UNIVERSITÄT DUISBURG ESSEN

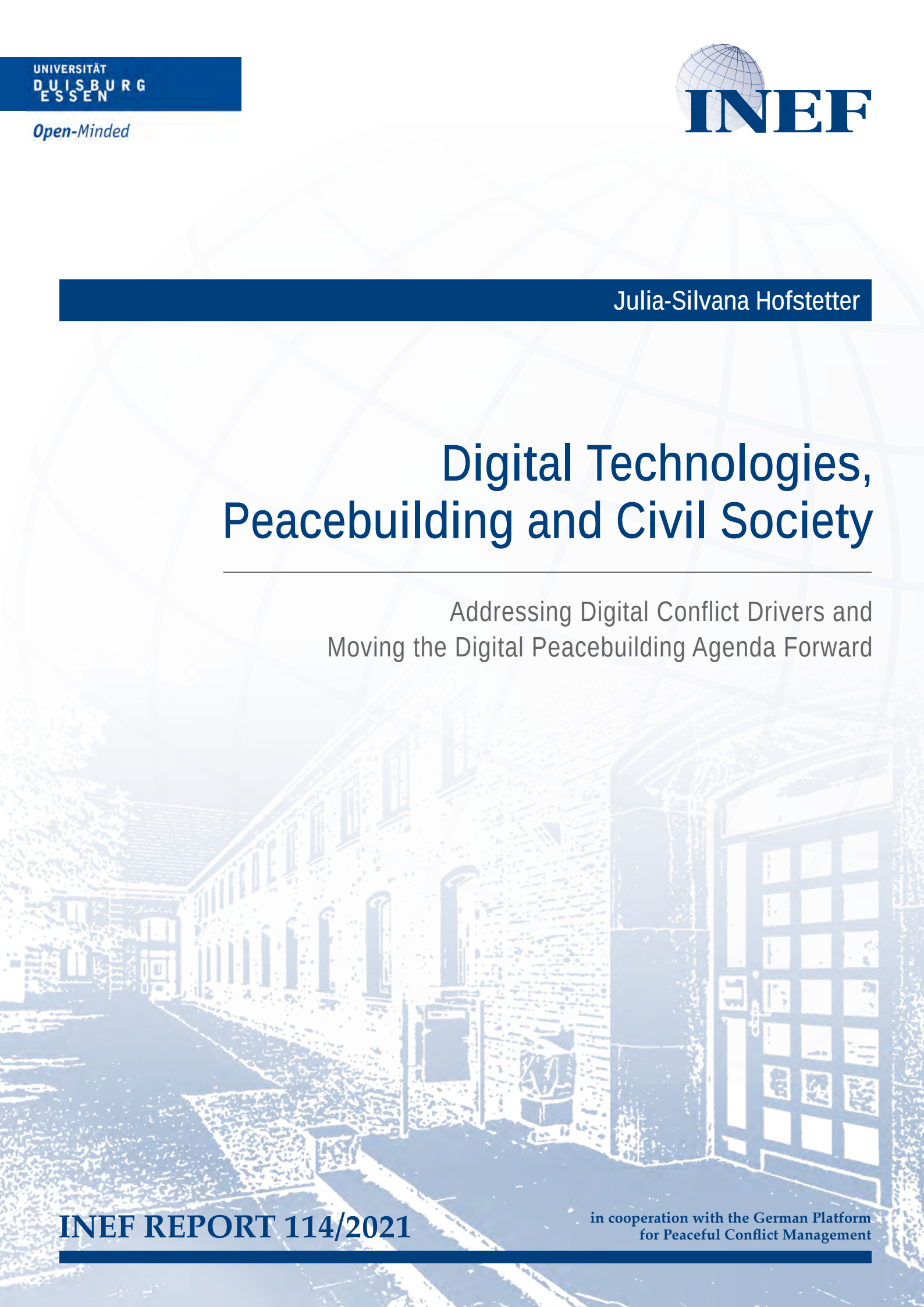
Open-Minded

INEF

Julia-Silvana Hofstetter

Digital Technologies, Peacebuilding and Civil Society

Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Agenda Forward



INEF REPORT 114/2021

in cooperation with the German Platform for Peaceful Conflict Management

NOTE ON THE AUTHOR:

Julia-Silvana Hofstetter M. A., is advisor at the ICT4Peace Foundation. Her research focuses on innovations in peacebuilding, the impact of emerging technologies on peace and security, and the women, peace and security agenda.

E-mail: juliahofstetter@ict4peace.

This study was commissioned with funding by the German Federal Ministry for Economic Cooperation and Development (BMZ).

BIBLIOGRAPHICAL NOTE:

Hofstetter, Julia-Silvana 2021: Digital Technologies, Peacebuilding and Civil Society. Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Agenda Forward, INEF Report 114/2021, Duisburg: Institute for Development and Peace.

Imprint

Editor:
Institute for Development and Peace (INEF)
University of Duisburg-Essen

Logo design: Carola Vogel
Cover design: Doppelpack Ohmen

Lotharstr. 53 D - 47057 Duisburg
Phone +49 (203) 379 4420 Fax +49 (203) 379 4425
E-Mail: inef-sek@uni-due.de
Homepage: https://www.uni-due.de/inef

ISSN 0941-4967

Julia-Silvana Hofstetter

Digital Technologies, Peacebuilding and Civil Society

Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Agenda Forward

INEF Report 114/2021

In cooperation with

PLATTFORM ZIVILE KONFLIKT BEARBEITUNG

University of Duisburg-Essen
Universität Duisburg-Essen

Institute for Development and Peace
Institut für Entwicklung und Frieden (INEF)

Hofstetter, Julia-Silvana 2021: Digital Technologies, Peacebuilding and Civil Society. Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Agenda Forward, INEF Report 114/2021, Duisburg: Institute for Development and Peace.

ABSTRACT

The wide availability of digital technologies is increasingly impacting the work of peacebuilders, altering both peacebuilding practices and conflict dynamics. The malicious use of technology – from the weaponization of social media to digital authoritarianism and cyberattacks – poses new threats to peaceful societies and urges peacebuilders to consider new fields of action in cyberspace. However, digitalization has also brought major innovations to the work of peacebuilders, establishing a new field of practice, 'digital peacebuilding'. Many of the innovative uses of peace technologies – for conflict prevention, transformation and reconciliation – have been driven by civil society organizations, who are at the forefront of addressing the rising threat of digital conflict drivers, too. This report provides an overview of the opportunities and challenges digital technologies create for peacebuilders, discusses how they alter the role of civil society, and proposes future directions for the digital peacebuilding agenda.

ZUSAMMENFASSUNG

Die breite Verfügbarkeit digitaler Technologien wirkt sich zunehmend auf die Arbeit von Friedensakteuren aus und verändert sowohl die Praktiken der Friedensförderung als auch Konfliktdynamiken. Der böswillige Einsatz von Technologie – vom Einsatz sozialer Medien als Waffe bis hin zu digitalem Autoritarismus und Cyberangriffen – stellt neue Bedrohungen für friedliche Gesellschaften dar und drängt Friedensförderer dazu, neue Handlungsfelder im Cyberspace zu berücksichtigen. Die Digitalisierung hat allerdings zugleich wichtige Neuerungen für die Arbeit von Friedensakteuren gebracht und ein neues Praxisfeld, die "digitale Friedensförderung", etabliert. Viele der innovativen Anwendungen von Friedenstechnologien – für die Konfliktprävention, -transformation und -aussöhnung – wurden von zivilgesellschaftlichen Organisationen vorangetrieben, die ebenso eine führende Rolle spielen, wenn es darum geht, die steigende Bedrohung durch digitale Konflikttreiber anzugehen. Diese Studie gibt einen Überblick über die Chancen und Herausforderungen, die digitale Technologien für die Friedensförderung mit sich bringen, diskutiert, wie diese die Rolle der Zivilgesellschaft verändern, und zeigt auf, in welche Richtung sich die Agenda der digitalen Friedensförderung weiterentwickeln kann.

Content

1. Introduction[1]

The rapid growth and wide availability of digital technologies in recent years are increasingly impacting the work of peacebuilders, altering both peacebuilding practices and conflict dynamics. With the global lockdown and widespread travel restrictions caused by the COVID-19 pandemic, the digitalization of peacebuilding has received increased attention. Digital solutions helped many organizations to implement their activities remotely by moving the communication with staff and partner organizations, but also training or even negotiations with conflict parties, online. However, the adaptation of digital technologies for peacebuilding is not a recent development. From state actors to multilateral organizations and non-governmental organizations (NGOs), a range of peacebuilding actors have already digitalized their activities and established new structures and initiatives to come up with innovative uses of digital technologies. Growing steadily in line with technological innovations over the last two decades, these activities have led to the establishment of a new field of practice, 'digital peacebuilding'.

Beyond moving existing activities to the digital space, digital technologies have brought major innovations to the peacebuilding field. They allow peacebuilders to expand their fields of action and objectives and to redefine their own roles. The greatest transformative potential of digital technologies, however, lies in their scope to empower affected communities – making peacebuilding processes more inclusive but also giving citizens the possibility to self-organize and develop alternative infrastructures of peacebuilding. Digital technologies thus change *who* can become a peacebuilder and shift civil society's role from an object of peacebuilding to a subject. Moreover, many of the innovative uses of digital technologies for peacebuilding are driven by local civil society organizations.

Civil society actors are more flexible and operate under different conditions and on different scales than states or multilateral organizations, which makes them better placed to come up with new and innovative initiatives. These organizations thus play an important role in innovating the peacebuilding sector and have become the forerunners in developing new practices of digital peacebuilding. With regard to the *negative* impacts of digital technologies, too, civil society organizations have been at the forefront of developing new strategies to address the rising threats of digital conflict drivers. The increased global availability of digital technologies broadens the range of conflict stakeholders, provides conflict parties with new instruments of mobilization and violence, and opens new spaces in which conflicts are fought.

Despite the growing attention to the malicious use of technology by conflict parties – from the weaponization of social media to the use of surveillance technologies and cyberattacks – the question of how these altered conflict parameters might spoil peacebuilding efforts and how peacebuilders could incorporate these new threats into their conflict management frameworks is still underexplored. In contexts below the level of conventional armed conflict, too, emerging conflict frontiers in cyberspace are of increased relevance to peacebuilders. While a growing number of civil society organizations have started to address the threats that digital technologies pose to peaceful societies, these efforts still constitute an exception in the peacebuilding landscape.

To provide an overview of the opportunities and challenges digital technologies create for peacebuilders, this report maps how digitalization alters conflict dynamics and how digital tools offer innovation opportunities for peacebuilding practices, with a focus on the role of civil society. Civil society here refers to civil society organizations (at the international, national and local level), as well as civil society not formalized in an organization (which could involve grassroots movements and citizen-to-citizen initiatives, as well as individuals from affected communities).

[1] The author is grateful to interviewees and reviewers for their time and support and would like to thank Jakob Bund, Hannes Ebert, Julie Hawke, Maude Morrison, Branka Panic, Bernd Rieche, Lisa Schirch, Ginger Schmitz, Daniel Stauffacher and Cornelia Ulbert.

Based on desk research and expert interviews, the report discusses how non-digital peacebuilding strategies can be applied to conflicts arising in cyberspace (Section 2), but also how digital tools are utilized for conventional peacebuilding objectives (Section 3). It also offers an overview of general risks and structural barriers that peacebuilders are likely to face when using peace technologies, and maps strategies to address these challenges (Section 4). Lastly, the report provides an outlook on future directions, and points to key challenges which the peacebuilding community will have to address in order to move the digital peacebuilding agenda forward (Section 5).

2. How Digital Technologies Influence Conflict Dynamics – And How Peacebuilders Can Respond

Digital technologies alter the parameters of conflict, from the actors involved to the fighting strategies deployed, as well as the spaces in which division and violence are incited. Social media open up new avenues for the escalation of conflict, intensifying political polarization, accelerating the spread of disinformation, and blurring the lines between online and offline violence (see Section 2.1). Lowering the threshold for individuals to perpetrate or incite violence online, they also widen the spectrum of conflict stakeholders. Moreover, conflict parties and repressive governments can deliberately use digital technologies as tools to mobilize support or to silence or spy on opponents and activists (see Section 2.2). Cyberattacks have become an increasingly relevant instrument in armed conflicts and the rising proliferation of offensive cyber capabilities among state and non-state actors threatens to further escalate political tensions (see Section 2.3).

With conflict increasingly shifting to virtual spaces, peacebuilders need to expand their efforts and reach out to conflict stakeholders and peace constituencies online and mitigate the new threats these altered conflict dynamics impose on the non-digital world. In settings beyond conventional armed conflict, too, the field of peacebuilding can make a valuable contribution to addressing the threats of digital technologies. While the peacebuilding community has only started to realize the significance of digital conflict drivers for their work, the sections below describe current discussions on the threats posed by digital technologies and initial attempts by civil society peacebuilders to address these new challenges (see Box 1). A special emphasis is put on how digital technologies affect civil society organizations and individuals, both as targets and perpetrators of violence and as agents of peacebuilding.

