrastructure within their borders.[17] In some contexts, governments, often with the acquiescence of - or by legally compelling - the telecoms sector, have completely blocked access through filtering techniques, internet or DNS takedowns.[18] Indeed, the practice of internet shutdowns – and the risks they pose to civilians – has become so common that AccessNow has developed an entire stream of work around the topic and the UN Human Rights Council has denounced such actions, as have relevant UN Special Rapporteurs.[19] In armed conflict, these tactics are often implemented in tandem with an uptick in state-backed violence.[20]

Parties to civil conflicts increasingly view control of domestic information infrastructure as a critical aspect of their operations and strategy. Take, for example, Yemen. As both a kinetic and cyber battlefield, Yemen's civil war reveals an interesting array of regional and global powers "attempting to project their power and manifest their interests" including with regard to the country's information infrastructure.[21] At the national level, when rebels seized the capital, Sana'a, they gained control over the country's main internet provider, Yemenet, as well as smaller ISPs and the country's main mobile operator.[22] Shortly thereafter, government sites were overhauled to broadcast rebel propaganda while the very access controls and censorship tools previously used by the government "to disrupt, degrade or monitor internet activity" were quickly turned against government internet sites.[23] Regional and international powers supporting one or other party on the ground have reportedly been involved in many of these developments, complicating matters even further, particularly from a peacemaking perspective.

For peacemakers, understanding and analysing trends in these kinds of practices can help determine whether shutdowns and other access issues should be considered in talks with conflict parties, particularly ahead of or following critical phases of a settlement, or ahead of or in the immediate aftermath of events such as elections or referenda.

Cyber operations

Offensive cyber operations involve attacking (destroying, damaging, degrading, disrupting, denying

Digital Technologies and Conflict Analysis in Civil Armed Conflicts

Increasingly internationalised and entangled with transnational crime and terrorism

Possible DT uses by combatants or third parties

- Requires analysis of how conflict parties use digital technologies to achieve their goals and how such uses can contribute to an increase in tensions, the intractability of a conflict, or delay the delivery of peace and other dividends.

Social media

- [Info. ops] For propaganda, disinformation/ misinformation purposes; to control/influence domestic or international narratives; to enlist the support of influencers; to spread hate speech, incite violence; to monitor political activities, rights or advocacy groups; to leak/disclose confidential information relevant to a political process or key political actors.

Surveillance technologies

- For surveillance and potential targeting of political opposition/rights groups; surveillance and intimidation of a mediation effort or similar.

Specific to offensive cyber ops tools or services

- To destroy, damage, degrade, disrupt, or deny system/network access or information critical to an adversary's pol/mil strategy; to exfiltrate confidential information critical to an adversary's pol/mil strategy; to exfiltrate or undermine the integrity of information relevant to a mediation effort (positions/interests of the negotiating parties.)

Other levers

- Blocking of social media or internet access.

Applicable law, norms and other relevant measures

- Requires analysis of the different norms and measures that mediators can lean on to reinforce the legitimacy of a process, the durability of an agreement, or to marshal international support for the peace effort.

Common to all uses

- UN Charter; customary international law; international human rights law; international humanitarian law; relevant UNGA and UNSC resolutions.
- National constitution and domestic legislation and policy (national security, cybersecurity, intelligence, defence, human rights, criminal, elections and telecommunications, critical infrastructure protection).
- Crisis communication mechanisms.
- Ceasefire arrangements or similar in which conflict parties agree to restraint measures regarding social media uses/ deployment of offensive cyber capabilities.
- Back channeling (with conflict or third parties to moderate online behaviours or to commit to measures of restraint regarding offensive cyber capabilities/ops).

Specific to social media

- Terms of service of social media and other relevant companies.
- Back channeling with social media companies for moderation of online behaviours of conflict parties and/or third parties.

