PRINCIPLES *for* PEACE

A new path to lasting peace

The Digital Space and Peace Processes

A Thought Piece

May 2022

BY: Lisa Schirch
University of Notre Dame/Toda Peace Institute

FONDATION HIRONDELLE
media for peace & human dignity

ICT for peace foundation

Contents

This brief informs the Principles for Peace (P4P), a global participatory initiative to develop a new set of principles, standards and norms to fundamentally reshape how peace processes are structured, sequenced, and actualized. Recognizing that over half of formal peace agreements fail to sustain peace, the P4P explores a multidimensional model. P4P's Peacemakers' Covenant defines legitimate peace as requiring sustained long-term processes to transform state-society and intergroup relations through locally led, inclusive, and pluralist governance as well approaches based on a partnership compact between national and international actors.[1]

This brief is a result of a series of interviews and a workshop organised through the thematic track of digital space and peace co-convened with Fondation Hirondelle and ICT4Peace Foundation. Beyond informing the P4P iterative process, it also identifies a menu of thematic tracks for the Swiss government to promote while participating as a non-permanent member on the Security Council.

1 See https://principlesforpeace.org/

Introduction

Digital spaces bring both risks and opportunities to peace processes from Zimbabwe to Venezuela from Ukraine to the US, and from Sri Lanka to Syria.

This paper begins by describing hybrid information ecosystems and their role in sustained peace processes. Public interest news media is essential for democratic decision-making and successful peace processes. Digital media interacts with legacy media, such as radio, television, and newspapers. Ultimately, solutions require supporting both online and offline public interest news media.

Digital risks to sustained public peace processes likely outweigh the current contributions of the digital space to peace.

Next the paper maps digital risks. Both state and non-state political actors are weaponizing tech platforms which by their very design tend to amplify divisive and antagonistic content. The digital space can dramatically increase risks by enabling the rapid spread of false information aimed at undermining an election or referendum. Digital risks likely outweigh the current contributions of the digital space to peace, as illustrated in a variety of case studies in this paper.

This brief then reviews how digital tools and spaces can contribute to sustained public peace processes. This section explores conflict analysis, information ecosystem analysis, planning interventions, and a review of the types of digital tech tools and approaches useful for peace processes. New digital forms of communication can scale public inclusion and improve efficiencies in peace processes. Digital spaces can transform how people share information and communicate with one another. Digital spaces can offer more inclusive and equitable avenues for participation and can incentivize the development of policy options.

The final section of the paper identifies trade-offs and dilemmas, practical strategies for analysing and intervening in digital spaces, and policy recommendations to governments, tech companies and civil society groups on a variety of themes.

A Note on Hybrid Information Ecosystems

In this paper, digital spaces and legacy media spaces coexist within a hybrid information ecosystem. Legacy media now produce and broadcast in digital spaces. Legacy media can also use digital information such as a post on social media as a source of information for a news story in newspapers, radio, or TV. Online and offline media reinforce each other, if there is false or deceptive information on social media, this can bleed over to radio or TV, and vice versa.

The digital space is unique from legacy media. Digital information travels faster, further, and more quickly than information on legacy media. Digital spaces can transform how people share information and communicate with one another. These digital affordances offer new possibilities for scaling public engagement, improving collaborative multi-stakeholder decision-making, and supporting elements of sustained public peace processes.[2]

2 Schirch, Lisa. 'Digital Information, Conflict and Democracy'. In *Social Media Impacts on Conflict and Democracy: The Techtonic Shift*, edited by Lisa Schirch, 1st ed. Sydney: Routledge, 2021.

Digital affordances enable individuals to create user-generated content and to endorse information, including false, deceptive, and polarizing information.[3]

Digital amplification of false and distorted information can quickly sway public opinions about the prospects for peace and cause massive disruptions in democratic processes such as referendums or elections. Digital technologies can amplify polarisation, disinformation, and discrimination patterns fuelling conflict dynamics.

These distinctions affect the quality of the information, and the level of accountability for unverified information. As a tool, social media lends itself to unverified information, as in most countries technology companies are not held accountable for hosting hateful or false information. Public-interest oriented legacy media can provide opportunities to provide accurate information on trusted media sources to counter viral mis/disinformation online. Legacy media are bound to professional journalism standards, while content on social media is not.

Public interest media is essential to sustained peace processes and the healthy expression of conflicts within a democratic system.

Public interest media is essential to sustained peace processes and the healthy expression of conflicts within a democratic system. Democratic discussions and decision-making are difficult if the public consumes false, deceptive, or divisive information on either legacy media, digital media or both. Ultimately, creating information ecosystems the provide the public with verified information on both legacy news media outlets and in digital spaces is essential. The newly launched International Fund for Public Interest Media (IFPIM), headed by Nobel Peace Prize winning Filipino journalist Maria Ressa, recognizes the urgency in addressing information ecosystems both for democracy, and for the prevention of violent conflicts relevant to sustained peace. [4]

3 Lisa Schirch. "The techtonic shift: How social media works" in *Social Media Impacts on Conflict and Democracy*. Edited by L. Schirch. (Sydney: Routledge, 2021).

4 See https://ifpim.org

Digital Risks to Sustained Public Peace Processes

Digital technologies pose at least six risks or challenges to peace processes. With low barriers to access and use, both state and non-state actors weaponize digital technologies, compromising the access to and integrity of information and undermining the ability of stakeholders to communicate safely and effectively. Digital authoritarianism is trending globally, with powerful leaders hijacking technologies to undermine democratic norms.

This section of the report outlines the digital risks and offers key examples or case studies. The first two categories of digital risks relate to big tech platforms' infrastructure, design, and profit models. The risks described in points 3-6 relate to the weaponization of digital technology in a widening playbook of digital authoritarianism.

01. Amplifying Polarization, Discrimination, and Extremism

There are widespread reports of social media platforms amplifying polarization, hate, and extremism in virtually every country. News reports of digital impacts on polarisation and democratic processes are widespread in Europe and North America.[5] While there is less attention to the Southern Hemisphere, local journalists and analysts are finding that social media is also impacting countries across Africa, Asia, and Latin America.[6]

Many platforms' profit models drive conflict. Platforms that offer users free access do so in exchange for collecting or extracting private information about users' beliefs and preferences. These companies then sell ads tailored to individual users based on this data. The profit models guide the design of their platform offerings, such as the newsfeed or recommendation features, and the algorithms that run them, to engage and maximize users' attention. User engagement translates to greater profit in what is known as the "attention economy." These algorithms and affordances create two dynamics that drive conflict.

First, affordances and algorithms show users information that most likely *reinforces their current beliefs and biases* rather than showing them diverse, reliable, and fact-based sources of information. While research is inconclusive, many suspect such "*filter bubbles*" amplify ideological and identity group polarisation.