2.1 The 'Weaponization' of Social Media

In recent years, social media have taken center stage in the discussion on digital conflict drivers (Mercy Corps 2019). Through digital technology, every individual has the possibility to develop and disseminate false information and hate content with increased speed, volume and reach. Social media deepen the polarization of online discourses and provide a platform for users to quickly mobilize violent action. These dynamics pose a great threat in terms of escalating societal tensions that might encourage outbreaks of violence and have the potential to disrupt peacebuilding, especially when the deliberate 'weaponization' of social media targets peace processes or organizations directly.

The negative influence of digital technology on the polarization of political discourses has received growing attention. Political polarization and the dominance of extreme views in public discourse thrive on social media because these platforms are designed to bring like-minded people together and to maximize users' engagement, which tends to promote extreme content (Laub 2019) and leads to selective exposure to information and confirmation bias (Mercy Corps 2019: 18). Different factions within society thus no longer have common meeting spaces that would be crucial for the fostering of understanding and empathy for each other. These tendencies might unintentionally lead to a polarization of online communities but can also be misused to deliberately radicalize individuals. The anonymity of the web prevents online users from being

Box 1: Addressing Digital Conflict Drivers

Digital technologies alter conflict dynamics, allowing a broader field of stakeholders to become perpetrators of violence, offering new fighting strategies and forms, and opening new spaces in which conflicts are fought. This urges peacebuilders to consider the digital conflict drivers in their conflict management mechanisms, but also poses the question whether peacebuilders should expand their fields of action to contexts of non-conventional armed conflict. Civil society peacebuilders in particular can address digital conflict drivers in three new fields of action:

(1) The 'Weaponization' of Social Media:

To address political polarization, digital disinformation and dangerous speech on social media, civil society peacebuilders can:

- **Mediate online conflicts by seeking dialogue with online users or moderating online content** (content moderation strategies include peace messaging, reporting dangerous content, fact-checking, and spreading verified information);
- **Support society's resilience against disinformation and hate speech** through digital media literacy training and hate speech awareness campaigns;
- **Reach out to conflict party leadership to negotiate acceptable online behavior in the context of armed conflict**, possibly in the form of social media codes of conduct;
- **Engage in global advocacy** to improve the design and regulation of online platforms.

(2) Digital Authoritarianism:

To address the rising threats of digital authoritarianism, civil society organizations can:

- **Monitor and document the abuse** of digital technologies by governments and engage **in global advocacy** to hold governments but also technology companies accountable;
- Support local civil society actors by providing **guidelines and training on how to fend off digital repression** and by offering **emergency support**.

(3) Offensive Cyber Capabilities:

To address the impact of potential cyberattacks on conflict dynamics, civil society peacebuilders can reach out to conflict parties to:

- **Incorporate offensive cyber capabilities into existing conflict management mechanisms** in the context of armed conflict (this could include defining unacceptable targets of cyber operations or establishing structures to manage cyber incidents that arise during a peace process);
- **Set up new mechanisms for dialogue to avert the escalating cyber hostilities** in situations where armed conflict has not yet occurred.

Different Roles for Different Actors from Civil Society:

- International and local civil society organizations **with specialized knowledge** (e.g. on cybersecurity, digital disinformation or hate speech) can help to strengthen societies' and activists' resilience against threats arising in cyberspace.
- Global civil society organizations with **experience in human rights advocacy** can raise awareness of digital authoritarianism and the negative impact of social media platforms on conflict dynamics.
- Civil society organizations that have **experience in third-party mediation of armed conflicts** can reach out to conflict party leadership in order to address tensions arising from their behavior on social media or relating to offensive cyber capabilities.
- **Citizens** can contribute actively to the monitoring and moderation of dangerous online content.

Peacebuilders need a better understanding of how digital technologies influence conflict dynamics and which strategies civil society peacebuilders can apply to emerging challenges since digital conflict drivers are likely to become more prevalent in the future and threaten to disrupt peacebuilders' work if they remain unaddressed.

held accountable for their shared content and therefore lowers the threshold for the spread of hate speech[2]. Users might perceive their online identity as detached from their offline identity, lowering their inhibition to voice hateful views, or become perpetrators of online violence (Rio 2020: 6).

Social media also favor the spread of false information. Verified information, which takes time to analyze, evaluate and communicate, cannot compete with the immediate dissemination of fictitious stories and rumors through digital channels (Vosoughi/Roy/Aral 2018: 1146-1151). Moreover, for people who do not follow the news regularly and who use social media for entertainment only, the information they consume involuntarily on these platforms might be their only news source, which makes them particularly vulnerable to misinformation. (Schirch 2018: 16). Next to the unintentional spread of false content (misinformation), false information is in many cases deliberately created and shared in order to harm (disinformation). There are various strategies to disseminate disinformation by digital means, from coordinated bot networks[3] to using fake domains, replicating websites or social media profiles, and the hijacking of an organization's or individual's social media account to spread false content (Oh/Adkins 2018).

There is growing concern that disinformation campaigns and online attacks might directly target civil society organizations in order to sabotage their work. As peacebuilders increasingly rely on social media platforms to communicate with the public, they are vulnerable to hackers gaining control of their social media accounts to spread disinformation, to create uncertainty and distrust, or to silence these organizations (Accessnow 2017). Disinformation is especially concerning in the context of peace processes, where it threatens to destabilize public trust in peacebuilders and buy-in and might spoil the processes (Jenny et al. 2018: 11). The further refinement of Artificial Intelligence (AI) technology and its application to produce 'deep fakes' of video and audio material threaten to increase these risks in the future (Kakoma/Marques 2020: 7; Höne 2019).

Besides the deliberate weaponization of social media to deepen polarization and spread disinformation, these platforms are especially dangerous when online dynamics incite the outbreak of violent incidents in the non-digital world. Social media platforms make it possible to quickly call large numbers of people to collective action, which means that the spread of disinformation and online hate might swiftly turn into digital vigilantism. The term often used in this context is 'dangerous speech', which compared to 'hate speech' aims specifically to amplify intergroup violence.[4] These coordinated efforts by social media users to collectively attack and harass other online users or incite against a certain social group can eventually turn into offline violence and physical assaults. Recent examples of these dynamics within the context of the COVID-19 pandemic show that online hate and scapegoating are often directed against already marginalized groups. For example, in India, COVID-19 infections caused by mass gatherings of the Muslim group Tablighi Jamaat sparked a wave of online hate. Hundreds of thousands of online posts used the hashtag '#CoronaJihad' to call for violence against the group, which resulted in direct attacks against members of this religious minority (Desai/Amarasingam 2020).

With online discourses increasingly impacting conflict dynamics in many fragile contexts, the monitoring and evaluation of online interactions will have to become an integral part of conventional conflict analysis mechanisms, as ignoring them might spoil peacebuilders' work (see Sections 3.1.1 and 3.1.2 on how peacebuilders use digital tools to monitor online dynamics). As the unfolding of conflict shifts online, peacebuilders also have to expand their efforts to prevent violence and foster peaceful dialogue in online spaces. They can do so (1) by directly mediating online conflicts by seeking dialogue with online users or moderating online content, (2) by supporting communities' resilience against disinformation and hate speech, or (3) by reaching out to conflict party leadership.

---

[2] Hate speech' refers to "speech which demeans or attacks a person or people as members of a group with shared characteristics such as race, gender, religion, sexual orientation, or disability", Faris et al. 2016: 5-6.

[3] A bot is an autonomous program that performs automated tasks on the internet.

[4] On indicators of 'dangerous' speech see Benesch 2014.

(1) To mediate online conflicts, civil society organizations can directly reach out to conflict parties' constituencies on social media and engage in content moderation. Content moderation strategies can include peace messaging (Peace Direct 2020: 24), the reporting of dangerous content to social media platforms, fact-checking online content, and supporting the spread of verified information (Schirch 2020a). For instance, the NGO Dangerous Speech Project implemented the initiative 'Nipe Ukweli' in the context of electoral violence in Kenya, which provided public information on dangerous speech and mechanisms to report and remove dangerous content.[5] While efforts to counter hate speech, disinformation and polarization through content moderation and dialogue with online users are increasing, such initiatives still require a large amount of human resources. In particular, if dialogue is based on one-on-one conversations between online users and moderators, scaling up these initiatives can be challenging.[6] The mobilization of civil society plays an important role in human resource-intensive content management strategies, and organizations often rely on volunteers to become moderators or contribute to reporting problematic content. For instance, The Commons project, initiated by the global NGO Build Up, trained volunteers to engage in online moderation of polarized political discussions in the US, which also included moderators sharing resources with social media users they engaged with to encourage them to start facilitating online depolarization themselves (see Box 2).

(2) Beyond this, peacebuilders can also take preventative measures and strengthen societies' resilience to these new threats, improving the local population's digital media literacy and ability to identify misinformation and hate speech. This might also entail offering training to citizens on how to apply counter-speech strategies and empowering them to stand up against online hate speech themselves.[7] The spread of verified information can also be supported using targeted ads on social media, chat bots or online focus group discussions. Notably, the global NGO Peace Tech Labs develops hate speech lexica in various contexts, such as the elections in South Africa in 2019. The NGO partnered up with a local organization, Media Monitoring Africa, to gather hate speech terms as a basis for semi-automated online and offline media monitoring (Gichuhi 2019). Such initiatives have shown themselves to be especially successful when they are implemented by or in cooperation with local organizations that already have legitimacy in local communities, and when they are based on two-way communication with target communities.[8] Entering into dialogue with local communities not only improves the gathering of data on circulated misinformation and rumors, but also allows peacebuilders to identify community-specific information gaps efficiently and to better target the dissemination of verified content.

(3) Moreover, peacebuilders can prevent and mitigate the negative effects of social media on conflict escalation by addressing these issues at the formal negotiation table. The Centre for Humanitarian Dialogue (HD Centre), for instance, has developed guidelines for social media codes of conduct as a new conflict mediation tool. Such codes of conduct, when agreed upon by conflict parties, could help to stop the spread of hate speech and disinformation that jeopardize a peace process (Harlander/Morrison 2020). However, this presupposes that the leadership of a conflict party has authority over perpetrators of online violence and disinformation campaigns. Such activities might, instead, be started by groups or individuals that operate independently of official conflict party structures and might in fact be difficult to identify as the source of hate speech and disinformation.

Next to reaching out to conflict stakeholders online, moderating content and supporting societies' resilience to disinformation and hate speech, civil society actors need to coordinate and to engage in advocacy to address the rising challenges of the weaponization of social media. This should

---

5 https://dangerousspeech.org/nipeukweli/

6 Interview with Julie Hawke, Build Up, 12 January 2021.

7 See, for example, https://love-storm.de/trainieren/.

8 Interview with Maude Morrison, Centre for Humanitarian Dialogue (HD), 15 January 2021.

Box 2: 'The Commons' – Depolarizing Online Political Discourse in the US

'The Commons' is a program that addresses online polarization in the US. The initiative was set up in 2017 by the global NGO Build Up in partnership with MIT International Science and Technology Initiatives (MISTI) and funded by HumanityX and the city of The Hague. After an initial pilot phase, Build Up ran a scaled-up version of the project throughout 2019, testing a variety of strategies to depolarize political conversations on Twitter and Facebook. The objective of The Commons is to address polarization by inducing a change in the behavior of social media users, encouraging them to engage in critical reflection on their online behavior, and to adopt productive strategies for healthy conversations around political differences online and offline.

To do so, the project identified online users who took part in political discussions about the US and analyzed the likelihood that they were at risk of polarization. Individuals were then engaged in conversations with trained facilitators. The conversations were also used as an entry point to provide further resources and avenues for action towards depolarization. To identify target communities on Twitter, the project tweeted automated messages using a Twitter bot that posted liberal or conservative hashtags about political topics. People who responded positively to a tweet were automatically assigned to a trained facilitator who started a conversation on Twitter. On Facebook, the initiative posted specific prompts on 'The Commons Project' Facebook page and spread them with micro-targeted ads. The ads were targeted towards the 'most polarized cities' as based on political campaign donations, and either asked people whether they recognized a political divide in their city or focused on key political issues that were most likely to be divisive (e.g., gun control, immigration or healthcare). It also included the creation of an automation platform that identified relevant hashtags and target communities, automatically provided facilitators with a list of candidates to contact and a suggested response, and tracked all conversations as well as Facebook and Twitter metrics for monitoring and evaluation purposes.