Specific to surveillance technology and offensive cyber ops tools or services

- Back channeling with relevant tech/ cybersecurity companies or CI operators.
- Voluntary norms/principles applicable to third parties supporting one or other conflict party (e.g., GGE norms and CBMs relevant to critical infrastructure, CERTs/CSIRTs).

Actors with responsibilities, mandate or leverage

- Requires a differentiation between actors with direct or indirect roles in the conflict, their understanding of the role DT play in the conflict; their spoiler potential; the leverage or sway they might have at different stages of a mediation effort.

Common to all uses

- UNSC.
- HRC and specialised bodies.
- Law enforcement (INTERPOL, EUROPOL).
- UN, AU, EU, OSCE, OAS, ARF (good offices/ mediation/crisis management).
- Friendly states (good offices/ intelligence).
- Regional powers (good offices/ intelligence).
- Principal donors/IFIs in a given context.
- ICRC.
- Specialised INGOs (conflict dynamics; human rights, mediation).

Specific to social media

- Social media companies.
- Human rights and other advocacy groups.
- Academia/think tanks.

Specific to surveillance technologies

- Surveillance technology vendors.
- Wassenaar Arrangement members.
- HRC and specialised bodies.
- INGOs (conflict dynamics; human rights NGOs, mediation).

Specific to offensive cyber ops. tools or services

- UN (SC and other relevant departments/ entities), AU, EU, OSCE, OAS, ARF (good offices/mediation/fact-finding, peacekeeping, crisis management).
- ISPs.
- Critical infrastructure operators.
- CERT/CSIRT networks.

ARF = ASEAN Regional Forum, CBMs = Confidence-building measures, DT = Digital Technologies, GGE = Group of Governmental Experts,
HRC = Human Rights Council, ICRC = International Committee of the Red Cross, INGOs = International non-governmental organisations,
ISPs = Internet service providers, NGOs = Non-governmental organisations, OAS = Organisation of American States,
OSCE = Organisation for Security and Cooperation in Europe, UNSC = United Nations Security Council

system/network access or information) or exploiting (removing confidential information) an adversary's computer networks.[24] In many civil conflicts, parties might not have the capacity or resources to deploy the "highly structured campaigns" that tend to receive media and expert attention.[25] But options for access to cyber operations tools and services are steadily growing, not just for state parties. For instance, if there is an existing computing sector or base of computer engineers and cybersecurity experts in the country, the development of reliable, cheap and effective cyber operations tools by either party is certainly plausible, facilitated by increasingly accessible malware pieces that can be easily "harvested, modified, repurposed, and deployed."[26] Alternatively, with the right backing or resources, conflict parties can rely on external parties (e.g., their traditional weapons providers, major powers, regional or religious allies, or criminal organisations) to supply the tools and intelligence required to deploy offensive capabilities, and, if needed, serve as their delivery mechanism.

While the deployment of cyber operations or capabilities are, for many reasons, still few and far between in civil conflicts, peacemakers need to be aware that conflict parties – including third parties seeking to tip the conflict or a negotiation (ceasefire, peace settlement etc.) in one direction or another to meet their own interests – have currently few incentives to refrain from using them.[27] Coupled with information operations, such activity will likely increase in the coming years, posing important risks to civilians, particularly if critical infrastructure and facilities providing essential public services are targeted.[28]

For peacemakers, understanding key factors, including indicators of capability such as whether the parties are known to have deployed cyber capabilities previously and who might provide such services to the conflict parties in the event that they themselves do not have the necessary capacity and resources is paramount, as is understanding the intent behind such behaviours.[29] It is equally important for peacemakers to understand the views and positions of conflict parties (and the states or coalitions of states providing them with support) on relevant norms of restraint and their participation in crisis management or confidence-building mechanisms.[30] Such analysis can help shape engagement strategies at different phases of a mediation, signalling where additional emphasis might be placed, directly with the conflict parties, and indirectly with third parties, and also inform future conflict management efforts.