Second, algorithms are not morally neutral. Algorithms reflect the biases and prejudices of the people that create them. Researchers have found algorithms tend to reinforce discrimination along identity lines, including race, gender, ethnicity, class, and so on.[7][8]

Third, algorithms amplify posts with high levels of engagement, as these increase profit. Some studies suggest false information spreads six times faster than true information.[9]

5 Paul M. Barrett, Justin Hendrix, and J. Grant Sims. "Fueling the Fire: How Social Media Intensifies U.S. Political Polarization and What Can Be Done About It." New York University. September 2021.

6 Schirch, 2021.

7 Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. The Crown Publishing Group, 2016.

8 Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge, UK; Medford, MA: Polity, 2019.

9 Karen Kaplan, "On Twitter, Fake News Spreads Faster and further than Real News - and Bots Aren't to Blame," *Chicago Tribune Online*. 2018.

Reports from Facebook's internal research indicated that algorithms amplified emotional and inflammatory posts because they tend to generate greater user engagement.[10] Because conspiracies and extremist content are often inflammatory, researchers have repeatedly found that tech platforms' own algorithms amplify extremism[11] and generate hate. The "Stop Hate for Profit" movement calls on big tech to change its algorithms.[12]

Digital amplification of polarization, discrimination, and extremism pose significant threats to democratic elections and peace processes aimed at preventing, reducing, or ending violence. For example, in a country with multiple religious and ethnic groups, digital communication may exacerbate fragile intergroup relationships.

02. Disrupting the Financial Viability of News Journalism

Large digital platforms disrupt the digital revenues and financial viability of news outlets that follow professional journalist ethics.

First, digital spaces republish news, drawing people away from paid subscriptions to news channels. This takes funding away from the time-consuming work of professional journalism, which includes commitments and responsibilities for accuracy, verification of sources, fairness to represent multiple points of view, and thoroughness to explain enough of the wider context of a story.

Second, advertisers have moved their ads away from legacy media outlets with more general audiences toward digital news sources that track user profiles, enabling advertisers to target ads to specific audiences. Around the world, legacy news outlets are closing or reducing their journalism coverage. This trend shrinks public access to verified information necessary for democratic elections and public participation in inclusive governance.[13]

Digital disruption of news journalism's financial viability poses a threat to public interest journalism where peace processes take place. Public interest media is essential to helping policymakers and the public navigate through a peace process. For example, if people stop buying newspapers with public interest journalism and instead rely on unverified digital information sources, a sustained peace process may be vulnerable to false information.

03. Waging Cognitive Warfare and Epistemic Insecurity

Digital technologies disrupt information ecosystems in a variety of ways.

First, while news editors in legacy media control information that is deemed newsworthy, digital technologies democratize who has access to share text, photos, and videos. While democratic access to social media channels for sharing information such as citizen reports on government corruption can have positive impacts, malicious actors weaponize technologies to spread hateful or false information.

Second, political actors can use digital technologies to distract public attention. *Strategic distraction* disrupts the information ecosystem by flooding digital news platforms with personal interest stories that confuse and distract the public from engaging in political discourse.

Third, political actors can spread false or deceptive information to alter political beliefs or behaviours. *Information pollution* makes it more difficult for the public to distinguish between fact from fiction. By provoking a sense of chaos and uncertainty,

10 Keach Hagey and Jeff Horwitz, "Facebook Tried to make its Platform a Healthier Place. it Got Angrier Instead. Internal Memos show how a Big 2018 Change Rewarded Outrage and that CEO Mark Zuckerberg Resisted Proposed Fixes," *The Wall Street Journal Online*. September 15, 2021. https://global.factiva.com/en/du/article.asp?accessionno=WSJO000020210915eh9f002mh.

11 "Reps. Malinowski and Eshoo Reintroduce Bill to Hold Tech Platforms Accountable for Algorithmic Promotion of Extremism." *Congressional Documents and Publications*. 2021.

12 https://www.adl.org/stop-hate-for-profit-0

13 Rasmus Kleis Nielsen, Alessio Cornia and Antonis Kaleogeropoulos, *Challenges and Opportunities for News Media and Journalism in an Increasingly Digital, Mobile, and Social Media Environment*. Council of Europe: Reuter, 2016.

political actors contribute to "*epistemic insecurity*" where the public no longer can discern what to believe or how to behave. In this collapse of truth, authoritarian control and manipulation over the public becomes possible.

Drawing on decades of off-line propaganda warfare, Russia has experimented in large scale, digital *dezinformatsya* campaigns run by government-paid 'troll farms' to divide and destabilize democracies like its neighbours and further in the West. The University of Oxford's program in Computational Propaganda estimates that dozens of countries are setting up cyber units to control and manipulate information.[14] NATO guidance suggests this social media-based "cognitive warfare" undermines human capacities for critical thinking and agency.[15] Information disorders are likely to play a significant role in undermining democratic decision-making processes, including elections and peace processes. On the eve of an election or referendum, or during a delicate mediation, for example, the spread of false or deceptive information might have a dramatic effect on conflict dynamics. Even in countries where there are fact-checking systems in place, these are still relatively slow, weak, and have not been able to counteract false information in places like the US, where election disinformation during the 2016 and 2020 elections significantly altered conflict dynamics in the country.

The "borderless" nature of the internet means that actors based in one jurisdiction can plant mis/disinformation in other jurisdictions, making oversight and accountability to laws and standards extremely difficult, if not impossible.

Digital strategies to wage cognitive warfare through false information and the collapse of truth pose a threat to peace processes that require public trust. For example, a false post about what is being discussed in a peace process could cause public panic or even lead to violence. Without trust in verified information sources, the public may either lose interest or actively oppose a peace process.

04. Digital Access, Net Neutrality, and Internet Shutdowns

Many scholars and practitioners argue the internet should be treated as a public utility. It is difficult for any person or small business to function as a member of society without digital access. A free and open internet is necessary for an empowered public to access information and communicate, preconditions for sustained peace. Yet the digital divide persists. Large parts of the world's population do not have access to digital technologies. The digital gap increases existing inequalities between poor and wealthy, literate and illiterate, urban and rural and between people of different gender identities.

Digital access also suffers because of a lack of *net neutrality*, the principle that internet access should be offered to everyone on a non-discriminatory basis, without favouring certain websites, applications, or services. Political and economic forces disrupt free public access to the internet, prioritize paid ads or profit-oriented information on internet searches, and block some information sources and/or push government information sources.[16]

Meta, formerly known as Facebook, launched a program known as "Free Basics" to increase digital access to the internet. In many countries today, Facebook and other Meta programs are preloaded on mobile phones. Local users access selected "free" sources of information on the internet through Facebook. However, as mentioned above, Meta uses algorithms to tailor news feed to users pre-existing beliefs, so these seemingly free sources of information can contribute to further polarisation and conflict Repressive governments leverage their relationship with Facebook to ensure the platform censors some news sources.[17] For example, in Vietnam, the government told Facebook it could only operate in the country if the company censored some political content on the platform.[18]

Internet shutdowns are a new weapon of

14 Samuel C. Woolley and Philip N. Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. New York: Oxford University Press, 2018.