In the second phase of the project, approximately 500,000 people were exposed to the automatically distributed tweets and Facebook posts, 2,122 of whom engaged in conversations with Build Up's facilitators, at an average length of 6 to 7 replies. Of these, at least 991 people accessed resources for further action on contributing to depolarization that facilitators recommended. To evaluate the impact of the initiative, the project team analyzed users' online behavior after having been contacted by its facilitators. Comparing the retweet behavior of control and treatment groups, for instance, showed that connections across groups with different ideologies increased more for people who were engaged in conversation.

For more information see: Build Up 2019

include collaboration with tech companies to improve the design of online platforms and lobbying governments and international organizations to hold platform providers accountable.[9]

2.2 Digital Authoritarianism

Regarding the malicious use of digital technologies, the peacebuilding community is paying growing attention to the phenomenon of 'digital authoritarianism', meaning the repressive use of digital technology by governments against political opponents, civil society actors and peace and human rights organizations. Strategies of digital authoritarianism include: (1) restricting the ability to use Information and Communications Technologies (ICTs), (2) censoring online content, (3) spreading online propaganda and disinformation, (4) using surveillance technologies, and (5) using online regulation as a pretext for prosecution.

Repressive governments often dissolve opposition by shrinking civil society's spaces for digital action. Strategies to restrict political opponents' and activists' online activities can include hacking individuals' and organizations' social media accounts to intimidate and silence them, shutting down the internet to prevent protesters from communicating or organizing, or censoring opposing views online in cooperation with big technology platforms (Puyosa 2019: 19-20). Social media platforms have been used by governments to spread disinformation and propaganda, or to raise

[9] For more strategies and a broad agenda of civil society advocacy regarding social media, see Schirch 2020a: 19-20.

support for their policies, by intimidating citizens into reacting to and sharing officials' online content, or even linking access to government services to online behavior (Schirch 2020a).

There is increasing evidence of governments, in autocracies as well as democracies, using surveillance technologies to collect data on their citizens and civil society organizations. For instance, Amnesty International has reported numerous cases of state surveillance where hacking tools were used to collect personal data of human rights activists in Saudi Arabia (Amnesty International 2018). With digital technologies, surveillance has become much easier and less costly to maintain (Kendall-Taylor/Frantz/Wright 2020).

Moreover, under the pretext of fighting hate speech and disinformation, oppressive regimes have started to introduce legislation that illegalizes certain online content or behavior in order to target and prosecute political opponents, activists and journalists. Recently, the authorities in the Philippines introduced a new COVID-19 law that criminalizes the spread of false information about the virus and used it as an excuse to arrest political opponents and activists for sharing content on social media which the government claimed to be 'fake news' (Wiseman 2020).

To address the rising threats of digital authoritarianism, international and national civil society organizations can (1) carry out research and monitoring and engage in global advocacy to raise awareness and to hold governments but also technology companies accountable. To support local organizations, they can (2) provide guidelines and training on how to fend off digital repression and build resilience, or offer direct emergency support.

(1) International NGOs are playing a major role in uncovering and addressing rising tendencies of digital authoritarianism. Amnesty International recently released a report (Amnesty International 2021) detailing the abuse of surveillance technologies by South Sudan's National Security Service (NSS) to persecute journalists, activists and government critics. The report also calls upon the South Sudanese government, as well as telecommunication and surveillance tech companies that cooperate with it, to respect human rights, and asks states to implement an immediate moratorium on the purchase, sale and transfer of surveillance equipment. Civil society groups globally will have to continue to raise awareness about the misuse of ICTs and surveillance technologies for authoritarian repression and advocate for governments that employ such strategies, but also companies that help enable them, to be held accountable.

(2) Besides global advocacy work, international and national civil society organizations can support local human rights and peace activists and civil society movements by providing guidelines and training on how to evade government surveillance and continue their operations when faced with internet shutdowns. The Tactical Technology Collective, for example, developed the Security in a Box toolkit, which provides civil society organizations and activists with guidelines on how to protect their devices from malware.[10] Specialized centers, such as Access Now's Digital Security Helpline, also advise individuals and organizations on how to improve their digital security practices and even provide rapid response emergency assistance to actors already under attack.[11]

2.3 Offensive Cyber Capabilities and the Escalation of Political Tensions

Cyber operations are increasingly recognized as a relevant threat to international peace and security. Offensive cyber capabilities – defined as operations in cyberspace to manipulate, deny, disrupt, degrade or destroy targeted computers, information systems or networks (Uren/Hogeveen/Hanson 2018) – can be deployed to cause virtual as well as physical damage. While such attacks are still relatively rare and have not yet caused large-scale physical harm, they are becoming more relevant for peacebuilders due to their potential to alter conflict dynamics and

[10] https://tacticaltech.org/projects/security-in-a-box/

[11] https://www.accessnow.org/help/

spoil peace processes. But the peacebuilding community should also pay greater attention to contexts where armed hostilities did not yet occur, but where the proliferation of offensive cyber capabilities threatens to induce the escalation of political tensions and spark new outbreaks of armed conflict.

As many states develop offensive cyber capabilities, cyberattacks on political opponents' computer infrastructure and information systems have become an additional instrument in conventional armed conflicts to destabilize an opponent's internal and external processes (Danyk/Maliarchuk/Briggs 2017). While cyberattacks have mainly been an issue in inter-state conflicts, they are becoming increasingly relevant in civil war contexts, with offensive cyber capabilities being increasingly available to, but also used against, non-state actors (Kavanagh 2021). While in the past offensive cyber operations have mostly been conducted below the level of armed conflict, they have often intensified political tensions (Kausch 2017). The proliferation of offensive cyber capabilities alters conflict dynamics and increases the risk of conflict escalation due to the difficulties of attributing these attacks to a specific source. With the proliferation of offensive cyber capabilities among non-state actors, nation-states can also rely on proxies to conduct cyberattacks on adversaries, which deepens existing challenges of attribution. The possibility to shift the responsibility of an attack to other actors also offers opportunities for staging false flag operations to incite the escalation of political tensions between unwitting parties (Skopik/Pahi 2020).

Cyberattacks are especially concerning due to their potential threat to civilians. Disrupting the provision of essential services, for example by shutting down critical infrastructure, may induce a humanitarian crisis (Caltagirone 2019). Moreover, cyberattacks differ from conventional strategies of armed conflict in that they might spread uncontrollably and affect societies that were not initially targeted, as several global malware attacks have shown in the past. The WannaCry malware, for instance, disrupted operations of companies and public services providers in over 150 countries (Whittaker 2019).

Since cyber operations expand the range of attack strategies below the level of armed conflict and due to attribution problems, they lower the risk of perpetrators having to face retaliatory attacks and may thus lower the threshold for engaging in aggression. For these reasons, and due to the wider availability of offensive cyber capabilities even to smaller states and non-state actors, cyberattacks are likely to occur more frequently in the future, both in contexts of armed conflict and in other fragile settings.

As it has become increasingly evident that cyber operations have the potential to jeopardize peacebuilding processes while also posing a considerable threat in fragile non-conflict settings, peacebuilders have started to consider the cyber dimension in their conflict resolution activities. Cyber operations can be addressed by peacebuilders on two levels: (1) by incorporating the cyber dimension into their conventional conflict resolution mechanisms in the context of armed conflict; or (2) by entering the field of cyber diplomacy and applying their conflict resolution strategies to prevent and mediate cyber conflicts.

(1) In the context of conventional armed conflict, peacebuilders will need to integrate capacities to analyze the cyber dimension in each specific conflict setting in order to gain a better understanding of how cyber incidents might affect the peace process and their activities. They might also consider addressing offensive cyber capabilities in formal ceasefire agreements, disarmament and demobilization processes, and in related monitoring activities (UNDPPA/HD 2019: 19-20). This could entail defining unacceptable targets of cyber operations such as critical infrastructure or establishing mechanisms to manage and resolve cyber incidents that arise during a peace process (Kane/Clayton forthcoming 2021). Hesitation to add the cyber dimension to the negotiation agenda is based on a potential trade-off between preventing cyber incidents and efficiency in moving the process forward.[12]

[12] Interview with Hannes Ebert, Centre for Humanitarian Dialogue (HD), 15 January 2021.

Therefore, peacebuilders will have to evaluate the context-specific risk of cyber capabilities disturbing the peace process or potentially causing humanitarian costs.

(2) The increasing threat that cyber operations pose to international peace and security has given rise to the growing field of 'cyber diplomacy', advanced mainly through multilateral fora such as the United Nations Group of Governmental Experts (GGE) on "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" and the UN Open-Ended Working Group (UN OEWG) on "Developments in the Field of ICTs in the Context of International Security", which have developed binding and non-binding norms of responsible state behavior in cyberspace. Transferring strategies and tools from conventional conflict mediation to cyber incidents has proven to be increasingly relevant for the prevention and de-escalation of cyber conflicts. Notably, a key focus of the cyber diplomacy bodies set up by the UN and also the Organization for Security and Co-operation in Europe (OSCE) has been the development of cyber confidence-building measures (CBMs) aimed at reducing the risks of armed conflict caused by cyber incidents (Healey et al. 2014).

Conversely, civil society peacebuilding organizations, such as the HD Centre, have started to expand their portfolio, applying their conflict resolution experience to the context of cyber conflicts and setting up mechanisms for dialogue to avert the escalation of cyber hostilities. What is remarkable about this new field of action is that mediation will take place in the context of aggressions below the level of armed conflict and thus focus on prevention rather than the resolution of an armed conflict. Setting up such dialogue formats seems especially relevant in contexts where the proliferation of offensive cyber capabilities and political tensions overlap and established conflict settlement platforms do not exist. In contexts where no prior diplomatic channels were established, talks could start off with less politically sensitive issues and focus on involving technical communities such as national Computer Emergency Response Teams (CERTs).[13] Civil society peacebuilding organizations could play an important role in the cyber diplomacy field, especially since multilateral fora such as the UN OEWG are only slowly making progress, and dialogue facilitation by governmental actors might be hindered by third-party states' own cyber capabilities and interests. While the idea to establish a 'cyber peacekeeping' unit within the UN system has repeatedly been discussed in the past, such initiatives are difficult to implement in practice and are likely to face reluctance from member states possibly concerned about revealing their national defensive and offensive cyber capabilities (Dorn/Webb 2019).

3. How Digital Technologies Transform the Field of Peacebuilding

Digital technology's application in peacebuilding is usually differentiated in two categories: the non-strategic use of digital tools that innovates operational processes; and the strategic use of digital technology that pursues a specific peacebuilding goal the latter thus defining a new field of practice, 'digital peacebuilding'.[14] "Non-strategic" use refers to the application of digital tools in the general management of peacebuilding organizations. On the operational level, digital technologies can potentially make peacebuilders' work more efficient by helping them to overcome logistical and financial barriers (Peace Direct 2020: 20) In particular, the possibility to conduct certain activities remotely – from communication with staff and partner organizations to training, capacity-building, and monitoring and evaluation – makes digitalization intriguing for peacebuilders. 'Digital peacebuilding' in the narrower sense is distinct from merely digitalizing operational activities, in that the technological component is of *strategic importance* for achieving

[13] Interview with Hannes Ebert, Centre for Humanitarian Dialogue (HD), 15 January 2021.

[14] Others rely on a less restrictive definition of 'digital peacebuilding' and include the non-strategic use of digital technologies or even define digital peacebuilding as the broader nexus of digital technologies and peacebuilding that also includes addressing digital conflict drivers by non-digital means (e.g., Schirch 2020b: 2).

peacebuilding objectives (Cottary/Puig Larrauri 2017). Besides integrating existing digital products in peacebuilding initiatives, this often includes the development of new digital tools that are designed for a specific peacebuilding goal or context, so-called 'peacetech'. As well as moving existing peacebuilding activities to the digital space, digital technologies have the potential to bring about major innovations in the peacebuilding field. They allow peacebuilders to expand their fields of action and peacebuilding objectives and to redefine their own role. Section 3.1 maps these innovations across the different phases of peacebuilding. Digital technologies – and their strategic and non-strategic use for peacebuilding – also have important implications for power structures within the peacebuilding architecture in that they have the potential to empower local organizations and alternative peacebuilding infrastructures (see Section 3.2).

3.1 Digital Peacebuilding and Innovation across Different Phases

Digital peacebuilding includes the strategic use of a variety of hardware and software, from information and communication technologies (ICT), geographic information systems (GIS) and unmanned aerial vehicles (UAVs) such as drones, to software used for data processing, analysis and storage involving artificial intelligence (AI) and blockchain technology. These technologies help to innovate peacebuilders' work on three functional levels (Build Up 2018: 3; Schirch 2020b: 9-10):

(1) They can improve *access to information* by providing new opportunities for data collection, organization and analysis. Data collection is innovated in that technologies give access to data sources and subjects that were not available before. For example, with the help of drones or satellites, GIS systems provide access to remote areas, data scraping tools can help to collect information across the internet, and online and mobile surveys measure public perceptions. Sophisticated data analysis software allows access to vast amounts of data and provides peacebuilders with new ways of utilizing this information, for example by creating digital crisis maps.

