5

Cyber Peace and Intrastate Armed Conflicts

Toward Cyber Peacebuilding?

Jean-Marie Chenou and John K. Bonilla-Aranzales

1 INTRODUCTION

South Africa is a renowned case for its remarkable peacebuilding process that followed the transition from the apartheid era in the 1990s, particularly in terms of reconciliation, restorative justice, forgiveness, and healing from a violent past (Borris, 2002). However, the reconciliation process is ongoing, as seen in the first five days of September 2019 when some xenophobic, looting, and violent attacks emerged in Johannesburg. This time, the victims of those violent attacks were not black South Africans. Instead, the victims were Nigerians who lived and worked in South Africa (Holmes, 2019). This episode of violence could be impacted by different factors, including social media promotion. This example highlights a common feature of online communication in conflict-torn and postconflict societies in various parts of the world. The digital transformation has blurred the boundaries between cyberspace and "physical" space, creating a continuum between online and offline violence. As such, cyberspace has become a realm for political confrontation. Information and data can both be tools to empower dissidents while also being weapons for users, decision makers, governments, and armed groups (Berman, Felter & Shapiro, 2020; Duncombe, 2019). In this context, threats of violence are published on webpages and social media platforms to create and exacerbate a climate of fear. Violence targeted at specific minority groups reproduces offline practices of discrimination and hatred (Alexandra, 2018). Moreover, social media and messaging applications are used to mobilize populations generating large-scale collective actions that have created meaningful changes or call for actions worldwide, such as the cases of the Arab Spring (Salem, 2014), the Black Lives Matter movement in the United States (Zeitzoff, 2017), or the feminist movement in Argentina (Chenou and Másmela, 2019). These dynamics are particularly important in postconflict contexts where new opportunities for truth and reconciliation emerge while conflictual relationship might migrate online.

https://doi.org/10.1017/9781108954341.005 Published online by Cambridge University Press

Many cybersecurity studies focus on state actors and, more specifically, on great powers with strong capacities to conduct cyber operations on a global scale, such as the Stuxnet attack (Valeriano and Maness, 2018), or the digital attack on the Ukrainian power grid in 2015 (Deibert 2018). However, the resolution of intrastate conflict dynamics, which are crucial elements undermining the existence of a sustainable, stable, and secure cyberspace, usually goes ignored. The use and impact of Information and Communication Technologies (ICTs) in cyberspace during intrastate conflicts has also drawn much attention due to its impact, expanding the analysis of the media's role in conflicts. However, cyberspace's role in peacebuilding has been less studied, despite the Tunis Commitment for the Information Society, adopted by the UN in 2005, which acknowledges the potential of ICTs to promote peace by "assisting post-conflict peacebuilding and reconstruction" (United Nations, 2005). As illustrated by the aforementioned South African riots case, the issue of peacebuilding in cyberspace goes beyond access and safe use of technology. It also includes the regulation of violent content and information. This chapter proposes a dialogue between Internet studies and the analysis of peacebuilding to define the notion of cyber-peacebuilding based on the cases of Colombia and South Africa. Drawing upon the four pillars of cyber peace (Shackelford, 2020, preface), it identifies the main venues for cyber peacebuilding research. We propose a working definition of cyber peacebuilding as those activities that delegitimize online violence, build capacity within society to peacefully manage online communication, and reduce vulnerability to triggers that may spark online violence. These efforts include, but are not limited to, the prevention of the use of online violence as a conflict reduction strategy. They also seek to address the structural causes of conflict by eliminating online discrimination, detecting possible threats and power abuses, and promoting inclusion and peaceful communication in cyberspace.

This chapter, organized into three parts, contributes to structuring the emerging field of cyber peacebuilding research. It draws a bridge between cyber peace, understood as a global public good, and its implementation at the national level by drawing on the cases of South Africa and Colombia.

It begins by broadening the perspective of cyber peace studies to include intrastate armed conflicts located mostly in the Global South. The second section outlines the challenges posed by intrastate conflicts for global cyber peace and draws upon cybersecurity and conflict resolution literature to define cyber-peacebuilding. The third section focuses on how the four pillars of cyber peace used as a framework in this volume – namely human rights, access and cybersecurity norms, multistakeholder governance, and stability – can help structure cyber peacebuilding research and even inform policymakers with a particular focus on South Africa and Colombia. Finally, the chapter concludes with the relevance of cyber peacebuilding research and draws some examples for further research on the issue.

2 TOWARD A COMPREHENSIVE CYBER PEACEBUILDING APPROACH

The use of ICTs both affects the dynamics of violent disputes and helps to generate peacebuilding activities (Puig, 2019). The use of these technologies does not follow a deterministic path. Technologies, including social media platforms, provide new ways of communication between parties that could increase harm as well as provide novel forms of cooperation. To better understand their impact, we explore some challenges that intrastate armed conflicts generate in a global scenario, then we discuss the role of cyberspace in internal conflicts. Finally, we propose some ideas about the relevance of cyber peacebuilding based on intrastate conflict resolution scenarios.