15 François du Cluzel, *Cognitive Warfare*. Brussels: NATO Innovation Hub, 2020.

16 Deji Olukotun, *How's Your Country on Net Neutrality?* 2015.

17 Justin Scheck, Tom McGinty and Newley Purnell, "Facebook Promised Poor Countries Free Internet. People Got Charged Anyway." *Wall Street Journal* 24 January 2022. https://www.wsj.com/articles/facebook-free-india-data-charges-11643035284.

18 Reuters Southeast Asia, "Vietnam Tells Facebook: Yield to Censors Or we'll Shut You Down, Source Says," *VOA*. 20 November, 2020. https://www.voacambodia.com/a/5670180.html.

authoritarian governments to silence their critics and punish citizens. The global movement known as *Access Now* documented at least 50 internet shutdowns in 21 countries in the first half of 2021.[19]

Digital access and net neutrality may be especially important in a sustained peace process which relies on an informed public. If internet access is not available, it may be more difficult for citizens to share information or communicate with each other about public issues.

05. Privacy and Mass Surveillance

The U.S. Department of Defense created the first model of the internet in the 1960s. Working with academic institutions, corporations, and a group of progressive activists and libertarians, the US military saw the potential of the internet to enable intelligence collection to help them identify threats.[2021] Today, governments, political actors, and technology companies themselves obtain vast troves of personal data from digital technologies. In countries like China and Venezuela, governments are experimenting with mass surveillance, biometric identity markers, and vast social control programs.[22] The pandemic also actually increased the accuracy of facial recognition programs to be able to identify masked persons. Citizens may be tracked for what they say on social media and either rewarded or punished based on their behaviour. Doxxing, the sharing of private information with digital technologies, can lead to mob violence against individuals. Given widespread attention to internet privacy breaches, citizens may also self-censor themselves on social media for fear of possible repercussions.[23]

During a polarized policy discussion, election, referendum, or peace negotiation, privacy concerns may threaten key leaders, silence vulnerable populations from voicing their opinions, or leak sensitive information. In Ukraine, for example, the doxing of private information of journalists led to threats against them.[24] Doxxing information about mediators, or conflict stakeholders who are meeting with mediators, could be dangerous both to the individuals involved and to a delicate negotiation process.

Privacy and mass surveillance are relevant to a sustained peace process because mediators, key leaders or influencers may be identified and traced on digital devices. Spoilers motivated to undermine a peace process may be able to use digital tracking to organize digital or physical attacks on key people central to a peace process.

19 Marianne Diaz Hernandez et al., *#KeepItOn Update: Who is Shutting Down the Internet in 2021?* Access Now, 2021.

20 Walter Isaacson, *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution*. New York: Simon & Schuster, 2014.

21 Yasha Levine, *Surveillance Valley: The Secret Military History of the Internet* (New York: PublicAffairs, 2018).

22 Iria Puyosa, "Venezuela: 21st Century Authoritarianism in the Digital Sphere," in *Social Media Impacts on Conflict and Democracy: The Techtonic Shift*, ed. Lisa Schirch. Sydney: Routledge, 2021.

23 Ekaterina Zhuravskaya, Maria Petrova and Ruben Enikolopov, "Political Effects of the Internet and Social Media," *Annual Review of Economics 12*, no. 1. 2 August, 2020. 415-438. doi:10.1146/annurev-economics-081919-050239. https://www.annualreviews.org/doi/10.1146/annurev-economics-081919-050239.

24 *Ukraine: Law Enforcement and Policymakers should Take Swift Action to Protect Journalists* (Washington, D.C: Freedom House, 2020.

06. Cybersecurity and Malware Attacks

Conflict actors can weaponize digital technologies in a variety of ways. *Cybertheft* involves taking information or property. *Denial of service* attacks prevent the use of digital technologies such as bank machines or computers. *Wiper-ware* deletes data and shuts down computerized programs. *Malware* can corrupt or infect government agencies, potentially disrupting electric grids, water systems, nuclear power plants, healthcare facilities, train signals, and countless other digitized elements. Fears of a cyber-Hiroshima or a cyber-9/11 evoke images of a mass attack leading to large scale casualties from nuclear meltdowns, train crashes, exploding pipelines, or widespread incapacitating electric shutdowns.

Cybersecurity attacks can undermine a peace process. For example, the Cyberpeace Institute has put together an extensive timeline of ongoing Russian cyberattacks on Ukraine.[25] Such cyberattacks seek to debilitate the country, destabilize the government, and manipulate public opinion through cognitive warfare. Such cyberattacks could undermine any form of democratic decision-making or public peace process.

25 Cyberpeace, *Ukraine: A Timeline of Cyberattacks*, 2022. https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

Digital Opportunities to Support Peace Processes

The digital space also offers a range of tools and opportunities that have the yet-unrealized potential to dramatically scale and improve our ability to understand the drivers of conflict as well as how to support a sustained peace process. Big technology companies as well as smaller tech start-ups are designing new affordances to limit digital risks and contribute to peace. International organizations, states, civil society groups and social movements are leveraging digital spaces to support elements of sustained peacebuilding.[26]

This section of the report outlines the opportunities for digital spaces first for our analysis of conflict and information ecosystems, and then for how peace organizations go about designing and intervening in conflict with digital tools. Planning peace interventions should always begin with conflict analysis. While analysing information ecosystems of online and offline sources has not previously been integrated into conflict analysis processes, it is now urgent given the information disorders detailed earlier in the paper.

Digital Conflict Analysis

Digital technologies are contributing new methods of collecting data for conflict analysis, which is a research process essential to planning effective peace efforts. Conflict analysis gathers information about the "who, why, how, what, where, and when" elements of a conflict. *Who* are the stakeholders, or the people affected by a conflict? *Why* are they motivated to pursue their positions, interests, and needs? *How* are they mobilizing power to achieve their goals? *What* types of tactics or behaviours are they using? *Where* are the spaces where people engage across the lines of conflict? When are their windows of opportunity or vulnerability in the present and future given the historical narratives of traumas or glory?[27]

Digital conflict analysis tools include geospatial information systems such as satellites or drones, surveillance cameras, social media and internet data scraping, AI for sentiment analysis, crowdsourcing, public surveys, and tools for citizen journalists who document conflict dynamics with digital video, photos, audio, and text. These tech tools can significantly expand information about conflict dynamics, particularly in regions difficult to reach because of security challenges, difficult terrain, or in humanitarian emergencies.[28]

There are at least two challenges of digital data collection. First, often big data produces quantity, but not quality information. As detailed earlier, some forms of digital information are difficult to verify, and may in fact be "information pollution" that adds confusion rather than clarity to conflict analysis. Artificial intelligence (AI) programs are rapidly increasing the ability to sort through big data sets to reduce the "noise" of too much information, and uncover trends, patterns, or critical pieces of information that can help people make meaningful assessments.