(2) Digital technologies also offer new opportunities in terms of *strategic communication*, providing peacebuilders with new avenues for sharing information more quickly with a broader audience. ICTs thus help peacebuilders to make their work more transparent, promote peace messages more widely, and share verified information more quickly.

(3) Digital technologies also innovate *forms of engagement*. Digital spaces provide a new platform where peacebuilding organizations and civil society can meet, network and coordinate. ICTs help individuals, too, to organize in order to achieve shared goals, improve their participation and representation in political processes, and offer new platforms for public dialogue.

On all three functional levels, the transformative potential of digital technologies is largely, but not exclusively, based on improving peacebuilding organizations' ability to scale the inclusion of local civil society in peacebuilding or to provide citizens with the opportunity to develop their own peacebuilding initiatives, as appropriate. Reaching out to affected populations through digital technologies improves peacebuilders' ability to gather relevant information, not only about the conflict but also about citizens' needs and interests (*access to information*); communication technologies also allow peacebuilders to share information with citizens directly, bypassing possibly blocked local government institutions (*strategic communication*); digital technology provides more ownership and agency to local organizations and citizens who can make their voices heard or mobilize through digital platforms (*forms of engagement*).

The following sections therefore focus particularly on examples of how digital technologies create new and innovative forms of local civil society inclusion and ownership in peacebuilding, and give an overview of their application across different peacebuilding phases: (1) early warning and conflict prevention, (2) conflict transformation, and (3) transitional justice and reconciliation.

3.1.1 Early Warning and Conflict Prevention

Digital technologies have innovated conflict analysis and early warning systems by improving the collection, analysis and sharing of relevant information on conflict dynamics: ICTs allow citizen involvement in data-gathering processes through crowdsourcing and expand the reach of early warning mechanisms, while GIS gives access to data from remote areas, social media analysis provides new sources of information, and AI accelerates the processing of growing amounts of data.

Civil society peacebuilders increasingly use crowdsourcing technology that gathers real-time conflict data with relatively few resources. Crowdsourcing technologies allow the local population to report on violent incidents using simple ICTs, such as mobile phones. This not only expands the information base but also gives a voice to local communities' experiences (Schirch 2020b: 4). One of the first initiatives to make use of this technology to map local violence was Ushahidi, an online platform developed in Kenya in 2008 that gathers data from text messages, emails and social media to map violence hotspots, provide data visualization, and manage data. Besides monitoring election violence in Kenya, Ushahidi has been applied in many other conflict contexts, for example to report on violence in Syria.[15]

Moreover, GIS, drones and satellite imagery help to overcome territorial access problems and reduce the security risks and costs associated with data-gathering on the ground (Hirblinger/Morrison/Puig Larrauri 2020). While these technologies have in the past mainly been used by international organizations such as the UN,[16] which have significant resources at their disposal, crowdsourcing technology is an important low-cost alternative for smaller organizations and there is a growing number of open-source satellite imagery analysis tools available.[17]

Another innovation is automated data analysis using Artificial Intelligence (AI). With the help of Machine Learning (ML), Natural Language Processing (NLP) and pattern recognition, large amounts of data can be analyzed in a relatively short time. This enables peacebuilders to make use of new data sources which they did not have the capacity to access before. The automatized 'scraping' and analysis of data from online media allow large-scale sentiment analysis to be conducted, for instance. The acceleration of data processing allows organizations to monitor developments on the ground in real time. Multilateral actors such as the UN (through its Global Pulse initiative[18]), the European Union (EU Conflict Early Warning System[19]), and the African Union (Continental Early Warning System[20]) have, for some time, been integrating these data analysis tools into their conflict prevention programs to monitor regional peace and security indicators. Social media data-scraping and data analytics tools in particular are now frequently used by smaller organizations. Peacebuilders conduct social media analysis to monitor online hate speech and disinformation and digitally map where and how it is spreading.

Beyond improving conflict analysis through accelerated data collection and analysis, new digital tools also bring crucial innovations for early warning systems, allowing the findings of these analyses to be shared in real time and with a broader audience (Panic 2020: 22). In this way, affected communities can be reached and warned directly and independently, with no involvement by local government entities that might slow down or even block the response

---

15 For more examples see https://www.ushahidi.com/uploads/case-studies/ImpactReport_2018.pdf.

16 For example, the UN Geospatial Information Section (UN GIS) (https://www.un.org/Depts/Cartographic/english/htmain.htm) and UNOSAT (https://unitar.org/sustainable-development-goals/satellite-analysis-and-applied-research).

17 UNDPPA/HD 2019: 12. Examples are 'Airbus Defence and Space', 'Global Incident Map', 'Jane's Satellite Imagery Analysis', 'Liveuamap', 'MDA Geospatial Services' and 'Ushahidi'.

18 https://www.unglobalpulse.org/

19 https://knowledge4policy.ec.europa.eu/publication/eu-conflict-early-warning-system-objectives-process-guidance-implementation_en

20 https://au.int/en/directorates/conflict-prevention-and-early-warning

Box 3: Una Hakika? – Monitoring and Mitigating Dangerous Rumors in Kenya

'Una Hakika?' ('Are you sure?') is a Kenyan initiative that crowdsources information about dangerous rumors, providing local communities with ways to report and verify rumors using mobile phones. The initiative was founded by The Sentinel Project, a Canadian NGO, in cooperation with local actors in the context of the 2013 elections in Kenya where the widespread of disinformation fueled violence and inter-communal tensions. The initiative set up a free mobile phone-based reporting system as a rumor verification hotline. As well as text messaging and phone calls, users can report rumors via a website or a trained community ambassador. In a next step, project staffers analyze the incoming submissions to prioritize which to act on first, with reports of violence taking precedence. The initiative also emphasizes the importance of building trust in its activities by providing users with feedback on their submissions and signaling that the initiative takes action in a timely manner. Once it has been determined which rumors to address first, staffers try to verify the information provided, consulting a network of trusted stakeholders. The initiative engages a wide variety of sources from civil society, local media outlets, international NGOs, UN agencies, government officials and local leaders. It emphasizes the importance of consulting multiple sources regarding the mitigation of bias but also aims to gain multiple perspectives and gather as much information as possible. To streamline the gathering, analysis and categorization of reported rumors, the organization developed the free and open source software 'WikiRumours', a web- and mobile-based platform that is designed to optimize the triaging and response to false information. To identify the best way to respond to a rumor, the initiative consults with stakeholders such as community volunteers, local leaders and government authorities. Response strategies include mass messaging to spread verified information, in-person engagement and advocacy for government action. The initiative has also expanded its activities to other parts of Kenya such as the Kakuma Refugee Camp and nearby areas of northwestern Kenya and has recently been used to fight disinformation about COVID-19. The Sentinel Project also used Una Hakika? as a model for similar initiatives in other countries, such as Uganda and South Sudan.

For more information see: www.unahakika.org

mechanism for political or capacity reasons. Equipping citizens with digital tools to verify/falsify information and rumors is an important addition to this. For example, Una Hakika?, a Kenyan initiative established in the context of election violence in 2013, provides users with a way to quickly report dangerous rumors via a mobile phone-based hotline and uses mass messaging to spread verified information (see Box 3). Early warning tools not only help to improve communication with affected populations; they can also support peace activists and organizations in building protection systems for themselves. With support from the GIZ Peace Fund, Movilizatorio, a Colombian NGO, has recently developed an app for self-protection and early warning through which activists can build a network for collective action and exchange information on perceived threats.[21]

Involving local voices is a crucial first step in making conflict analysis and early warning processes more inclusive. Beyond participatory data-gathering, this should, however, also extend to feeding this information back to local communities and encouraging them to mobilize collective early response (Puig Larrauri et al. 2015). Besides preventing these processes from being extractive and disempowering of communities, this helps to address a major obstacle to conflict prevention – the lack of resources or blocked authorities that prevent adequate early responses to emerging tensions.

3.1.2 Conflict Transformation

Often subsumed under the term 'digital mediation', new technologies offer a number of strategic applications to innovate conflict transformation. Peacebuilders may use digital tools to make peace processes more inclusive, and to facilitate intergroup dialogue and bottom-up initiatives (forms of engagement), to share information with the public and make peace processes more

[21] https://www.movilizatorio.org; see also GIZ 2020: 51.

Box 4: Digital Inclusion of Civil Society in the Libyan National Conference Process

In the run-up to the Libyan National Conference, the UN Special Representative of the Secretary-General for Libya invited the Centre for Humanitarian Dialogue (HD) to organize preparatory consultations on the objectives and strategy of the conference. The objective of the consultations was to provide an opportunity for Libyans from all parts of society to voice their opinions on key issues relating to the conflict and the future of the Libyan state. The consultation process was the first bottom-up and national process to occur in Libya for decades and aimed to reach out to those who had previously been left out of the elite political dialogue.

While in-person consultations constituted the main element of the process, it was also supported through participatory online campaigns. The aim of the online campaigning was to engage with politically and geographically marginalized groups that were unable to participate in public events. Citizens had the chance to participate in the process through an online platform, by submitting completed questionnaires and email contributions. The website also provided information on the various options for participating in the consultations and on upcoming events and shared summaries and visual content from past events. Social media were also used to promote the consultations online and to enable direct communication with Libyan citizens throughout the country. The social media campaign reached a total of 1.8 million Libyans. Half a million comments were collected on Facebook and Twitter from around 130,000 followers, together with 2,000 formal online submissions to the website, which included academic papers, joint proposals from Libyan organizations and individual contributions from citizens. The collected submissions were analyzed qualitatively and summarized in the final report of the National Conference Process. While the digital platform was a major element in increasing civil society participation in the conference process, it did not meet expectations on increasing the participation of marginalized groups such as women, as participation patterns were similar to the offline meetings.

For more information see: Centre for Humanitarian Dialogue 2018

transparent (strategic communication), or to monitor public opinion on peace negotiations in real time and to evaluate citizens' needs and opinions (access to information).

The innovative potential of digital technologies for conflict mediation is most evident in the context of civil society representation in peace processes, often referred to as 'digital inclusion'. Digital technologies offer new opportunities for more inclusive peace processes by involving a wider and more diverse audience in the mediation process – without necessarily crowding the formal negotiating table. Social media, online surveys, text messaging apps or crowdsourcing platforms provide ways to involve civil society and give local actors a stronger voice (Hirblinger 2020). For example, in Libya, the HD Centre established an online platform to collect inputs from academia, civil society organizations and individuals regarding their priorities for the agenda of the Libyan National Conference in 2018 (see Box 4).[22]

Digital platforms can also facilitate intergroup dialogue, allowing citizens from both sides of a conflict to meet online when fragile contexts do not allow physical gatherings. Providing citizens with the opportunity to self-organize and connect across conflict lines, digital technologies also enable bottom-up projects such as the Donbass Dialogue, an online dialogue platform that brings together communities from both sides of the conflict in Ukraine and which was initiated by citizens.[23]

Digital technologies are an important tool in making peace processes more transparent. Mediators can use social media and data visualization to inform citizens regularly about the developments in the process and make their mandate easier for the general public to understand (Lanz/Eleiba 2018). Social media analysis can be used by mediators to measure the mood in the broader population and to better understand their needs as well as their attitude towards the peace process. As public dialogue shifts online and digital platforms shape conflict and peace narratives, it is increasingly relevant for mediators to be aware of these online discourses as they

[22] See Centre for Humanitarian Dialogue 2018; and www.multaqawatani.ly.

[23] https://www.donbassdialog.org.ua/

might also influence the behavior of the conflict parties. Mediators can apply this knowledge in real time to adapt facilitation and public communication strategies.

While digital technologies make an important contribution to increasing the inclusiveness and transparency of peace processes, they might also reinforce certain patterns of exclusion within society, as marginalized groups might have less access to digital participation processes (e.g., due to language, gender, location, literacy). Open-source data might be biased, and online discussions are unlikely to adequately represent marginalized groups. Analysis of social media content should therefore be complemented with curated data collection through online focus groups or targeted surveys, for instance (Hirblinger/Morrison/Puig Larrauri 2020).

3.1.3 Transitional Justice and Reconciliation

Improving capacities for monitoring, documenting and reporting violent incidents and human rights violations through the use of digital technologies has proven crucial for accountability mechanisms in the context of transitional justice. Crowdsourcing technology, drones and satellite imagery allow access to information even in fragile contexts, AI-enabled data processing software facilitates the analysis and validation of the gathered information, and blockchain technology can help to improve the security of stored evidence. In the field of reconciliation, digital platforms and various forms of digital media provide new ways of preserving memories and sharing experiences.