Intrastate armed conflicts have emerged as a new complex challenge globally, particularly in the Global South (Pettersson & Öberg, 2020). A substantial increase in intrastate disputes occurred in the post–Cold War period, becoming the most frequent and deadly form of armed conflict in the world (Mason & Mitchell, 2016), with devastating consequences at social and psychological levels (Wallensteen, 2018). Intrastate armed conflict can be defined as civil wars (Sarkees & Wayman, 2010) or understood as asymmetric conflicts (Berman, Felter & Shapiro, 2020). Intrastate armed conflicts include periods of military hostility between government security forces and members of one or more armed opposition groups within a state lasting ten or more days, without regard to the number of fatalities (Mullenbach, 2005). They can be categorized according to the dispute's issue and the rebels' goals, such as ideological revolutions, ethnic revolutions, and secessionist revolts. Moreover, they can be characterized by the causes of their occurrences. Internal armed conflicts can be explained by *greed*, centered on individuals' desire to maximize their profits; *grievance*, where conflict occurs as a response to socioeconomic or political injustice; and *opportunity*, which highlights factors that make it easier to engage in violent mobilizations (Cederman & Vogt, 2017).

The role of cyberspace in internal conflicts can be interpreted as a double-edged sword, as it enhances the interaction between users, digital platforms, and governmental agencies across multiple technological devices. However, the tensions concerning its positive or negative use not only depend on the users, who range from ordinary citizens to political leaders, rebels, and extremist groups, among other societal actors – all of whom interact using ICTs. The social and political contexts of its use are relevant because those conditions allow for the presence of new actors that behave with complex rules, which undoubtedly change the dynamics of civil wars and peacebuilding scenarios. In short, cyberspace matters in the development and ending of intrastate conflicts because they have become information centric (Berman et al., 2020; Steinberg, Loyle, & Carugati, in this volume).

Cyberspace capabilities contribute to the creation and tracking of analytical elements concerning the tensions, positions, narratives, and changes in the domestic balance of power of states and non-state actors. It offers the possibility to develop conflict prevention actions, as discussed in Chapter 4. Moreover, cyberspace represents a nurturing ground that allows for the generation and promotion of conflict

resolution initiatives. As Ramsbotham, Miall, and Woodhouse (2016, p. 432) argued, the "virtual world of cyberspace is, therefore, contested and conflictual in the same way as the 'real' world is, but the challenges are the same in the sense that emancipatory agendas of conflict resolution apply as much to cyber peacemaking as to 'conventional' peacemaking." In short, this digital space represents a hybrid and dynamic environment (Gohdes, 2018), in which uncertainty and threats emerge, but also where the conflicting parties can create peaceful ways to coexist.

The potential for utilizing cyberspace in peacebuilding activities, particularly to enhance the role of mediators and generate policy change, is a positive example of such technologies (Tellidis & Kappler, 2016; Puig Larrauri & Kahl, 2013). A relatively recent development in cyberspace is the emergence of social media, where users can create content and interact across both micro and macro communities (Kaplan & Haenlein, 2012). The use of social media has undoubtedly changed how we communicate and relate to our world. Its negative uses have raised new complex concerns about ethical and security issues. The recruitment of extremists (Weimann, 2016; Walter, 2017), the increasing polarization among the minority groups who are most active in discussions about public affairs (Barberá, 2020), and the promotion of hate speech (Mathew et al., 2019) are some negative uses that heighten conflict dynamics, not only in cyberspace but also in physical space. However, the use of social media also reduces the costs of information distribution in the framework of violent conflict (Hochwald, 2013), which could generate new social mobilizations and reduce collective action problems (Margetts et al., 2015). Additionally, social media can generate new data and information about the conflict environment that might forecast new violent actions. Its use is also a critical factor in the promotion of narratives that could establish peaceful engagement using a bottom-up approach and could even help foster polycentric information sharing, as was discussed in Chapter 3.

Given the background, our definition of cyber peacebuilding draws upon different strands of literature. Previous efforts to analyze the role of ICTs in the termination of conflicts include cyber peacekeeping and the ICTs for peace frameworks. Moreover, we subscribe to the positive definition of peace adopted by cyber peace scholars. Finally, our definition of cyber peacebuilding is based on a contemporary conflict resolution approach that echoes critical cybersecurity perspectives.

Along with the diffusion of interactions into cyberspace in conflict-torn and postconflict countries, the role of ICTs in peacekeeping operations, and as tools to promote peace, has been increasingly acknowledged by scholars and intergovernmental organizations. From the use of big data in peacekeeping operations (Karlsrud, 2014) to the institutionalization of cyber peacekeeping teams and operations in the United Nations, such as the United Nations' Digital Blue Helmets (Almutawa, 2020; Robinson, et al., 2019; Shackelford, 2020), the literature has broadened to include cyberspace in the analysis of peacekeeping. Cyber peacekeeping is an evolution of an idea that emerged in the 1990s, which posited that ICTs could promote peace. During the process that led to the World Summit on Information Society, the idea of ICTs

being used for peace was further developed and included in the Tunis Commitment for the Information Society (United Nations, 2005). However, the use of the concept remained limited in scholarly publications with some exceptions (see Laouris, 2004; Spillane, 2015; Young & Young, 2016) and declined with the massification of social media and the subsequent debate on its role in polarization. While the ICTs for peace scholarship generally focus on access and the infrastructure layer from a techno-optimistic perspective, an analysis of the content layer, and the particular role of social media in conflict and peace dynamics, is a starting point to develop novel inquiries.