---

26 This report draws on a variety of reports on digital peacebuilding, including the following: David Lanz and Ahmed Eleiba. "The Good, the Bad, and the Ugly: Social Media and Peace Mediation." Swisspeace Policy Brief 12. 2018. Lisa Schirch. "25 Spheres of Digital Peacebuilding and Peacetech." Tokyo: Toda Peace Institute, 2020. "Smart Prevention: Digital Approaches in the Peace and Security Sector of Development Cooperation." Germany: GIZ, 2020.

27 Lisa Schirch, *Conflict Assessment and Peacebuilding Planning: Toward a Participatory Approach to Human Security*. Boulder, Colorado: Kumarian Press, 2013.

28 Patrick Meier. "Early Warn Systems and the Prevention of Violent Conflict." In Peacebuilding in the Information Age. Edited by D. Stauffacher, B. Weekes, U. Gasser, C. Maclay and M. Best. ICT4Peace, Berkman Center for Internet and Society, and Georgia Institute of Technology, January 2011.

A second challenge relates to ensuring the privacy of data. Collecting information on sensitive information or vulnerable populations may inadvertently increase digital risks to vulnerable populations and conflict dynamics. Blockchain technologies might be able to assist in keeping such sensitive data secure.[29]

There are a wide variety of data collection, processing, and visualization programs available.[30] For example, the United Nations uses an E-Analytics toolkit, sponsored by the UN Department of Political and Peacebuilding Affairs, Global Pulse and other partners since 2017.[31] One tool is Crimson Hexagon used by the Middle East Division to conduct Natural Language Processing (NLP) for Arabic dialect sentiment analysis and opinion mining. Dataminr uses AI, machine learning, and NLP to detect outbreaks of violence or conflict events through social media and blog analysis to detect, qualify and classify public information.[32] UN Global Pulse created a tool called Qatalog to extract, analyse, and visualize data gathered from radio broadcasts, Facebook and Twitter posts and private sector data providers.[33]

Analysing Information Ecosystems

Effective use of digital tools to support peace begins with analysing information ecosystems. For many decades, conflict analysis and context assessment tools have been essential to developing effective peacebuilding and development programs.[34] Growing polarization and state-sponsored disinformation campaigns highlight the need to add an analysis of information ecosystems and how digital spaces and their interaction with offline spaces may be driving conflict or offering new spaces for peace processes. Each context has a unique information ecosystem, and a unique set of conflict dynamics. The process for analysing and designing digital interventions to support peace includes a variety of stages or approaches.

Broader Information Ecosystem Analysis

1. What are the sources of information used by local people (disaggregated by gender, age, race, religion, or other relevant identity markers) to understand conflicts or political issues (e.g. word of mouth, community radio, national radio, print news media, television, social media)?
2. How do local people perceive the reliability of their information sources?
3. What languages and dialects are spoken online and offline? What level of cultural, religious, ethnic, gender, age, and other forms of diversity do local journalists represent?
4. What is the level of professionalism and technological capacity among relevant journalists in the local context? Are they capable of facilitating democratic deliberation with public input?
5. What is the regulatory or normative context of laws or restrictions on legacy media, social media or the broader rules on freedom of speech and privacy?
6. Who owns local news outlets and what profit model guides editorial decision making.

29 United Nations, *Digital Technologies and Mediation in Armed Conflict*. Helsinki: Department of Political and Peacebuilding Affairs; Centre for Humanitarian Dialogue, 2019.

30 Branka Panic, *Data for Peacebuilding and Prevention Ecosystem Mapping: The State of Play and the Path to Creating a Community of Practice* (New York: NYU Center on International Cooperation, 2020.

31 Global Pulse, *E-Analytics Guide: Using Data and New Technology for Peacemaking, Preventive Diplomacy and Peacebuilding* (New York: United Nations, 2019).

32 https://www.dataminr.com/technology

33 https://www.unglobalpulse.org/microsite/qatalog/

34 Lisa Schirch. *Conflict Assessment and Peacebuilding Planning: Toward a Participatory Approach to Human Security*. Lynne Rienner Press, 2013.

Social Media Analysis

1. How relevant is social media in the local context (community, city, region, or country)?
2. What social media channels are most popular in the local context and why? This can define data sources for further analysis with specific digital tools (described in a separate box).
3. Who are the digital influencers, or who is leading the debate on social media, how, and why?
4. Where do digital information sources originate?
5. Is a social media post authentic, or from a bot, profit-motivated individual, or political actors using coordinated inauthentic accounts?
6. What are the key issues, the key hashtags, memes, terms (including symbols or metaphors to hide hate speech) or social media campaigns?

Tools for Social Media Analysis

There are a variety of new tools for conducting social media analysis. There are many free and corporate social media analysis tools available. Two tools were specifically designed to support peace processes.

Phoenix is an open-source, non-commercial, customisable process and tool to support peacebuilders and mediators who want to work ethically with social media data to inform programming. It was developed by Build Up. (Found at https://howtobuildup.org/programs/digital-conflict/phoenix/)

The Phoenix process includes the following:

- Contextually grounded problem statements that address peacebuilding objectives
- Data pipeline to add the social media sources you need
- Customisable automatic labeling models to reduce manual organising of data
- Dashboard to visualise engagement, sentiment, and networks
- Evidence-based initiatives that respond to social media insights

Sparrow is a social media analysis tool created by and for UN DPPA (Department of Political and Peacebuilding Affairs) for analyzing Twitter to identify trending topics, hashtags, and key influencers. (Found at https://mysparrowreport.org/about)

Designing Digital Interventions to Support Peace

Two examples illustrate how analyses of information ecosystems contribute to planning interventions to support peace.

A collaborative research project in the DRC analysed sources of information and patterns of information sharing in North Kivu. The research team consisted of Fondation Hirondelle, Demos, Harvard Humanitarian Initiative and ICREDES, the Congolese Research Institute on Development and Strategic Studies.

The analysis included several dimensions. Household surveys of large samples in Eastern DRC provided insight into information sources. Radio is the primary source according to 78% of households surveyed, followed by 31% who follow TV, 19% who follow the written news media, and 26% who rely on digital sources. The surveys found that people in different *contexts* look to different *sources* of information for different *types* of information. In addition, women relied less on radio than men, possibly leading to their increased reliance on informal word of mouth speculation, particularly related to Ebola.

Researchers found that local community radio stations received news from national and international radio stations, followed by social media. While the general population did not have robust access to social media, local journalists did have access to social media, specifically Facebook, Twitter, and WhatsApp. Local journalists used these social media sources to gather information for their radio programs.[35]

The research project included several recommendations for supporting information ecosystems that would support peace.

1. Map and monitor local radio stations and personalities to identify reliable and influential sources of radio programming. Provide capacity building for local journalists to learn how to verify information offline and online.
2. Map and monitor digital influencers including political tweeters, journalists, bloggers and civil society organizations. Support these influencers with training and digital tools to help them to identify disinformation circulating on social media platforms.
3. Support the national Radio Okapi which was described as functioning as a national public broadcaster beyond the MONUSCO peacekeeping mission.
4. Integrate media and information literacy into education programs for the general population.