Digital technology helps to better evidence war crimes for prosecution, increasing the amount and diversity of information that can be recorded during a conflict and enabling the often vast amount of evidence to be analyzed more quickly (Widmer/Grossenbacher 2019). On-the-ground verification of war crimes is often associated with high security risks and relevant sites might not be accessible at all. Human rights organizations have therefore increasingly turned to crowdsourcing mobile photos and videos to gather evidence. Witnessing tools that gather

Box 5: 'Yemeni Archive' – Documenting Human Rights Violations in the Yemen War

In 2018, Yemeni Archive began compiling a database of videos and photos documenting human rights abuses by conflict parties in Yemen. The platform was founded by Mnemonic, a non-profit organization made up of human rights advocates, archivists, technologists and open-source investigators. The goal of the platform is to preserve, enhance and memorialize documentation of human rights violations and other crimes committed by all parties to the conflict in Yemen for use in advocacy, justice and accountability.

The gathered content includes submissions from journalists and civilians, as well as open-source videos from social media platforms such as Facebook and YouTube, and is preserved with blockchain technology to protect the data from being tampered with. The archive stores over half a million videos and social media posts and the initiative has so far verified and published 8,000 of these videos in a searchable online database.

To improve data-gathering and processing, the organization also collaborated with technology experts to build open-source tools to automatically download material and to automate the object recognition in videos and images. These digital tools were essential for processing the vast amount of crowdsourced material. Accelerating the archiving of online content has also proven critical as evidence uploaded to social media platforms might quickly be removed by platform administrators. The initiative follows a policy of transparency in its tools, findings and methodologies and making verified content publicly available and accessible for the purpose of reporting, advocacy and accountability processes. Efforts to share the gathered data with a broader audience also include training for activists, journalists, human rights defenders and lawyers on using the organization's digital tools and methodologies for their own investigative work.

Along with the Global Legal Action Network (GLAN), a non-profit that takes legal action against governments for human rights violations, the initiative has also started to curate evidence of specific human rights violations in a separate database (the GLAN Airstrike Database) and to bring legal actions before various domestic and international courts.

For more information see: www.yemeniarchive.org

individuals' conflict experience can also serve advocacy purposes, making human rights violations visible, and help to raise awareness among third parties (Firchow et al. 2017). For instance, the Yemeni Archive platform documents human rights abuses committed in the context of the Yemen conflict, gathering submissions from journalists, activists, and civilians, as well as open-source data from social media platforms (see Box 5). While crowdsourcing evidence often results in a large quantity of material that overwhelms activists' analysis and verification capacities, AI could potentially offer a solution by automatizing these processes (Hao 2020).

In the field of reconciliation, digital platforms have shown to be a promising tool to increase inclusivity. Digital participatory platforms provide a space for victims to share their experiences and engage in dialogue across conflict party lines (infoDev/World Bank 2013). Providing evidence in a variety of digital media, such as video and audio material, also makes reconciliation processes more accessible and helps to overcome the illiteracy barrier (Widmer/Grossenbacher 2019). Digital platforms also allow better inclusion of diaspora communities, which have played a crucial role in many reconciliation processes.[24] More recently, the use of digital technologies is being discussed in the context of cases of missing persons. Notably, the International Committee of the Red Cross (ICRC) is exploring the potential of AI for the reconciliation of name lists and application of facial recognition technology to photo databases to improve the organization's capacity to reunite families separated by conflict (ICRC 2019).

While recent discussions on the innovative contribution of technology to transitional justice and reconciliation center on the potential use of AI for data processing, peacebuilders should not dismiss the major innovations digital tools offer in terms of empowering affected communities. Allowing individuals to share their stories with the broad public – possibly even with a global audience – offers them agency and a tool for advocacy to raise awareness of their suffering (Firchow et al. 2017: 9).

3.2 Shifting Power Balances Towards Local Organizations and Alternative Peacebuilding Infrastructures

Digital technologies also have a transformative effect in terms of their potential to alter power structures in the peacebuilding sector. They strengthen the role of local organizations, emancipate civil society initiatives, and pave the way for alternative infrastructures of peacebuilding. They challenge existing organizational models and promote horizontal networks and decentralized decision-making by giving a large number of actors the opportunity to gain access to information and to jointly organize actions. Digital technologies and data have become largely accessible and affordable not only to governments and international organizations but also to civil society and individuals. In this way, they enable the emergence of alternative peacebuilding infrastructures by which civil society networks organize themselves, independently of established peacebuilding actors, through 'citizen-to-citizen' initiatives (Puig Larrauri et al. 2015). Many innovations in digital peacebuilding have emerged in the Global South, often initiated by local civil society organizations. Innovating peacebuilding does not necessarily need to involve sophisticated new technologies; simple digital applications and open-source tools used by local actors to implement digital peacebuilding initiatives often produce the best results in terms of effectivity and sustainability.[25] However, despite the apparent ease of use and accessibility of digital technologies, these local initiatives are often dependent on financial and technical support from external actors.

Regarding the power balance between international organizations and local civil society actors, digital technologies may not necessarily induce a shift towards local agency, but instead often reinforce established hierarchies. With decision-making processes and international fora shifting

[24] The digital inclusion process for diaspora communities in the context of the Syria conflict is notable; see Tenove 2019.

[25] Interview with Lisa Schirch, Toda Peace Institute, 5 February 2021.

online, larger organizations might take an even more prominent role in the peacebuilding field when internet connectivity becomes a 'new form of power' (International Alert 2020). Moreover, employing certain peace technologies requires specific know-how that might be too costly for smaller organizations to develop in-house or to access by engaging external experts, especially regarding more advanced technologies (Panic 2020: 27). Small organizations are also at a disadvantage when it comes to negotiating access to social media data, since they have diminished access to or leverage over big technology firms. Civil society organizations might, therefore, not have the necessary resources to take full advantage of the possibilities, tech-enabled peacebuilding offers. In the context of power balances between headquarters and local staff within multilateral organizations or globally active NGOs, digitalization might even have a negative effect. Digitalizing workflows and internal communication can exclude local staff from decision-making processes if they do not have access to the same digital infrastructure such as good internet connectivity. Likewise, the analysis of locally collected data and the associated decision-making power is often carried out by technical staff who are based in the headquarters (Read/Tithe/Mac Ginty 2016).

The transformative potential attributed to digital technologies with regard to the emancipation of local civil society has, to date, only been realized to a limited extent. While digital participatory platforms have been celebrated for scaling up the inclusivity of peacebuilding processes, peacebuilders have to acknowledge that 'digital inclusion' should also extend to the design and management of peacebuilding initiatives. The data gathered through crowdsourcing could, for instance, help local communities to better formulate their own priorities and to take a more active role in peacebuilding. Instead, their role is currently often limited to the provision of data, while the opportunity of initiating, designing and financing such digital projects as well as analyzing and implementing their results is still reserved for more established peacebuilding actors (Read/Taithe/Mac Ginty 2016). Discussions around 'data colonialism' address how international actors undermine local populations' rights to govern the collection, usage and ownership of their own data (Couldry/Mejias 2019).

However, whether or not the availability of new technologies and digitalization offer an opportunity for local actors and civil society to engage in peacebuilding depends to a large extent on the conflict context and the available infrastructure on the ground. Innovation and digital peacebuilding do not necessarily require the development of new peacetech tools; they can also rely on existing technologies and platforms. Often, smaller organizations do not need the same digital product as multilateral actors, who require far more advanced and expensive technologies since they implement projects on a larger scale and with a longer-term objective. Smaller organizations are more flexible and can often achieve their peacebuilding goals with cheaper and less elaborate digital tools.[26] Besides, many technology companies and peacetech start-ups offer their tools, as well as training on how to use them, to non-profit organizations for free.[27] There is also an increasing amount of free resources and self-learning courses available online that provide peacebuilders with an overview of current developments and best practices in digital peacebuilding.[28] Opportunities for local actors and small organizations to apply for financial support for the digitalization of their activities are on the rise as well. In the context of the COVID-19 pandemic, initiatives such as the Digital Inclusion Fund[29] have provided many local peacebuilders with micro-grants to give them access to digital tools they needed to continue their activities.

---

[26] Interview with Julie Hawke, Build Up, 12 January 2021.

[27] Interview with Branka Panic, AI for Peace, 1 February 2021.

[28] See, for example, the online course 'Digital Peacebuilding 101' offered by Build Up: https://howtobuildup.org/community-learning/courses/digital-peacebuilding-101-introducing-technology-for-peacebuilding/.

[29] https://www.shiftpowerforpeace.org/en/a/

4. Challenges and Risks of Digital Peacebuilding

While a growing number of international and local actors are adopting digital peacebuilding strategies, they still face a wide range of challenges often due to the difficult contexts they operate in. The effectivity of technology-enabled peacebuilding initiatives is contingent on structural context factors (Section 4.1), such as the political and technological ecosystem on the ground and operational complications (4.2). The innovation potential that new technologies offer for peacebuilding has to be weighed up with the possible risks that their application to fragile contexts poses and peacebuilders have to be aware of unintended negative consequences the use of peace technologies might entail (Section 4.3). The following chapters map these challenges and risks and give an overview of existing guidelines and frameworks for the implementation of conflict-sensitive and effective digital peacebuilding initiatives (Section 4.5).

4.1 Dependence on the Political and Technological Ecosystem

Using digital technologies for peacebuilding usually entails a certain dependence on external actors. Digital peacebuilding heavily relies on technologies that are governed by states or technology companies, from the provision of internet and telecommunication services to online platforms such as Facebook and YouTube. Peacebuilders have to be aware that their ability to implement technology-based initiatives often depends on the cooperation of local governments and technology firms and that the political situation on the ground as well as companies' user policies might change quickly and restrict their access to digital services.

Political Context and Dependence on Local Governments

Whether peacebuilding technologies can be used effectively or at all often depends on the political context and the cooperation of local governments. In many conflict-affected contexts, digital peacebuilding initiatives are challenged by the repressive governance of the information and communication infrastructure. This means that technology may not be available at all in situations when it is needed most. If governments shut down cell phone networks and internet access in order to prevent the organization of protests during elections, this also closes down digital peacebuilding initiatives that rely on civilians reporting violent incidents or accessing early-warning information online or via text messaging. Similarly, digital inclusion in peace processes requires the local population to believe that participation in the process benefits them and their communities. Particularly in contexts in which trust in the political regime and therefore also the peace process is low, this might not be the case, making the digital involvement of the broad civil society difficult to realize (Read/Taithe/Mac Ginty 2016). The greater the government's potential for technological repression, the narrower the space for digital peacebuilding and civil society inclusion will turn out to be.

Dependence on the Technology Sector

Besides the political context, the technological ecosystem in which peacebuilders operate can pose challenges to effective implementation of their peacetech applications. Digitalizing peacebuilding comes with a certain dependence on the technology sector, especially if peacebuilders rely on 'off-the-shelf' tools and platforms provided by global technology companies (Berg/Hirblinger 2020). Getting access to social media data, for example, can require peacebuilders to negotiate with big tech platforms. For smaller peacebuilding organizations, this might be problematic due to a lack of leverage, difficulties in finding the right 'language' to communicate their needs, and the challenges of approaching the relevant entities due to the often complex organizational structures of these companies.[30] Community-building and knowledge-

[30] Interview with Maude Morrison, Centre for Humanitarian Dialogue (HD), 15 January 2021.

sharing could help to overcome these challenges and collectively find strategies for approaching and negotiating with big tech firms.

4.2 Operational Stumbling Blocks

Peacebuilders also face obstacles on the operational level that affect the efficiency and impact of digital initiatives. Insufficient human resources and lack of long-term funding often limit the feasibility and sustainability of tech-enabled initiatives. Also, technology-centered planning that fails to incorporate local needs often leads to ineffective outcomes. Challenges with impact measurement and knowledge-sharing make it difficult to identify opportunities for improvement and develop best practices.

Insufficient Capacities and Short-Term Funding

Failure of digital peacebuilding projects can often be traced back to misjudgments regarding the required financial or human resources. The successful implementation of peace technologies often requires investments in organizational development and staff capacity that take considerable resources and time. False expectations about increased efficiency or saved costs due to automation and digitalization can cause organizations to insufficiently budget for human resources that are often required for the effective operation and maintenance of new technologies. Many crowdsourcing projects, for instance, have the problem that the amount of data collected exceeds their processing capacity. This was the case for an online platform created in the context of the national peace process in Colombia that enabled the population to submit proposals for the negotiating agenda either physically or electronically. The website received 67,371 contributions, which exceeded the project's analytical capacity (UNDPPA/HD 2019). Many digital peacebuilding initiatives have a limited impact also due to the lack of long-term funding. Local initiatives in particular suffer from the lack of sustainable funding sources and 'seed-funding' often ends just as newly established programs and tools reach the full development stage that would allow for meaningful impact (SecDev Group 2017: 5).