INTERNATIONAL LAW, NORMS AND OTHER PREVENTIVE MEASURES

As noted in the UN Guidance for Effective Mediation, peace frameworks consistent with international law and norms can "reinforce the legitimacy of a process and the durability of a peace agreement" as well as "marshal international support for implementation."[31] The behaviour of parties to an intra-state conflict, and particularly those actions affecting civilians, is limited by the same set of international law and norms governing armed conflict between states (especially the Geneva Conventions and human rights law).[32] The means and methods used by conflict parties does not change this basic assumption, even if work continues within the UN to determine *how* existing rules and principles of international law apply in practice, including in non-international armed conflicts.[33] As a result, mediators and other actors involved in peacemaking activities should sharpen their awareness of ongoing discussions about the international law and norms applicable to digital technology use by different actors and integrate this understanding into their peacemaking and follow-on strategies (see table on page 4).[34]

Beyond binding international law, and depending on the context, peacemakers might borrow from voluntary norms, including those recommended by the UN Group of Governmental Experts (GGE) to advocate for restraint among conflict actors (and their external backers) in their uses of digital technologies. This includes those norms that commit states to restraint in ICT activity that intentionally damages critical infrastructure, and that encourage states to respect relevant human rights instruments.[35] Peacemakers might also draw from the rich research around internet shutdowns, and seek a commitment from the parties to ensure that internet access remains open and uninterrupted. They will likely need to remind industry actors of the actions to which they, too, have committed, including the UN guidelines on business and human rights, and the Paris Call for Trust and Security in Cyberspace, particularly with regard to protecting the internet and safeguarding civilians from harm. [36]

Third party mediators or facilitators might also consider drawing from practices in other areas to encourage parties to a conflict (again, including third parties) to agree to a range of other 'do-no-harm' principles regarding surveillance of mediators and their interlocutors and the protection of critical information infrastructure or infrastructure providing essential services to the public. New research emerging on how cyber and information operations might be considered in ceasefire arrangements can also provide practical insights in this regard.[37]

Where social media is concerned, peacemakers may also find value in identifying alternative ways for parties to moderate or exercise restraint in their online behaviour at different phases of a peace process.[38] This can include, for instance, working with conflict parties to identify the types of behaviours that could, in their view, undermine a process or the safety and security of those involved; and forging basic ground rules, stand-alone, voluntary codes of conduct, or specific clauses in a broader agreement to mitigate against them. Close cooperation with social media platforms as well as civil society groups, researchers and journalists on the ground can also help identify coordinated inauthentic behaviours involving third parties that could potentially pose a risk to a peace process. Further cross-domain research on approaches like these, slim as it may be at present, is urgently needed to inform the work of mediators and other peace practitioners.[39]

NEW STAKEHOLDERS TO CONSIDER

Conflict parties' increasing reliance on digital technologies also means that a number of additional actors are directly or indirectly implicated in today's civil conflicts. The actions or non-action of many of these actors can have enormous sway on power dynamics between the parties and on the viability and sustainability of an agreement or settlement. Many of these same actors have been involved in stakeholder mapping in peacemaking for some time, although they have taken on new roles (e.g., providing direct or indirect material support or services to one or other party). Others are completely new to peacemaking. A more informed understanding of relevant stakeholders in civil conflicts is urgently needed, not only to inform the engagement strategies of peacemakers, but also to inform ongoing normative debates.

Major technology and defence industry companies continue to provide state parties with surveillance technologies.

For instance, major technology and defence industry companies continue to provide state parties with surveillance technologies, despite years of reporting on the related harms. Private cybersecurity companies or states already supporting the cause of one party or another (including through arms supplies or military exercises), can provide the means and know-how to spy on or counter or deny the effects of their opponents' tactics. Lone hackers or [h]activist groups may associate their own interests or causes with those of one of the parties to the conflict and provide technical or other support. Terrorist or extremist groups in some regions may use social media to manipulate local group grievances to recruit new members, incite further violence, spread propaganda or finance certain activities. As always, criminal groups will be on standby to see how they can take advantage – both online and offline – of the conflict in question.