A second example draws on the NGO Build Up's methodology working in Lebanon, Syria, West Africa and elsewhere. Build Up begins by partnering with a local organization or a cohort of organizations to identify a digital threat or peacebuilding challenge and how technology might help to increase the impact of their work. The partnership begins with participatory research. Mapping local technology use is part of a broader context analysis.36 The local group(s) identify a problem statement about social media and how it is impacting polarization or conflict. Together, Build Up and the local partners define a set of data sources based on what social media platforms are most used in the local context. Next, they collect and label data from these social media sources that can visualize and analyze the themes and issues on the social media platforms.

Build Up then mentors the local group over a period of approximately 6-18 months depending on funding. After an analysis of information ecosystems and determining a central issue driving digital conflict, Build Up advises to design a digital peacebuilding intervention which could include a narrative change program to seed digital conversations with new ideas and frames, or a facilitated digital dialogue.

35 Fondation Hirondelle, Demos, Harvard Humanitarian Initiative and ICREDES. "Influencers and Influencing for Better Accountability in the DRC." July 2019. Found at: https://www.hirondelle.org/en/our-news/1015-study-on-sources-and-circulation-of-information-in-north-kivu-drc

36 Helena Puig-Laurari and Maude Morrison. "Digital Drivers of Conflict." In H. Mahmoudi et al. (eds.), *Fundamental Challenges to Global Peace and Security*. Switzerland: Springer, 2022.

Intervention Planning, Design, and Evaluation

Given the information gathered through analysis of the information ecosystem and social media, what do local stakeholders identify as key issues or drivers of conflict either in legacy media or social media?

Human-centred design begins with local stakeholders discussing priorities that stand out in the information ecosystem and social media analyses. From these priorities, they can then identify options for intervening

Examples of interventions could be:

- Support the connections between verified information from legacy media outlets with online social media news sources and influencers
- Provide training in media literacy to social media influencers, legacy media journalists, and the public
- Provide local journalists training in professional journalism (including verification of information)
- Develop a narrative change program to seed digital conversations with new ideas and frames
- Facilitate spaces for digital dialogue and mediation on relevant social media channels

Most digital peacebuilding interventions are experimental and pilot programs. As there are more efforts to counter hate speech with simplistic campaigns such as #stophatespeech, it is essential to determine if these efforts actually impact conflict dynamics.

Types of Peace Process Interventions and "Peacetech"

Digital technologies contribute to peace processes in a variety of ways. This section of the paper identifies types of technology that can contribute toward different peace process elements.

01. Intergroup Dialogue and Participatory Decision-making

Digital technologies are creating the possibility for hundreds if not thousands of people to contribute qualitative and quantitative input on policy decisions, including elements of peace negotiations. A major issue with using technology to broaden inclusion is that people most marginalized in society often have little to no access to technologies. The digital gap creates a challenge to find ways to help people access technology so that they can then participate in new digital methods of dialogue and decision making.

Two technologies have already been used to foster digital dialogue, enabling policymakers to "listen at scale" to public inputs and preferences on policy trade-offs. The 2014 tech start up Remesh began with the mission to create a technology that would "represent the will of the people and amplify their collective voice." Conflict mediators, civil society groups, or governments can use Remesh to dialogue with and poll the public. Remesh software can extract key themes and draw insights from a dynamic and open-ended "conversation" with up to 1,000 people.[37] The UN used Remesh in Libya to gather stakeholder opinions of a proposed interim government. In Yemen, the UN used Remesh to listen to public perceptions of a cease-fire and opinions on the prospects for a peace process. The UN is now considering using Remesh for peace support in Sudan, Mali, Afghanistan, and Iraq.[38]

Similarly, the Polis platform enables large groups of people to identify areas of consensus and policy proposals that hold majority support. Combining public qualitative inputs with up and down voting by citizen peers, Polis is a form of "computational democracy." Polis has successfully helped to move polarized publics toward social cohesion in a variety of contexts.[39] For example, Taiwan's Digital Ministry has used the Polis platform to address dozens of polarized policy challenges. Polis enabled identifying actionable legislation in 80% of

37 https://www.remesh.ai
38 Fortune Magazine. "Impact 20: Remesh" Change the World list. 2021. Found at: https://fortune.com/impact20/2021/remesh/
39 Josh Smith et al., *Polis and the Political Process*. London: Demos, 2020.

the cases using the platform.[40] The platform could easily be harnessed for use in public discussion of policy trade-offs and options as part of an ongoing peace process in divided societies.

Smaller tech start-ups are designing affordances to enhance virtual face-to-face dialogue. Both Remesh and Polis platforms enable large-scale, but impersonal dialogue. During the pandemic, the use of virtual platforms like Zoom and Webex increased. While such widely used platforms are accessible and easy to use for many people, they were not designed with the explicit goal of intergroup dialogue. The peacebuilding group Soliya[41] has been running digital dialogues for many years on a platform with design features that aim to help build relationships. Newer tech start-ups such as Gatheround[42], Marco Polo,[43] and Kazm[44] offer affordances that enhance human empathy and relationships. Kazm for example, brands itself as a "conversation engine" for "scaling facilitated dialogue." Kazm enables a dialogue facilitator to post dialogue questions, host events, conduct polls, make word clouds from digital comments, and post resources for a group to discuss. Facilitator support helps to provide guidance for navigating difficult conversations.[45]

Several tech start-ups are also exploring how to use virtual reality to foster intergroup dialogue and empathy. The group HackthePlanet[46] offers a variety of programs to build public understanding of other people. The United Nations Department of Political and Peacebuilding Affairs Innovation Cell worked with a tech company called Superbright to create VR programs to help UN decision makers experience an immersive VR conflict environment to better understand the voices of people on the ground.

While digital formats have great potential for further inclusion, they also have some limitations compared to in person format. It may be more challenging to establish the kind of trust to be able to discuss compromises. It may also be difficult to be 100% sure of who else is listening, or what types of surveillance there is in a digital space. While these new technologies can improve public inclusion in long-term peace processes, technology can also further amplify existing patterns of marginalization. For example, the use of Remesh in the Libyan Dialogues did not improve the inclusion of women's voices. Highlighting the voices of marginalized voices required data analysts to disaggregate the views of female Libyans and of ethnic minorities.[47]

02.Mediation and Diplomacy

The delicate work of mediation between groups in conflict is fraught with dangers from digital technology, identified earlier in this paper. Because of the need to build trust and discuss difficult issues, mediation work is best done in person in a safe and private physical location. Given the difficulties of meeting in person because of security risks, crises such as the pandemic, or remote locations of key stakeholders, digital technology offers new possibilities for supplementing or replacing some in-person meetings.