Shortcomings of Technology-Oriented Planning and Design

In the design of technology-based peacebuilding, there is generally a tension between the planning around a particular technology and the planning towards a programmatic goal (Brown 2014). Shifting from goal-oriented to technology-oriented program planning risks the actual peacebuilding goal fading into the background or being redefined according to the technological possibilities. A strong focus on technology can even lead to other (necessary) measures being replaced because they do not fit into the new objective or cannot be integrated into the new digital workflows. In practice, digital peacebuilding initiatives tend to reflect what is technologically possible and not what is needed on the ground. Moreover, peace technologies, especially if designed by global or Western-based tech companies, often fail to consult peacebuilding experts and local communities in the design and testing process (Panic 2020: 27). As a result, many technologies on the market are not sufficiently adapted to local conditions to meet peacebuilding goals and communities' needs effectively.

Challenges with Impact Measurement and Knowledge-Sharing

Comprehensive impact analysis frameworks or best practices that would allow peacebuilders to measure and evaluate the impact of peacetech tools are rare. So far, evaluations of technology-based peace initiatives have mainly been case-specific, anecdotal or limited to the operational level (Currion 2011: 41). Peacebuilding initiatives and especially mediation processes are often bound to high standards of confidentiality. Sharing experiences, developing synergies and building a knowledge community are difficult to realize under these conditions (Hirblinger 2020: 40).

4.3 Unintended Negative Consequences

The implementation of digital peacebuilding strategies might entail unintended negative consequences, from jeopardizing citizens' or conflict parties' trust in the process, to reinforcing discriminatory structures, and putting already vulnerable populations at risk.

Challenges with Trust *in* Technology and Trust-Building *through* Technology

The effective functioning of peace technologies and clear communication of what digital peacebuilding can offer, and where its limits lie, are key to securing local populations' trust in digital peacebuilding initiatives. However, the promise of digital inclusion might create unrealistic expectations, which, when not met, threaten to damage trust in peacebuilders and cause individuals to turn their back on the process instead. Similarly, when fighting disinformation, guaranteeing that fact-checking services are reliable and timely is crucial to gain the trust of their users, as they otherwise create even greater confusion and mistrust in official information sources (Singh 2020).

Moreover, digitalization replaces face-to-face interaction, which is, however, crucial for trust-building. When shifting mediation online and replacing field visits with remote data-gathering capacities, peacebuilders have to carefully weigh up the benefits of digitalized processes with the possible loss of trust among conflict parties (Diaz-Prinz 2020) but also between peacebuilders and local communities (Mac Ginty 2017).

Digital Divide and Discriminatory Technology

While the use of digital technologies promises to make peacebuilding more inclusive and participatory, applying these new tools in fragile contexts – where limited access to technological infrastructure, digital illiteracy and marginalization construct a 'digital divide' within societies – might replicate and reinforce structures of discrimination and amplify root causes of violence (Faith 2019). Exclusion from participatory digital peacebuilding processes and online discourses also means that these social groups and their needs are not represented in the data gathered, thus leading to a biased view of what constitutes the 'public opinion' or 'local needs' and challenging the value and legitimacy of digital content analysis (Hirblinger 2020).

Moreover, digital technologies are not a 'neutral tool': the values of technology developers, the contexts in which technology is tested, and the data sets algorithms are trained with influence how technologies function (Mac Ginty 2017). Depending on who develops digital tools and under which circumstances, their application in peacebuilding might thus produce biased results and reinforce existing patterns of discrimination (Ebadi 2018).

Data Security Risks and Misuse of Sensitive Data

Data security risks are inherent in the use of digital technologies and data breaches cannot be ruled out completely, even when implementing high cybersecurity standards. These risks are already evident in non-conflict settings and become even more pressing in fragile contexts, where data security is difficult to implement and the collected data often holds very sensitive information. In these contexts, data breaches could inflict considerable harm on already vulnerable populations, if data falls into the hands of warring factions or repressive governments, for instance (Garcia 2018).

4.4 Overcoming Challenges and Mitigating Risks

New technologies offer an important innovation opportunity for peacebuilding, but their integration still poses a considerable challenge to many organizations and might even risk creating new divisions *within* and threats *to* affected communities. To allow for an effective use of peace

technologies and to minimize associated risks, the guidelines discussed in the following section provide peacebuilders with a frame of reference and will help them to draw realistic goals (see Box 6 for an overview).

Each digital peacebuilding initiative should undertake its own context-specific 'do no harm' and risk assessments and consider ethical guidelines in its planning across all stages of intervention. These assessments usually include reflections on risks relating to data security and privacy, as well as on unintended discrimination and ethical issues relating to informed consent and data ownership. Recommendations include the development of context-specific risk analysis and mitigation frameworks that consider all phases of the project or program. Various international organizations and specialized centers have developed resources that help peacebuilders with technology-related risk management. For example, JustPeace Labs developed a toolkit on how to apply ethical and 'do no harm' standards in practice, providing peacebuilders with step-by-step guidelines throughout a project lifecycle (from strategy and planning to software engineering and design; provision of technology; data-gathering, storage, analysis and dissemination; provision of options for support and legal recourse; and data archiving) (JustPeace Labs 2017). As well as policy guidelines, several organizations offer rapid response emergency assistance and training to help smaller initiatives to better understand their own digital risks and to develop practices to protect their data and online operations.[31] For guidance on ethical data governance in fragile contexts, peacebuilders can learn from the humanitarian sector, which has produced comprehensive guidelines such as the International Committee of the Red Cross (ICRC) Handbook on Data Protection in Humanitarian Action (Kuner/Marelli 2020). Discussions in the humanitarian field also shed light on issues regarding the level of data anonymization, pointing out the risks of 'demographically identifiable data' [32] that are especially crucial in the context of big datasets, as well as discussing the development of remedy mechanisms for victims of data protection violations.

Beyond this, a thorough context analysis helps to identify structural challenges that the implementation of tech-based initiatives is likely to face. This should include analyzing the political context and the capabilities of local governments for technological repression, as well as mapping the technological ecosystem in terms of the infrastructures provided on the ground and identifying which ICTs and online platforms are used most by local communities. The technology ecosystem mapping should also include an analysis of technology users' demography and differences in the population's access to digital tools and digital literacy, in order to evaluate risks of new exclusions potentially being created due to the 'digital divide'. Pinpointing local initiatives and organizations that are actively engaged in digital peacebuilding and that might already have developed digital tools is crucial to identify opportunities for cooperation and the use of existing infrastructure.[33]

On the operational level, available guidelines also address the effectivity, efficiency and sustainability of tech-enabled initiatives. For the effectivity of an initiative, goal-oriented planning and a clear definition of the added value of a new technological component are crucial. This ensures that the intervention promotes programmatic objectives and is not tailored to the mere availability of a particular digital tool. It also emphasizes that technology should only serve as a complementary tool and should not replace non-digital activities and more traditional peacebuilding instruments. Peacebuilders should also strive for a human-centered design that considers users' context-specific needs to effectively meet peacebuilding goals (Panic 2020: 30).

Guidelines from the international development sector also provide valuable examples of best practice relating to the efficient use of digital technologies. For instance, the Principles for Digital

---

31 See UNDPPA/HD 2019: 9 and Widmer/Grossenbacher 2019: 11 for examples of existing resources and guidance.

32 For a thorough discussion on why data privacy and security considerations should go beyond the risks of 'personally identifiable information' and also address 'demographically identifiable information', see Raymond 2017.

33 Interview with Maude Morrison, Centre for Humanitarian Dialogue (HD), 15 January 2021.

Development[34] address how using openly accessible and free tools can help improve collaboration in the digital community, and how reusing and improving existing products, resources and approaches improve effectivity and efficiency. They also provide guidance on how to ensure sustainability of digital initiatives, from building programs that are adaptable, to engaging local governments and identifying partners in the local technology ecosystem.

However, while useful resources exist in other fields such as the humanitarian and international development sector, more guidelines are needed that specifically speak to the heightened ethical and security risks of using digital tools for peacebuilding. Developing more specific impact assessments and monitoring guidelines would also help to improve the evaluation of digital initiatives. Intensifying efforts to build a knowledge community on best practices in digital peacebuilding would be a first step in addressing these gaps.

5. The Road Ahead: Shifting from 'Digital Inclusion' to 'Digital Agency' and Approaching New Fields of Action in Cyberspace

As both conflict and peace stakeholders increasingly use digital technologies, the peacebuilding community has to develop a better understanding of how to identify and overcome current shortcomings of digital peacebuilding and redefine peacebuilders' role in the light of digital conflict drivers and new conflict frontiers in cyberspace. Moreover, the transformative potential that digital peacebuilding offers has so far been realized only to a limited extent. Digital technologies promise to innovate peacebuilding, especially regarding the emancipation of local civil society and alternative infrastructures of peacebuilding.

However, many participatory digital peacebuilding projects have a limited approach to inclusion and are rather 'extractive' in that the local population is often treated as a mere source of data. 'Digital inclusion' and empowering local actors should go beyond collecting data on civil societies' opinions and needs and encompass the program design and technology development phase as well, to ensure local communities' agency and ownership of digital peacebuilding programs. For instance, data obtained through crowdsourcing could, when shared with local civil society actors, help communities to collectively identify and communicate their own priorities and needs in a more targeted manner and to take a more active role in peacebuilding processes. However, how meaningful inclusion and giving affected communities more agency could look like in practice is difficult to determine. Integrating local knowledge and ensuring agency and ownership by local populations requires additional resources for coordination and might thus be difficult to implement. This might be difficult to achieve, especially with advanced data science methods and large amounts of data, which require considerable technical expertise and time to understand.[35] Local civil society's inclusion and agency in developing peacetech and tech-enabled initiatives will also have to include efforts to mediate discriminatory structures within society to prevent digital peacebuilding initiatives from reinforcing the marginalization of certain groups. Developing a better understanding of these dynamics, and coming up with strategies on how to shift from 'inclusion' of civil society to 'agency' *in* and *through* digital peacebuilding in practice, will have to take center stage on the future agenda of digital peacebuilding. Research on the digital divide and its implications for discrimination in digital peacebuilding should also include developing metrics to measure digital inclusion and the preconditions for access to participatory digital processes (UN 2020: 24).

---

[34] The principles are: Design with the User; Understand the Existing Ecosystem; Design for Scale; Build for Sustainability; Be Data Driven; Use Open Standards, Open Data, Open Source, and Open Innovation; Reuse and Improve; Address Privacy & Security; Be Collaborative. https://digitalprinciples.org.

[35] Interview with Branka Panic, AI for Peace, 1 February 2021.

Box 6: Guidelines for Digital Peacebuilding

There is a growing body of resources that developed best practices for digital peacebuilding. These guidelines usually include recommendations on risk and mitigation frameworks, context analysis and practical issues on the operational level relating to effectivity, efficiency and sustainability of digital initiatives.

(1) Security Risk Assessment and Mitigation Frameworks:

Digital peacebuilders should conduct a context-specific security risk analysis and develop mitigation frameworks at the start of a project. This should include the following:

- Analyze risks to the organization itself, including risks to its ability to gain and maintain access to data and users;
- Consider rights of and risks to individuals, demographic groups and communities;
- Develop possible scenarios of data breaches and data misuse by third parties;
- Plan for secure data storage options for the time when a project has ended;
- Develop data privacy and data security policies, as well as remedy mechanisms.

Numerous international organizations and specialized centers have developed resources that help peacebuilders with technology-related risk management. This includes policy guidelines, training to help smaller organizations to better understand their own digital risks and to develop practices to protect their data and online operations, and rapid-response emergency assistance.

(2) Context Analysis:

A thorough context analysis helps to identify structural challenges that the implementation of tech-based initiatives is likely to face. This should include analyzing the political context and mapping the technology ecosystem:

Technology Ecosystem:

- Assess which digital tool is most feasible as regards the technological infrastructure provided on the ground and determine which ICTs and online platforms are used most by local communities;
- Identify local initiatives and organizations that are actively engaged in digital peacebuilding and might already have developed digital tools to identify opportunities for cooperation;
- Consider how a 'digital divide' and power dynamics within society influence the selection of participants and how the initiative might reproduce discriminatory structures. Develop strategies to remedy any exclusions.

Political Context:

- Identify whether and how the use of and access to technology infrastructure might be restricted, and who governs access to the various technologies;
- Analyze how a repressive government or lack of trust in local authorities might influence citizens' ability or willingness to participate;
- Consider how political changes might affect the use of technology.

Peacebuilders have to be aware that their ability to implement technology-based initiatives often depends on the cooperation of local governments and technology firms and that the political situation on the ground as well as companies' user policies might change quickly and restrict their access to digital services.

(3) Effectivity, Efficiency, and Sustainability:

On an operational level, available guidelines also address the effectivity, efficiency and sustainability of tech-enabled initiatives. Recommendations include:

- Prioritize goal-oriented over technology-oriented planning and define the added value of new technological component;
- Use tech-enabled initiatives as complementary tools to traditional peacebuilding instruments and processes;
- Apply a human-centered design process and take into account the needs of the local communities;
- Where possible, cooperate or coordinate with other digital peacebuilders, use openly accessible tools to improve knowledge-sharing in the digital peacebuilding community and avoid duplication of work;
- Plan for sustainability from the start, by striving for long-term funding, designing initiatives and tools that are adaptable to other contexts and identify partners in the local technology ecosystem.