Human rights groups will often engage in situations where authoritarian governments attempt to silent dissent, providing the means and know-how to opposition groups to circumvent government control or bolster their own privacy and cybersecurity. Sometimes these efforts are funded by an outside state, which may, unintentionally, undermine the legitimacy of the effort.

Specialised bodies such as computer emergency and incident response teams (CERTs or CSIRTs) may be unwittingly drawn into a civil conflict when requested to respond to cyber incidents, and may even be compelled by a state party to work at its behest, thus creating a significant ethical dilemma for the CERT or CSIRT.[40] Technology and social media companies, too, play a significant role in this area as their tools or platforms can be used for both offensive and defensive purposes by the parties in a conflict or for information operations. Their responses to a given conflict situation can tip the balance of power in one direction or another. In some instances, technology companies may be compelled to adapt their terms of service to comply with state regulations or face closure. Yet, as has been widely reported, engaging or even establishing basic contact with the very companies whose technologies or platforms are used by conflict parties is particularly complex in conflict situations.

At the same time, many of these same actors – in particular, technology and social media companies, CERTs/CSIRTS, cybersecurity researchers, human rights groups – have some degree of leverage in a conflict or can be critical to preparing the ground for a settlement. They can help minimise the harm caused by malicious uses of technology at critical moments or contribute positively to moderating behaviour. To inform their engagement strategy, peacemakers should analyse how such actors contribute to a given conflict and its potential settlement in both the commonly cited senses: *negatively* (ending the fighting or, in this case, the negative or disruptive behaviours *vis-à-vis* the technologies) and *positively* (seeking sustainable solutions to the conflict and building effective non-violent rules and systems for political and other forms of competition).

CONCLUSION

Civil conflicts will likely remain on the international agenda for some time. The international community must pay more attention to the growing use of digital technologies by conflict parties in these settings. As noted, it is in these contexts, in particular, that societies are more vulnerable and likely to be more affected by the misuse of digital technologies. It is also in these contexts that all actors – state and non-state, internal and external - have significant responsibilities, although these have not yet been fully articulated or recognised.

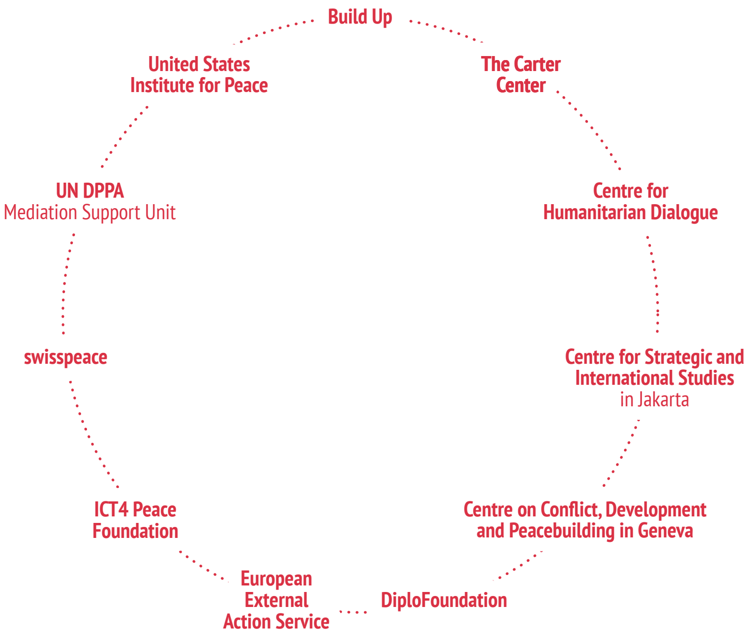
As a consequence, peacemakers must integrate a more sophisticated analysis of technological factors into their broader analysis and engagement strategies. As a first step, this should include an analysis of digital technology use by conflict parties and the relevant implications for peacemaking; an understanding of how existing international law and norms apply to conflict actors and their uses of digital technologies; and a survey of the stakeholders directly or indirectly involved, including technology companies. To this end, organisations with strong preventive mandates could initiate discussions with experts from the cybersecurity, conflict, international law/policy and technical communities to address the basic assumptions highlighted in the framework laid out in the table on page 4. Any consideration of its elements should bear in mind the digital ecosystem of the context in question, the dynamic character of a conflict and a mediation process, and the fact that the factors outlined in the framework also change in tandem with these dynamics.