The risks and challenges of digital mediation create new dilemmas and trade-offs. In 2018, a Cyber-Mediation Network launched to provide a community of practice for mediation practitioners to learn about and discuss the risks and opportunities of digital technologies.[48] The UN published a digital toolkit on "Digital Technologies and Mediation in Armed Conflict in 2019.[49] In 2021, Swisspeace and the UN Department of Political and Peacebuilding Affairs (DPPA) co-published a practical framework on using social media in peace mediation.[50] In February 2022, the Cyberpeace Institute, CMI, and the UNPPA Mediation Support Unit launched an E-learning Platform on Cyber Hygiene and Digital Risk Management.[51] The NGO Build Up offers Toolkit on Digital Technologies and Mediation to raise awareness among mediation practitioners of the implications of the use of digital technology in mediation contexts and provide

40 Carl Miller, "How Taiwan's 'Civic Hackers' Helped Find a New Way to Run the Country," *The Guardian*. 27 September, 2020. http://www.theguardian.com/world/2020/sep/27/taiwan-civic-hackers-polis-consensus-social-media-platform.
41 https://soliya.net
42 https://gatheround.com
43 https://www.marcopolo.me
44 https://about.kazm.com
45 "Kazm Scaling Conversations" Presentation at the Alliance for Peacebuilding Community of Practice in Digital Peacebuilding. 18 November 2021. Access at: https://www.youtube.com/watch?v=qwkhc_8jZaI&feature=emb_title
46 https://www.hack-the-planet.io
47 IRCAI - Unesco International Research Centre on Artificial Intelligence. "AI for Peacebuilding." Accessed at: https://ircai.org/top100/entry/ai-for-peacebuilding/
48 https://twitter.com/CyberMediat_net/
49 United Nations, *Digital Technologies and Mediation in Armed Conflict*
50 David Lanz, Ahmed Eleiba, Enrico Formica, Camino Kavanagh. "Social media in peace mediation a practical framework." swisspeace and UN DPPA. June 2021.
51 https://cyberpeaceinstitute.org/news/digital-risk-management-e-learning-platform/

mediators with concrete examples and practical information of how it could impact their work.

Consumer dispute resolution systems such as Modria and private e-mediations and robot mediations have had significant success addressing smaller scale conflicts. A robust literature exists within the Alternative Dispute Resolution field.[52] E-mediators use digital technologies to reality test options with stakeholders, to assess and calculate their options, and to find creative solutions thinking "outside of the box." Some of the e-mediation affordances may be transferable to society-level conflicts. However, to date, there has been little cross-over between mediators working in the consumer, family, and community fields, international diplomacy and the media.

03. Strategic Communication and Public Diplomacy

Digital technologies are useful for governments and civil society to promote inclusive narratives to support intergroup peace efforts. Diplomats and mediators may use social media together with offline media, for example, to explain a policy discussion and its trade-offs, or to provide information on how a public process will work and the speed it will take place. Public diplomacy efforts increasingly take place online, with government officials and civil society influencers using their Twitter and Facebook accounts to make statements on policy issues related to peace.[53] But in conflict-affected contexts, reaching out to the wider and often much less connected population requires synergies with offline media and non-media intermediaries.

04. Peace Education and Peace Narratives

The *Peacemakers' Covenant* recognizes the need for wider public inclusion and civic engagement. Peace education has a long history of preparing diverse stakeholders for constructive communication across lines of conflict to build social cohesion. Peace education requires the promotion of a culture of inclusive and fair dialogue. It is often supported by public interest media that create spaces for diverse stakeholders to represent a variety of viewpoints.

Digital forms of peace education may be able to replicate some aspects of this. Chatbots such as the "CliMate: The Climate Conversation Coach" are useful in teaching communication skills to discuss challenging topics like the climate crisis.[54] IBM's "Project Debater" is an AI system that can debate humans on complex topics. The goal is to help people build persuasive arguments and make well-informed decisions.[55] Video peace games may also foster empathy and appreciation for diverse viewpoints. In 2014, the UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development launched a gaming challenge. They received hundreds of proposals for video games to educate players on peace and sustainable development.[56] In Israel and Palestine, a group called "Games for Peace" is experimenting using video games such as Minecraft to foster dialog and trust between young people in conflict zones.[57]

05. Social Movements

Compared to the exclusivity and cost of legacy media, digital technologies are increasing access to people-powered journalism and social movements. There is a growing literature and set of case studies supporting the synergy between nonviolent social movements and peacebuilding.[58] Negotiations and mediations often stall because of an imbalance of power. Social movements can help motivate all stakeholders to reach a negotiated agreement. Social movements provide a pathway for public inclusion in peace processes. Shifting power may be an essential part of an ongoing, sustained public peace process.[59] As evidenced in global social movements from Mexico's Zapatistas to the Arab Spring, social movements are using a wide variety of technology tools to recruit new

52 Colin Rule, *Online Dispute Resolution for Business*, 1st ed. ed. San Francisco: Jossey-Bass, 2002. http://www.loc.gov/catdir/toc/wiley031/2002072982.html. Colin Rule, "Making Peace at Ebay: Resolving Disputes in the World's Largest Marketplace," *Quarterly Magazine of the Association for Conflict Resolution*. Fall, 2008, 8-11. Amy J. Schmitz and Colin Rule, *The New Handshake* (Lanham: American Bar Association, 2018). https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=5440324 .

53 See Twiplomacy for reports on the usage of Twitter and Facebook by government leaders. https://twiplomacy.com

54 See the David Suzuki Foundation at: https://davidsuzuki.org/climate-conversation-coach/

55 See IBM Project Debater at: https://research.ibm.com/interactive/project-debater/

56 Anamika Gupta, *Beyond the Zombie Apocalypse: Video Games for Peace and Sustainability*. UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development, 2014.

57 http://www.gamesforpeace.org

58 Nadine Bloch and Lisa Schirch, *Synergizing Nonviolent Action and Peacebuilding*. Washington DC: US Institute of Peace, 2018.

59 Véronique Dudouet, *Powering to Peace: Integrated Civil Resistance and Peacebuilding Strategies* (Washington, D.C: International Center for Nonviolent Conflict, 2017.

members, organize events, and develop a narrative about social change.[60]

06. Human Rights Investigations and TRC functions

Sustainable peace processes require mechanisms for documentation of human rights violations, transitional justice, and truth-telling. Digital technologies enable documentation of video, photo, text-based information that preserve information for the historical record that may be helpful for a society to address and deal with the past. Digital information may help to memorialize shifts in public consensus. Digital records can be useful to hold up a mirror to society's past, helping the public reflect on their own history.[61]

Human rights groups now use digital technologies to document violations by searching the internet for digital artifacts that can be used as evidence in criminal justice processes. For example, Amnesty International gathers digital information to document human rights abuses. They gather digital information about a possible mass grave through cell phone images triangulated with satellite images.[62] At the University of Berkeley, California, a new Human Rights Investigation Lab teaches students and human rights defenders how to document abuses with digital technologies.[63]

07. Ceasefire Monitoring and Early Warning of Violence

Digital technologies can also be used to monitor ceasefires or provide early warning of violence. For example, Hala System's Sentry multi-sensor system monitors Syria airspace and gives civilians a warning system for civilians on where bombs might fall and a window of time to seek protection.[64]

Community early warning systems on social media such as Ushahidi, based in Kenya, to map incidences of election-related violence so that early response peace teams could respond immediately. Ushahidi uses both online and offline sources of information to do "activist mapping" and builds bridges between different community members to prevent violence.