While there is a growing set of guidelines that address these shortcomings and develop best practices for digital peacebuilding, this is less the case for the implications of digitalization on conflict dynamics and how they impact the work of peacebuilders. As conflict parties and stakeholders increasingly rely on digital technologies, peacebuilders as well will have to build capacities to address new challenges of technological conflict drivers. Despite the growing awareness that digital technologies might accelerate social tensions and conflict, more research is needed on how these new dynamics alter the parameters of conflict resolution and possibly undermine peacebuilding efforts. This should also include identifying new conflict stakeholders, the type of technology they use, and which social groups are most vulnerable to the new threats they pose. To that end, peacebuilders should strive to build a knowledge community, reaching out to technical communities and experts from cybersecurity and cyber diplomacy. Peacebuilders should also further explore how emerging conflict frontiers in cyberspace, such as rising political tensions due to cyberattacks or online polarization, open up new fields of action for them. Civil society peacebuilders' experience and knowledge can make a valuable contribution to a better understanding and resolution of these new challenges, also beyond contexts of conventional armed conflict.

With regard to both digital peacebuilding and digital conflict drivers, more research is needed on their implications for marginalized and vulnerable social groups. For instance, the gender-specific implications in particular are still underexplored. Further research is needed on the digital divide and women's invisibility in datasets and exclusion from digital dialogue processes, but also on the potential of digital peacebuilding to combat gender-based violence and support women's agency and empowerment in conflict contexts.[36] Regarding digital conflict drivers, such as the abuse of surveillance technology and online violence, (Naciri 2020) more attention needs to be paid to gender-specific vulnerabilities.

Lastly, digital technology's transformative effect on peacebuilding can be embedded within a broader discussion in the field of international peacebuilding: the critique of the liberal peacebuilding paradigm, which exposes and denounces the international peacebuilding architecture for its state-centric approach and axiom of Western superiority. Digital technologies and their emancipating potential for local organizations and civil society challenge these assumptions. The rise of grassroots initiatives proves that innovation in peacebuilding does not necessarily rely on external support but is often developed in conflict contexts by local actors. The influence of digital technology in opening up new forms of violence and spaces in which conflicts are fought also obliges peacebuilders to reconsider their own role. Beyond contexts of conventional armed conflict, peacebuilders have started to expand their activities to new fields of action in cyberspace. The rising threat digital technologies pose to peace and democracy affects societies globally. Therefore, the knowledge and capacity the peacebuilding sector offers in the fight against these new threats are not only crucial for the Global South; they are of increased relevance in the context of Western democracies as well.[37] Build Up's The Commons (see Box 2) is one example. Expanding peacebuilding to new fields of actions should therefore be considered not only with regard to cyberspace but also in terms of geographical areas. Addressing the challenges of global digitalization will have to involve advocacy work on the need to reconsider the operational areas of peacebuilding in order to include new geographic locations and threats below and beyond the level of armed conflict.

[36] See, for example, the case of Sudanese women's role in protest movements: Robertson/Ayazi 2019.

[37] Interview with Lisa Schirch, Toda Peace Institute, 5 February 2021.

6. References

Accessnow 2017: The 'Doubleswitch' Social Media Attack. A Threat to Advocates in Venezuela and Worldwide, Access Now, 09.06.2017. https://www.accessnow.org/doubleswitch-attack/ (14.04.2021).

Amnesty International 2018: Amnesty International Among Targets of NSO-powered Campaign, 01.08.2018. https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/ (14.04.2021).

Amnesty International 2021: 'These walls have ears'. The chilling effect of surveillance in South Sudan. London: Amnesty International. https://www.amnesty.org/en/documents/afr65/3577/2021/en/ (14.04.2021).

Benesch, Susan 2014: Countering Dangerous Speech. New Ideas for Genocide Prevention, Dangerous Speech Project, Harvard University: Berkman Klein Center for Internet & Society. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3686876 (14.04.2021).

Berg, Elin/Hirblinger, Andreas 2020: Pandemic Peacebuilding. How to Leverage Digitalisation for Societal Resilience in: Africa, Accord, 26.08.2020. https://www.accord.org.za/analysis/pandemic-peacebuilding-how-to-leverage-digitalisation-for-societal-resilience-in-africa/ (14.04.2021).

Brown, Rachel. 2014: Designing Peacebuilding Projects that Utilize Technology, White Paper, Build Peace Conference 2014. http://lyvoices.org/wp-content/uploads/2014/04/BP14-Panel-project-design.pdf (14.04.2021).

Build Up 2018: Innovative Peacebuilding in Syria II – An Update on the Strategic Use of Technology to Build Peace in the Syrian Context. https://howtobuildup.org/wp-content/uploads/2020/06/INNOVATIVE-PEACEBUILDING-IN-SYRIA-II.pdf (18.04.2021).

Build Up 2019: The Commons – An Intervention to Depolarize Political Conversations on Twitter and Facebook in the USA, 2019 Evaluation Report. https://howtobuildup.org/wp-content/uploads/2020/04/TheCommons-2019-Report_final.pdf (15.04.2021).

Caltagirone, Sergio 2019: Industrial Cyber Attacks. A Humanitarian Crisis in the Making, ICRC, 03.12.2019. https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/ (14.04.2021).

Centre for Humanitarian Dialogue (HD) 2018: The Libyan National Conference Process, Geneva: HD. https://www.hdcentre.org/wp-content/uploads/2018/11/Libyan-NCP-Report_English_web.pdf (14.04.2021).

Cottary, Olivier/Puig Larrauri, Helena 2017: Technology at the Service of Peace, 24.04.2017, SIPRI. https://www.sipri.org/commentary/blog/2017/technology-service-peace (14.04.2021).

Couldry, Nick/Mejias, Ulises A. 2019: Data Colonialism. Rethinking Big Data's Relation to the Contemporary Subject, in: Television & New Media, 20 (4), 336-349.

Currion, Paul 2011 : Conclusion, in : Stauffacher, Daniel et al. (ed.): Peacebuilding in the Information Age. Sifting Hype from Reality, Cambridge: ICT4Peace Foundation, Harvard University (Georgia Institute of Technology), 39-42. https://ict4peace.org/activities/foundation/peacebuilding-in-the-information-age-sifting-hype-from-reality/ (14.04.2021).

Danyk, Yuriy/Maliarchuk, Tamara/Briggs, Chad 2017: Hybrid War. High-tech, Information and Cyber Conflicts, in: Connections, 16 (2), 5-24.

Desai, Shweta/Amarasingam, Amaranth 2020: #CoronaJihad. COVID-19, Misinformation, and Anti-Muslim Violence in India, ISD Global. https://strongcitiesnetwork.org/en/coronajihad-covid-19-misinformation-and-anti-muslim-violence-in-india/ (14.04.2021).

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) 2020: Smart Prevention. Digital Approaches in the Peace and Security Sector of Development Cooperation, Eschborn: GIZ. https://toolkit-digitalisierung.de/app/uploads/2020/09/Smart-Prevention_engl_Web.pdf (14.04.2021).

Diaz-Prinz, Juan 2020: Yes, we Can Meet on Online. But Can we Negotiate Peace there?, United States Institute of Peace (USIP), 15.05.2020. https://www.usip.org/blog/2020/05/yes-we-can-meet-online-can-we-negotiate-peace-there (14.04.2021).

Dorn, Walter A./Webb, Stewart. 2019: Cyberpeacekeeping. New Ways to Prevent and Manage Cyberattacks, in: International Journal of Cyber Warfare and Terrorism (IJCWT), 9 (1), 19-30.

Ebadi, Bushra 2018: Artificial Intelligence Could Magnify Social Inequality, CIGI, 08.05.2018. https://www.cigionline.org/articles/artificial-intelligence-could-magnify-social-inequality (14.04.2021).

Faith, Becky 2019: Digital Technologies Use in Development Programme Design, Delivery and M&E in Fragile and Conflict-Affected Setting, K4D Helpdesk Report, Brighton: UK: Institute of Development Studies.
http://opendocs.ids.ac.uk/opendocs/handle/123456789/14537 (14.04.2021).

Faris, Rob/Gassner, Urs/Ashrar, Amar et al. 2016: Understanding Harmful Speech Online, Berkman Klein Center for Internet and Society Research Publication, Harvard University, 08.12.2016.
https://cyber.harvard.edu/publications/2016/UnderstandingHarmfulSpeech (14.04.2021).

Firchow, Pamina et al. 2017: PeaceTech. The Liminal Spaces of Digital Technology in Peacebuilding, in: International Studies Perspectives, 18 (1), 4-42.

Garcia, Beatriz 2018: The Human Cost of Data Unshared, Brunswick Review, 15.10.2018. https://www.brunswickgroup.com/un-pulse-predictions-i8531/ (14.04.2021).

Gichuhi, C. 2019: Hateful Language Trends in South Africa During 2019 Election, PeaceTech Lab. https://www.peacetechlab.org/lab-notes/2019/12/6/hateful-language-trends-in-south-africa-during-2019-election-1 (06.12.2019).

Hao, Karen 2020: Human Rights Activists Want to Use AI to Help Prove War Crimes in Court, MIT Technology Review, 25.06.2020. https://www.technologyreview.com/2020/06/25/1004466/ai-could-help-human-rights-activists-prove-war-crimes/ (14.04.2021).

Harlander, Jonathan/Morrison, Maude 2020: Social Media Codes of Conduct: Reflections for Mediators, Centre for Humanitarian Dialogue, 18.08.2020.
https://www.hdcentre.org/updates/social-media-codes-of-conduct-reflections-for-mediators/ (14.04.2021).

Healey, Jason et al. 2014: Confidence-Building Measures in Cyberspace. A Multistakeholder Approach for Stability and Security, Atlantic Council, Brent Scowcroft Center on International Security.
https://www.atlanticcouncil.org/in-depth-research-reports/report/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security/ (14.04.2021).

Hirblinger, Andreas T. 2020: Digital Inclusion in Peacemaking. A Strategic Perspective, CCDP Working Paper 14, Geneva: Centre on Conflict, Development and Peacebuilding.
https://www.graduateinstitute.ch/sites/internet/files/2020-07/Digital%20Inclusion%20in%20Peacemaking%20A%20Strategic%20Perspective_Andreas%20Hirblinger.pdf (15.04.2021).

Hirblinger, Andreas T./Morrison, Maude/Puig Larrauri, Helena 2020: Digital Analysis. Peacemaking Potential and Promise, Accord Issue 29, London: Conciliation Resources, https://www.c-r.org/accord/pioneering-peace-pathways/digital-analysis-peacemaking-potential-and-promise (14.04.2021).

Höne, Katharina E. 2019: Mediation and Artificial Intelligence. Notes on the Future of International Conflict Resolution, Geneva: DiploFoundation. https://www.diplomacy.edu/resources/books/mediation-and-artificial-intelligence-notes-future-international-conflict (14.04.2021).

infoDev/World Bank 2013: Cables, Commissions, and Cybercafés. ICTs in Post-Conflict Liberia, Washington, D.C.: IBRD/World Bank. https://www.infodev.org/infodev-files/resource/InfodevDocuments_1206.pdf (14.04.2021).

International Alert 2020: Can We Build Peace from a Distance? The Impact of COVID-19 on the Peacebuilding Sector, Background Paper, London: International Alert. https://www.international-alert.org/sites/default/files/COVID-19-Building-Peace-Distance-EN-2020.pdf (14.04.2021).

International Committee of the Red Cross (ICRC) 2019: Embracing Digital Transformation, ICRC Blogs, 02.07.2019. https://blogs.icrc.org/inspired/2019/07/02/embracing-digital-transformation-data/ (14.04.2021).

Jenny, Joelle et al 2018: Peacemaking and New Technologies. Dilemmas and Options for Mediators, Mediation Practice Series, Geneva: Centre for Humanitarian Dialogues. https://www.hdcentre.org/wp-content/uploads/2018/12/MPS-8-Peacemaking-and-New-Technologies.pdf (14.04.2021).

JustPeace Labs 2017: Ethical Guidelines for PeaceTech, JustPeace Labs. https://justpeacelabs.org/ethical-guidelines-for-peacetech/ (14.04.2021).

Kakoma, Itonde /Marques, Edward 2020: The Future of Mediation in the Post-COVID World, Strategic Security Analysis, Issue 12, Geneva: Geneva Centre for Security Policy. https://dam.gcsp.ch/files/images/the-future-of-mediation-in-the-post-covid-world (14.04.2021).

Kane, Sean/Clayton, Govinda forthcoming, 2021: Cyber Ceasefires. Incorporating Cyber Operations in Agreements to Stop Hostilities, Zurich: Center for Security Studies (CSS) ETH Zürich.