In addition, further research is needed on:

- Trends in digital technology use by conflict parties in ongoing civil conflicts.
- Practices in moderating the social media behaviour of conflict parties and recommendations for peacemakers for approaching such behaviours within a broader mediation strategy when there is an opening for negotiations (e.g. 2-3 paradigmatic case studies covering events that could drive escalatory behaviours such as an election; a political dialogue; negotiations leading to a ceasefire arrangement; or negotiations leading to a broader peace settlement);
- Offensive cyber operations in *internationalised* civil conflicts and implications for peacemaking, with specific emphasis on third party (States or their proxies) deployment of cyber and information operations or provision of related services in support of one or other conflict party, the norms or principles that apply in such cases, and how these behaviours might be considered in a mediation strategy.

Cyber Mediation Network

Members


Build Up
The Carter Center
Centre for Humanitarian Dialogue
Centre for Strategic and International Studies in Jakarta
Centre on Conflict, Development and Peacebuilding in Geneva
DiploFoundation
European External Action Service
ICT4 Peace Foundation
swisspeace
UN DPPA Mediation Support Unit
United States Institute for Peace

Finally, high-quality, evidence-based analysis and research must be the standard. While there is increasing evidence of digital technology's disruptive role in conflict settings, empirical research on the associated implications for peacemaking remains sparse. Operational guidance for peace practitioners is even more scarce, with the UN/HD Centre *Digital Technologies and Mediation in Armed Conflict* report and *Toolkit* among the few practical resources available to date.[41]

The recently established Cyber Mediation Network can serve as an important starting point for fielding key research questions to the academic community.[42] In the immediate term, the Cyber Mediation Network and individual members of the Network can be leveraged to raise awareness and develop analytical and guidance material for policymakers and practitioners working in the field of mediation/ conflict resolution; and possibly organise a bi-annual conference on digital technologies and other emerging technologies as they relate to civil conflicts and mediation/conflict resolution. These efforts alone will not suffice. Social media and relevant technology companies will also need to shift from their current reactive posture to one more grounded in prevention, starting with more effective engagement with these and other mediation actors.

References

[*] The author wishes to extend her thanks to the Swiss Federal Department of Foreign Affairs for supporting the initial work that led to this Brief and to the European Union Institute for Security Studies for seeing it through to publication. The author also wishes to thank the many colleagues who provided feedback, anonymous and otherwise, on earlier versions of the text.

[1] In this section of the Brief, peacemaking refers to: good offices, mediation, facilitation, dialogue processes or arbitration as well as a number of preventive measures such as conflict early warning, fact-finding, confidence-building measures, early deployment, humanitarian assistance, and demilitarised zones, as per Art. 99 of the UN Charter and the UN Secretary-General's 1992 report, *Agenda for Peace*.

[2] Adam Day and Jessica Caus, ”Conflict Prevention in the Era of Climate Change: Adapting the UN to Climate-Security Risks”, United Nations University, 2020.

[3] According to the final report of the UNITA Monitoring Mechanism, the UNITA 'representative' in Ireland, Mr. Leon Dias, was responsible for organising UNITA's communications network, including its satellite and internet capabilities. In particular he was responsible for procuring and installing communications equipment at Andulo and Bailundo throughout 1997, the latter aimed at enhancing UNITA's radio communications inside the country.