60 Nadine Bloch, "From Airtable to Zoom: An A-to-Z Guide to Digital Tech and Activism," *Toda Peace Institute*. April 2021. https://toda.org/assets/files/resources/policy-briefs/t-pb-107_nadine-bloch_from-airtable-to-zoom.pdf.

61 Emma Baumhofer, Bernard F. Reilly Jr. "Open source digital preservation. Guidance for practitioners. Bern: Swisspeace, 2022.

62 Amnesty International, "Digital Evidence: Using New Data Streams in Human Rights Research." Amnesty International, 2016.

63 https://humanrights.berkeley.edu/programs-projects/tech/investigations-lab

64 Louisa Loveluck, "The Secret App that Gives Syrian Civilians Minutes to Escape Airstrikes," Washington PostAug 19, 2018. https://global.factiva.com/en/du/article.asp?accessionno=WPCOM00020180818ee8h001gv

Key Dilemmas

The use of digital space for sustained public peace processes poses a variety of dilemmas and tradeoffs. These include the following:

- **Find the right balance of online and offline approaches:** Most peacebuilding efforts today rely on some form of digital technology, even if it is only email or video conferencing. Digital peacebuilding is not separate from other forms of peacebuilding. It is no longer optional for peacebuilding groups to exclude attention to digital spaces. All peacebuilders must pay attention to how information moves between online and offline channels even in low connectivity environments, and the dynamics of how online communication can contribute to offline violence**.** Hybrid elements of a sustained peace will need to right-size digital approaches to maximize synergy between digital and face-to-face interactions. While digital technologies can increase participation by some groups, it may further marginalize groups with less access to technology and less literacy on how to engage with those tools.
- **Move from digital inclusion to digital agency:** Digital spaces often reproduce and amplify inequities. While conflict analysis strategies might seem "inclusive" by capturing data from local populations, extracting data from local populations without their involvement and oversight can inadvertently disempower local communities.[65] Digital "inclusion" may keep women, gender minorities, and people of colour in a fundamentally marginalized role. The dilemma is to enable digital equity to balance digital inclusion with offline inclusion strategies**.**
- **Beware of tech solutionism while exploring peacetech:** While digital technologies provide new opportunities, they cannot solve fundamental, deep-rooted political, social, environmental, and economic problems that are at the heart of many protracted conflicts.
- **Ensure a people-centred "local first" approach:** Human-centred design processes that focus on local voices and unique local contexts are essential to preventing unintended tech harms. Digital tools can fail if there is not enough focus on local agency and inclusive design processes. External tech experts and peacebuilding advisors can play a role, but if they play too much of a role, they undermine the process and local ownership essential for effective peace processes.
- **Identify the trade-offs between digital accessibility and security.** Greater digital use increases digital risks. The greater the use of digital space to support peace processes, the more likely that spoilers will use digital space to undermine these processes. While widely used digital spaces such as WhatsApp may offer convenience, more secure digital spaces such as Signal may offer more security. Also assess the trade-off between accessibility and increased exposure to mis/dis/malinformation that creates "echo-chambers" and increases polarisation.

65 Julia-Silvana Hofstetter. "Digital Technologies, Peacebuilding and Civil Society." INEF Institute for Development and Peace. University of Duisburg-Essen. 2021.

Recommendations

Reducing digital risks and improving digital contributions to sustained public peace processes will require attention to at least four areas, outlined here:

01. Priority Recommendations for the Swiss Government during its Tenure on the UN Security Council

- **Promote the right to information and equity of digital access vis-a-vis the UN role in protecting human rights.** Everyone should have access to information and communication technologies. Identify ways to support access to digital tools such as mobile phones, computers, and the internet.
- **Support public interest media both online and offline.** Safeguard the producers of reliable and public interest contents. Support global publics in gaining critical skills in information and media literacy. Public interest media is essential to functioning democratic governance and peace processes. Identify ways to bolster local journalism, including via the newly created International Fund for Public Interest Media[66] to support local journalism and media programs to provide verified information and inclusive space for dialogue. Protect the independence and safety of Public Interest Media, ensure full transparency of media ownership, adopt international measures for taxing digital platforms, and promote hybrid funding for the media and pluralistic media environment.[67]
- **Develop media development strategies for UN peacekeeping and special political missions**, in order to improve their capacity to assess local information ecosystems and then accordingly tailor their creation of UN media capacities and support to local media actors, and their post UN-transition with a view to long-term sustainable peace.[68]
- **Create partnerships between social media companies and UN Missions involved in peacemaking and UN Mediation teams**, especially in key moments of elections and peace processes when there is high risk of disinformation. One example is the cooperation between Facebook and the UN mediator in Libya detailed in Social Media in Peace Mediation cited earlier.[69] One model for this is Facebook's current International Institutions and Relations staff providing support to UN missions on how to use the Facebook platform for UN strategic communications and digital public diplomacy.
- **Grant access to data from big tech platforms to humanitarian actors, conflict researchers, and peacebuilding experts.** Early warning of conflicts requires access to better understand digital trends that affect conflict dynamics.

66 https://ifpim.org/
67 Forum on Information and Democracy. *A New Deal for Journalism*. 2021.
68 See also the recommendations of the 2018 Geneva Roundtable on the transition of UN Peacekeeping Operations' radio stations.
69 Lanz, et al. 2021.

02. Form a Multi-stakeholder Alliance to explore Peace Processes and Digital Governance

Given the impact of digital spaces on conflict, a new initiative is necessary to represent the interests of sustained public peace processes in digital governance discussions with governments and technology companies. The peacebuilding field is lacking a unified voice and set of recommendations to govern tech companies' impacts on conflict.

The European Commission reached agreement on a Digital Services Act, a set of rules for digital platforms, marketplaces, and search engines in the public interest. The UN's B-Tech Project provides guidance for implementing the United Nations Guiding Principles on Business and Human rights (UNGPs) in the technology space.[70] While these existing forums may share some of the concerns related to sustained peace processes, five regulatory issues are especially important to peace processes.