Kausch, Kristina 2017: Cheap Havoc. How Cyber-Geopolitics Will Destabilize the Middle East, Policy Brief 35, Washington, D.C.: German Marshall Fund of the United States. https://www.gmfus.org/publications/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east (14.04.2021).

Kavanagh, Camino 2021: Digital Technologies and Civil Conflicts, Conflict Series, Brief 4, Paris: European Union Institute for Security Studies (EUISS). https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_4_2021_0.pdf (14.04.2021).

Kendall-Taylor, Andrea/Frantz, Erica/Wright, Joseph 2020: The Digital Dictators. How Technology Strengthens Autocracy, in: Foreign Affairs, March/April 2020. https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators (14.02.2021).

Kuner, Christopher/Marelli, Massimo 2020: Handbook on Data Protection in Humanitarian Action, Geneva: International Committee of the Red Cross (ICRC). https://www.icrc.org/en/data-protection-humanitarian-action-handbook (14.04.2021).

Lanz, David/Eleiba, Ahmed 2018: The Good, the Bad and the Ugly. Social Media and Peace Mediation, Policy Brief No.12, swisspeace. https://www.swisspeace.ch/assets/publications/downloads/Policy-Briefs/aa3fc8830f/Social-Media-and-Peace-Mediation-Policy-Brief-12-2018.pdf (14.04.2021).

Laub, Zachary 2019: Hate Speech on Social Media. Global Comparisons, Council on Foreign Relations, Backgrounder, updated 07.06.2019. https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons (14.04.2021).

Mac Ginty, Roger 2017: Peacekeeping and Data, in: International Peacekeeping 24 (5), 695-705.

Mercy Corps 2019: The Weaponization of Social Media, Seattle, Washington: Mercy Corps. https://www.mercycorps.org/sites/default/files/2020-01/Weaponization_Social_Media_FINAL_Nov2019.pdf (14.04.2021).

Naciri, Mohammad 2020: How Women are Fighting for Peace in a Militarised Cyberspace, Thomson Reuters Foundation News, 28.10.2020. https://news.trust.org/item/20201028171445-u9wn2/ (14.02.2021).

Office of the United Nations High Commissioner for Human Rights (OHCHR) 2006: Rule-of-Law Tools for Post-Conflict States (HR/PUB/06/4), New York and Geneva: United Nations.

Oh, Sarah/Adkins, Travis L. 2018: Disinformation Toolkit, Washington, D.C.: Inter Action. https://www.interaction.org/wp-content/uploads/2019/02/InterAction_DisinformationToolkit.pdf (14.04.2021)

Panic, Branka 2020: Ecosystem Mapping. The State of Play and the Path to Creating a Community of Practice, New York: NYU Center on International Cooperation. https://www.alnap.org/system/files/content/resource/files/main/data-peacebuilding-prevention-ecosystem-mapping.pdf (14.04.2021).

Peace Direct 2020: Digital Pathways for Peace, London: Peace Direct. https://www.peacedirect.org/wp-content/uploads/2020/08/PD-LVP-Tech-Report.pdf (14.04.2021).

Puig Larrauri, Helena et al 2015: New Technologies. The Future of Alternative Infrastructures for Peace, Geneva Peacebuilding Platform, White Paper Series No. 20. https://www.gpplatform.ch/sites/default/files/WPS%2020%20-%20New%20Technologies%20-%20Puig%20Larrauri%20-%20Davies%20-%20Ledesma%20-%20Welch_1.pdf (14.04.2021).

Puyosa, Iria 2019: Venezuela's 21st Century Authoritarianism in the Digital Sphere, Policy Brief No. 62. Tokyo: Toda Peace Institute. https://toda.org/assets/files/resources/policy-briefs/t-pb-62_iria-puyosa_venezuelas-21st-century-authoritarianism.pdf (14.04.2021).

Raymond, Nathaniel A. 2017: Beyond 'Do No Harm' and Individual Consent. Reckoning With the Emerging Ethical Challenges of Civil Society's Use of Data, in: Taylor, Linnet/Floridi, Luciano/van der Sloot, Bart (eds.): Group Privacy, Cham: Springer International Publishing AG, 67-82.

Read, Roisin/Taithe, Bertrand/Mac Ginty, Roger 2016: Data Hubris? Humanitarian Information Systems and the Mirage of Technology, in: Third World Quarterly, 37 (8), 1314-1331.

Rio, Victoire 2020: The Role of Social Media in Fomenting Violence. Myanmar, Policy Brief No. 78, Tokyo: Toda Peace Institute. https://toda.org/assets/files/resources/policy-briefs/t-pb-78_victoire-rio_role-of-social-media-in-fomenting-violence-myanmar.pdf (14.04.2021).

Robertson, Danielle/Ayazi, Mena 2019: How Women Are Using Technology to Advance Gender Equality and Peace, Washington, D.C.: United States Institute of Peace, 15.07.2019. https://www.usip.org/publications/2019/07/how-women-are-using-technology-advance-gender-equality-and-peace (14.02.2021).

Schirch, Lisa 2018: Social Media Impacts on Social & Political Goods. A Peacebuilding Perspective, Policy Brief No. 22, Tokyo: Toda Peace Institute.

https://toda.org/assets/files/resources/policy-briefs/t-pb-22_lisa-schirch_social-media-impacts.pdf (14.04.2021).

Schirch, Lisa 2020a: Social Media Impacts on Conflict Dynamics, Policy Brief No. 73, Tokyo: Toda Peace Institute.
https://toda.org/assets/files/resources/policy-briefs/t-pb-73_lisa-schirch_san-diego-report-social-media-impacts-on-conflict-dynamics.pdf (14.04.2021).

Schirch, Lisa 2020b: 25 Spheres of Digital Peacebuilding and PeaceTech, Policy Brief No. 93, Tokyo: Toda Peace Institute.
https://toda.org/assets/files/resources/policy-briefs/t-pb-93_lisa-schirch.pdf (14.04.2021).

SecDev Group 2017: Digitally-Enabled Peace and Security. Reflections for the Youth, Peace and Security Agenda.
https://www.youth4peace.info/system/files/2018-04/2.%20TP_Social%20Media_SecDev.pdf (14.04.2021).

Singh, Spandana 2020: The False Information Ecosystem in India, Policy Brief No. 55, Tokyo: Toda Peace Institute.
https://toda.org/assets/files/resources/policy-briefs/t-pb-55_spandana-singh_the-false-information-ecosystem-in-india.pdf (14.04.2021).

Skopik, Florian/Pahi, Timea 2020: Under False Flag. Using Technical Artifacts for Cyber Attack Attribution, in: Cybersecurity, 3 (8).

Tenove, Chris 2019: Networking Justice. Digitally-Enabled Engagement in Transitional Justice by the Syrian Diaspora, in: Ethnic and Racial Studies, 42 (11), 1950-1969.

United Nations (UN) 2020: Roadmap for Digital Cooperation, Report of the Secretary-General. https://www.un.org/en/content/digital-cooperation-roadmap/ (14.04.2021).

United Nations Department of Political and Peacebuilding Affairs (UNDPPA)/Centre for Humanitarian Dialogue (HD) 2019: Digital Technologies and Mediation in Armed Conflict. https://peacemaker.un.org/sites/peacemaker.un.org/files/DigitalToolkitReport.pdf (14.04.2021).

Uren, Tom/Hogeveen, Bart/Hanson, Fergus 2018: Defining Offensive Cyber Capabilities, Australian Strategic Policy Institute, 04.07.2018.
https://www.aspi.org.au/report/defining-offensive-cyber-capabilities (14.04.2021).

Vosoughi, Soroush/Roy, Deb/Aral, Sinan 2018: The Spread of True and False News Online, in: Science, 359 (6380), 1146-1151.
https://science.sciencemag.org/content/359/6380/1146 (14.04.2021).

Whittaker, Zack 2019: Two Years After WannaCry, a Million Computers Remain at Risk, The Crunch, 12.05.2019.
https://techcrunch.com/2019/05/12/wannacry-two-years-on/ (14.04.2021).

Widmer, Jasmine N./Grossenbacher, Andrea 2019: Information and Communication Technologies in Peacebuilding, swisspeace.
https://www.swisspeace.ch/assets/publications/downloads/Essentials/87df4dac25/Information-and-Communication-Technologies-Essential-1-2019.pdf (15.04.2021).

Wiseman, Jamie 2020: Rush to pass ‘fake news’ laws during Covid-19 intensifying global media freedom challenges, International Press Institute, IPI Newsroom, 22.10.2020.
https://ipi.media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/ (14.04.2021).

Recently Published INEF Reports

Hofstetter, Julia-Silvana: Digital Technologies, Peacebuilding and Civil Society. Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Agenda Forward. Duisburg (INEF Report 114/2021), 32 pp.

Saalfeld, Jannis: Before and Beyond Al-Shabaab: National Islamic Councils, Contentious Politics and the Rise of Jihadism in East Africa. Duisburg (INEF Report 113/2019), 40 pp.

Boege, Volker/Rinck, Patricia/Debiel, Tobias: Local-International Relations and the Recalibration on Peacebuilding Interventions Insights from the 'Laboratory' of Bougainville and Beyond. Duisburg (INEF Report, 112/2017), 57 pp.

Hippler, Jochen: Terrorism. Undefinable and Out-of-Context? Reconceptionalizing Terrorism as a Context-Specific Tactical Tool. Duisburg (INEF-Report, 111/2016), 60 pp.

Tromp, Dylan: Assessing Business-Related Impacts on Human Rights: Indicators and Benchmarks in Standards and Practice. Duisburg (INEF Report, 110/2016), 93 pp.

Hamm, Brigitte/Schax, Anne: Human Rights Due Diligence through Stakeholder Engagement? The Case of a Copper-Gold Mine in the Philippines. Duisburg (INEF Report, 109/2015), 52 pp.

Mußenbrock, Marie-Luise: A (Mis)Alignment of Governance Structures? The Two Water Concessions in Metro Manila. Duisburg (INEF Report, 108/2013), 47 pp.

Wulf, Herbert: India's Aspirations in Global Politics – Competing Ideas and Amorphous Practices. Duisburg (INEF Report 107/2013), 39 pp.

Lambach, Daniel/Bethke, Felix: Ursachen von Staatskollaps und fragiler Staatlichkeit: Eine Übersicht über den Forschungsstand. Duisburg (INEF-Report 106/2012), 48 S.

Hanrath, Jan: Transnationale Migrantengruppen und der Transport von Konflikten – Das Beispiel Türken und Kurden in Berlin. Duisburg (INEF-Report 105/2012), 44 S.

Bueger, Christian/Stockbrügger, Jan/Werthes, Sascha: Strategische Fehler der Pirateriebekämpfung. Somalia, Peacebuilding und die Notwendigkeit einer umfassenden Strategie. Duisburg (INEF-Report 104/2011), 44 S.

Single Copies can be ordered from:
University of Duisburg-Essen, Faculty of Social Sciences,
Institute for Development and Peace, D-47048 Duisburg.
Hardcopies can be ordered for 3.00 Euro (Germany) or 5.00 Euro (Europe) each.
Order forms are available on our homepage.
All INEF Reports can be downloaded for free from our homepage:
https://www.uni-due.de/inef/inef_report_en.php

The Institute for Development and Peace (INEF)

The Institute for Development and Peace (INEF), which was founded in 1990, is part of the Faculty of Social Sciences at the University of Duisburg-Essen. We combine basic with applied research contributing to academic debates as much as to political discussions.

We work on issues at the interface of development and peace. Empirically, we focus on the situation of vulnerable groups in the Global South and structures of violence, poverty and lack of rights. From 2018 to 2021, our academic work focuses on »Ordering and Responsibility in the Shadow of Hierarchies«; with the following research areas: »Transnational Governance and the Responsibility of Private Actors«, »Development Partnerships in Times of SDGs« and »Resistance and Political Ordering«.

A diverse set of third-party funded research projects allow us to generate basic knowledge on politically relevant issues and to collect data as part of our field research. INEF is integrated in a strong and viable international research and collaboration network. We work particularly closely with the Development and Peace Foundation (sef:), Bonn, and the Centre for Global Cooperation Research (Käte Hamburger Kolleg, KHK) at the University of Duisburg-Essen.

The INEF Report series

INEF Report is a series that appears at irregular intervals. It publishes major findings from the institute's ongoing research projects as well as overview studies on academic and policy debates concerning global issues. INEF Reports are primarily addressed to the research community and students of international relations, but also try to reach out to policymakers and practitioners interested in relevant scholarly results.

INEF-Report 114/2021 ISSN 09431-4967

Institute for Development and Peace (INEF) · Lotharstr. 53 · D-47057 Duisburg · inef-sek@uni-due.de · https://www.uni-due.de/inef · Tel +49 (203) 379 4420 · Fax +49 (203) 379 4425