[4] UNITA Monitoring Mechanism Report on the "Use of Electronic Technology - Internet and Email".

[5] The latter included a review of the contractual terms and conditions for website use of several major communications systems providers, leading the Committee to make use of Fujitsu's 'Conditions for Website Use' based on the US Departments of Treasury and Commerce export prohibitions and related sanctions. Having defined a website as an "asset", the two Departments had issued specific prohibitions "making the exportation or use of such technologies to any country or entity against which the United States has imposed sanctions, including UNITA, a criminal offence."

[6] UN Security Council Presidential Statement, "Security Council Sees Need to Improve Effectiveness of Sanctions on Rebel Group in Angola", (PRST SC/7215), November 15, 2001. See, in particular, the intervention of the government of Bangladesh, http://www.un.org/press/en/2001/sc7215.doc.htm.

[7] Ibid. (p.21-22). See also David Lanz and Ahmed Aleiba, "The Good, The Bad and The Ugly: Social Media and Peace Mediation", Swisspeace, *Policy Brief* no. 12/2018, https://www.swisspeace.ch/assets/publications/downloads/Policy-Briefs/aa3fc8830f/Social-Media-and-Peace-Mediation-Policy-Brief-12-2018.pdf.

[8] Thomas Zeitzoff , "How Social Media is Changing Conflict", *Journal of Conflict Resolution*, vol. 61, no. 9, 2017, pp. 1970-1991.

[9] Ibid. p. 15.

[10] See Stefania Milan, *Social Movements and their Technologies. Wiring Social Change* (Palgrave Macmillan, 2013); see also Camino Kavanagh, "The Limits of Dissent in Cyberspace", Policy Brief for the Annual Cyber Dialogue, Citizen Lab, University of Toronto, https://cyberdialogue.ca/wp-content/uploads/2012/2012briefs/brief-2.pdf.

[11] Ibid.

[12] Ibid. See also Evgeny Morozov, *To Save Everything Click Here* (London: Penguin Books Ltd, 2013).

[13] Email exchange with mediation expert, December 2017.

[14] Examples in Syria (e.g. assassination of Zahran Alloush, leader of Jaysh al-Islam by a Russian drone strike) and in the Israel-Palestine conflict. Email exchange with mediation expert, December 2017.

[15] Ibid.

[16] Nathaniel Gleicher and Daniel Agranovich, "Removing Coordinated Inauthentic Behavior from France and Russia", Facebook, December 15, 2020. For media coverage of Facebook's decision, see: François Reynaud, "Facebook met fin à une opération d'interférence en Afrique émanant « d'individus liés à l'armée française", *Le Monde,* December 15, 2020.

[17] Ronald Deibert et al., (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press) 2008.

[18] Sebastian Hellmeier, "The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes", *Politics & Policy*, vol. 44, no. 6, 2016.

[19] OHCHR, "Sudan: UN experts denounce Internet shutdown, call for immediate restoration", July 8, 2019.

[20] Anita R. Gohdes, "Studying the Internet and Violent Conflict", *Conflict Management and Peace Science.*, vol. 35, no. 1, October 2017. See also S. Kane and G. Clayton, "Cyber Ceasefires: Including cyber operations in arrangements to stop armed hostilities" (forthcoming, 2021, CSS ETH Zurich).

[21] Inskikt Group, "Underlying Dimensions of Yemen's Civil War: Control of the Internet", November 2018; See also Jakub Dalek et al., "Information Controls during Military Operations: The case of Yemen during the 2015 political and armed conflict", ICLab, 2015.

[22] Op.Cit., "Information Controls during Military Operations".

[23] Ibid.