- **Develop a normative framework** such as a Statement of Principles or a Code of Honor for tech company engagement in peace and conflict.
- **Explore global standards for conflict-sensitive social media algorithms.** Given the current analysis of algorithmic contributions to polarisation and extremism through amplifying false and hateful content, represent the interests of sustained public peace processes in policy discussions related to transparency and oversight on algorithms that run tech platforms including the Algorithmic Justice League[71] and the Algorithmic Transparency Movement.[72]
- **Translate conflict sensitivity, do no harm, and humanitarian standards into the digital space**. Consider the relevance and translate international law standards, including human rights, international criminal law, and humanitarian principles such as protection of civilians, neutrality, impartiality, independence, non-discrimination, and need-based approaches to the digital space. Develop ethical and do no harm standards drawing on a combination of human rights, conflict sensitivity, human security, and ethical frameworks.[73]

03. Engaging with Technology Companies on Conflict Sensitivity and Peace Processes

Big tech companies hold a tremendous amount of power. Small changes in their design, algorithms, and moderation policies can polarize populations, sway elections, escalate armed conflict, and result in mass atrocities. Tech companies have an enormous and urgent responsibility to integrate conflict-sensitive design, algorithms, and moderation policies. Big tech (eg Google, Facebook) as well as smaller and new tech start-ups need to build their capacity for reducing the risk of digital platforms fueling conflict and increasing their contributions to peace.[74]

ICT4Peace helped to launch Tech Against Terrorism, a coordination platform for government, tech companies, and CVE/PVE civil society groups to analyse and prevent the use of digital spaces to recruit and mobilize support for terrorism.[75] Civil society networks like Access Now focus on providing a platform for human rights groups to coordinate with tech companies.[76] To date, there is less understanding and emphasis on the need for conflict-sensitive technology and technology that contributes to social cohesion and peace processes.

- Forge more partnerships between big tech and civil society organizations (such as fact-checking services, news outlets, academia, peacebuilding and human rights orgs) to collaborate on key issues related to technology's role in driving conflict and promoting peace. One place for these types of partnerships is the soon-to-be-

70 https://www.ohchr.org/en/business-and-human-rights/b-tech-project
71 https://www.ajl.org
72 AlgoTransparency.org
73 Jennifer Easterday, Hana Ivanhoe, and Lisa Schirch. "Comparing Guidance for Tech Companies in Fragile and Conflict-Affected Situations." Tokyo: Toda Peace Institute, March 2022.
74 Jennifer Easterday and Hana Ivanhoe. "Technology in Fragile Contexts: Engagement, Partnerships, and Positive Action." Justpeace Labs and LSE Knowledge Exchange, 2021.
75 https://www.techagainstterrorism.org
76 https://www.accessnow.org

launched Council on Technology and Social Cohesion, a space for peacebuilding and bridge building organizations to address potential collaborative work between tech company staff and peacebuilding experts to prevent digital harms and amplify digital contributions to peace.

- Engage regional tech company offices in more closely watching their respective contexts for early warning of digital threats to conflict and violence.
- Build tech company staff capacity, including engineers, designers, and all program and policy staff, to understand and prioritize elements of sustained peace processes (e.g., conflict analysis, intergroup dialogue, and participatory decision-making) in tech product cycles.
- Recruit sufficient staff who speak languages in which these platforms are used, and invest in such staff's capacity to apply community standards and content moderation.
- Help tech companies to design national and regional consultation platforms involving government and diverse civil society stakeholders that can identify digital risks and help to generate ideas for locally relevant peacetech.
- Coordinate among peacebuilding organizations to develop organizational specialization on the broad issues related to technology. Participate in Build Up's annual conference on technology and peacebuilding.

04. Develop and Improve "Peacetech"

The United Nations is investing in a suite of technology tools to support peacebuilding. Big tech companies are focusing mostly on the moderation of disinformation and hate speech rather than affordances that would support peace. New tech start-ups and investors are interested in learning more about peacebuilding and conflict sensitivity and are beginning to explore the needs and affordances necessary for social cohesion.

- **Explore wider use of peacetech tools.** New digital tools such as Remesh, Polis, and Kazm hold tremendous potential for improving elements of sustained peace processes such as intergroup dialogue and participatory decision-making. Digital tools such as Phoenix for collecting, analysing, and visualising information related to peace and conflict offer news ways for policymakers and members of the public to understand the drivers of conflict and the opportunities for peace. While these tools and many others create a mediating bridge between technology and diverse stakeholders, these types of tools are not yet widely used. Greater funding to further develop these types of tools for wider use is necessary. Funders could invest in experimentation, piloting, and wider adoption for using these tools to transform state-society relations and transform conflict dynamics.
- **Create secure platforms for sensitive diplomatic negotiations.** Some diplomats and mediators have rejected the use of digital platforms such as Webex, Microsoft Teams, and Zoom because of security fears of surveillance, leaks, or interference. Based on Switzerland's historic neutral space and "good offices" for mediation, Switzerland could consider investing in developing a diplomatic platform with affordances that would support peace negotiations while ensuring and hosting the servers for maximum levels of safety and trust.

05.Increase Digital Literacy

Governments, mediators, civil society organizations, and all ages of the public, and especially marginalized groups. Methods could include public service announcements (PSAs), workshops for select audiences or community influencers, and school curricula. Digital literacy topics could include:

- Promote a healthy information diet from public interest media sources both on and offline.
- Identify, pre-bunk, and debunk disinformation and addressing information disorders and cultivating cognitive vigilance (including awareness of cognitive biases) and critical thinking to identify false and deceptive information
- Manage privacy and digital risks with digital safety protocols.
- Include content on digital communication strategies for healthy conflict and building social

cohesion, including "upstanding" or digital accompaniment of groups who are the targets of hate speech or cyberbullying (for example migrants).

Annex A: Research Methodology

This paper builds on more than a decade of research on the impacts of technology and peace processes, including more than 40 interviews with tech company staff, human rights, and media experts and extensive desk research. Specific to this brief, the author interviewed six peacebuilding organizations involved in working on issues of the digital space. Interpeace then facilitated a workshop on April 13, 2022 where a group of experts discussed the paper and provided further guidance and feedback. Annex B contains a list of the interviewees and workshop participants.

Annex B: Key Advisors, Interviewees and Workshop Participants

Special thanks to the following people who participated in providing guidance and advice, provided interviews and/or the attended the workshop to discuss this report:

Three advisors provided extensive guidance and feedback to this paper.

- **Sacha Meuter** from Fondation Hirondelle provided extensive guidance based on research on offline and online media hybridity.
- **Anne-Marie Buzatu** from ICT4Peace Foundation provided guidance based on their research on related issues.
- **Juuso Miettunen** from Principles for Peace Secretariat provided guidance to ensure the paper supported the P4P Process.

Interviewees and workshop participants included the following people:

5. **Emma Baumhofer**, Swisspeace
6. **María José Daza**, Institute for Integrated Transitions (IFIT)
7. **Ahmed Eleiba**, Swisspeace
8. **Jane Esberg**, International Crisis Group
9. **Jonathan Harlander,** formerly CMI, now HD Centre
10. **Andreas Hirblinger,** Geneva Graduate Institute
11. **David Lanz**, International Crisis Group
12. **Mariazel Maqueda Lopez**, EPFL EssentialTech Centre
13. **Helena Puig Larrauri**, Build Up
14. **Hiba Qasas**, Principles for Peace Secretariat
15. **Caroline Vuillemin**, Fondation Hirondelle

Principles for Peace Secretariat

Interpeace Headquarters

Maison de la Paix
2e Chemin Eugène-Rigot
CH-1202 Geneva
Switzerland

principles.secretariat@interpeace.org

+41(0) 22 404 59 00