[24] Herb Lin, "Fundamentals of Cyber Conflict", Lecture at Stanford University, 2017. Lin describes offensive cyber activity attack as elements of so-called 'cyber weapons' (for want of a better term), which increasingly form part of offensive cyber operations.

[25] Chris Bronk, "Kalashnikov Cyberwarfare: What capabilities and coalitions may emerge in war's new front?", *Medium*, October 20, 2020.

[26] Ibid.

[27] See for instance,”Cyber Ceasefires”, op. cit.

[28] Laurent Gisel, Tilman Rosenhäuser, and Knut Dörmann,, "Twenty Years on: International Humanitarian Law and the protection of civilians against the effects of cyber operations during armed conflicts", *International Review of the Red Cross,* September 2020.

[29] This could include, for instance, states that either party relies on for the supply of weapons, a third party with which the state party has signed military agreements (e.g., troop defence, air-defence etc. agreements), a third party that is reliant on the state party for resources (oil, gas) and thus has an interest in providing protection of the relevant infrastructure, including information infrastructure, and so forth.

[30] See reports of the UN Groups of Governmental Experts, or relevant CBMs adopted by regional organisations such as the OSCE.

[31] United Nations Guidance for Effective Mediation, *International Law and Normative Frameworks*, 2012, pp. 16-17, https://peacemaker.un.org/sites/peacemaker.un.org/files/GuidanceEffectiveMediation_UNDPA2012%28english%29_0.pdf.

[32] See Camino Kavanagh and Paul Cornish, "Cyber Operations and Inter-State Conflict and Competition: The Persisting Value of Preventive Diplomacy", EU Cyber Direct, September 2020.

[33] UN General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *UN document A/70/174*, July 22, 2015; and UN General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *UN document A/68/98**, June 24, 2013. Further discussion on how existing rules and principles of international apply to the use of ICTs by States is currently under discussion in the UN Open Ended Working Group and UN Group of Governmental Experts.

[34] See for instance, public statements by France and Australia on the international law applicable to cyber operations as well as Tallin Manuals.

[35] Op. Cit., "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *UN document A/70/174,* Section III.

[36] On the Paris Call for Trust and Security in Cyberspace, see particularly principles 2, 3, 5, 8 and 9. https://pariscall.international/en/

[37] S. Kane and G. Clayton (forthcoming 2021) have made an important contribution to the literature in this regard.

[38] United Nations Department of Political and Peacebuilding Affairs and the Centre for Humanitarian Dialogue, *Digital Technologies and Mediation in Armed Conflict*, March 2019, https://peacemaker.un.org/sites/peacemaker.un.org/files/DigitalToolkitReport.pdf; See also, https://www.hdcentre.org/publications/mediation-practice-series-peacemaking-and-new-technologies/

[39] A recent workshop co-organised by UNDPPA's MSU and Swisspeace discussed different approaches to approaching the social media behaviours of conflict actors, and associated challenges. The Geneva-based HD Centre is piloting a new initiative in this area.

[40] See FIRST's "ethicsFirst: Ethics for Incident Response and Security Teams", https://www.first.org/global/sigs/ethics/ethics-first-20191202.pdf.

[41] The author of this Brief has served as senior advisor to UNDPPA in the development and roll-out of the Toolkit.

[42] The Cyber Mediation Network brings together key multilateral and non-governmental organisations to discuss the opportunities and challenges of digital technologies across a growing range of topics relevant to mediation and conflict resolution.

Published by the EU Institute for Security Studies
and printed in Luxembourg by the Publications Office of the European Union.
Cover image credit: Arthur Edelman/unsplash

PRINT
ISBN 978-92-9198-993-5 CATALOGUE NUMBER QN-AK-21-004-EN-C ISSN 2599-8943 DOI 10.2815/80745
ONLINE
ISBN 978-92-9198-992-8 CATALOGUE NUMBER QN-AK-21-004-EN-N ISSN 2315-1110 DOI 10.2815/845653