Another source of inspiration for cyber peacebuilding is the ongoing effort to promote a positive definition of cyber peace in a scholarly debate primarily dominated by the issue of cyberwar. More specifically, we situate cyber peacebuilding within "the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks." (Shackelford, 2019, p. 163). In this chapter, we propose an analysis of a cyber peacebuilding approach, which mainly focuses on the national level in postconflict contexts, but also includes the participation of local and international actors. Moreover, the analysis of conflictual contexts and peacebuilding in the digital era can help explore new ways to address the increasing polarization at work in mature democracies.

Finally, cyber peacebuilding adopts a human-centered approach and promotes an emancipatory normative stance on the provision of cybersecurity (Collins, 2020). Within this context, cyber peacebuilding is a reformulation and an extension of the definition of peacebuilding adapted to the digital age. Drawing upon the definition of peacebuilding proposed by the Alliance for Peacebuilding (2012), we define cyber peacebuilding as an active concept that captures those activities that delegitimize online violence, build capacity within society to peacefully manage online communication, and reduce vulnerability to triggers that may spark online violence. Some activities involve, but are not limited to, preventing the use of online violence as a conflict strategy and highlighting the role of users, states, and Big Tech companies in this regard. They also seek to address the structural causes of conflict by eliminating online discrimination; enhancing the scope and impact in the territory of peacebuilding mechanisms; and promoting inclusion and peaceful communication in cyberspace. As such, cyber peacebuilding efforts represent an essential stepping stone in the pursuit of cyber peace as a global public good.

Such a focus on cyber peacebuilding is not entirely new (see, e.g., Puig Larrauri & Kahl, 2013; Tellidis & Kapler, 2016; AlDajani & Muhsen, 2020), even though its expression rarely appears as such. This chapter argues that it can be a useful concept for establishing and structuring a scholarly dialogue that explores the multiple dimensions of peacebuilding in cyberspace beyond a liberal approach, which is often limited to the establishment of liberal institutions – democracy, human rights, open economy, and the rule of law (Zaum, 2012). Here, we adopt a comprehensive approach that includes

all activities focused on preventing the causes of violent conflict and strengthen mechanisms to handle conflict in a constructive and nonviolent way (Parlevliet, 2017).

Cyber peacebuilding represents a contribution to global cyber peace from a polycentric approach. Beyond an exclusively top-down perspective on the necessity of global agreements and norms for building a peaceful and stable cyberspace, we adopt a polycentric approach in order to address how local threats to peacebuilding efforts undermine the existence of cyber peace at a global level (for a similar perspective, see Chapter 2). From this perspective, the proliferation of internal armed conflicts requires the construction of peaceful cyber contexts in conflict-torn and postconflict societies.

To further explore the prospects of cyber peacebuilding, we focus on two cases: South Africa and Colombia. With the victory of the African National Congress in the 1994 election, South Africa started a process of transition from the apartheid era, which notably entailed a new constitution and the establishment of a Truth and Reconciliation Commission in 1996. Despite important achievements, the reconciliation process is still ongoing (du Toit, 2017). On the other hand, Colombia has taken a number of major steps toward the termination of a five-decade-long internal conflict. One of the most important was the peace accord of 2016 between the government and the Revolutionary Armed Forces of Colombia (FARC) guerrilla organization. While the two countries are situated at different sites on the conflict/postconflict continuum, they both face the challenges of peacebuilding and reconciliation (Rodríguez-Gómez et al., 2016). Moreover, they are both middle-income and relatively highly digitized countries in the Global South (Chouci and Clark, 2018, p. 163). Also, in both cases, governmental stakeholders have ignored the relevance of cyberspace for the development of peacebuilding actions. Thus, they represent two diverse and interesting cases in which to explore the prospects of cyber peacebuilding.

3 THE FOUR PILLARS OF CYBER PEACEBUILDING

The broad definition of cyber peacebuilding outlined in the previous section encompasses many issues and actors. The four pillars of cyber peace (Shackelford, 2020) provide a framework to structure the analysis. Local threats to cyber peace and cyber peacebuilding efforts can be categorized within the pillars of cyber peace: access and cybersecurity, human rights, multistakeholder governance, and stability (see Figure 5.1).

3.1 *Human Rights, a Call of Action to Update the Social Contract*

The promotion of human rights and peacebuilding mechanisms can be analyzed as joint processes in which peacebuilding insights and methods can advance human rights promotion and protection (Parlevliet, 2017). However, some overlapping tensions must be considered, such as the complicated relationship between freedom of expression and political stability, and the disputes concerning how to handle

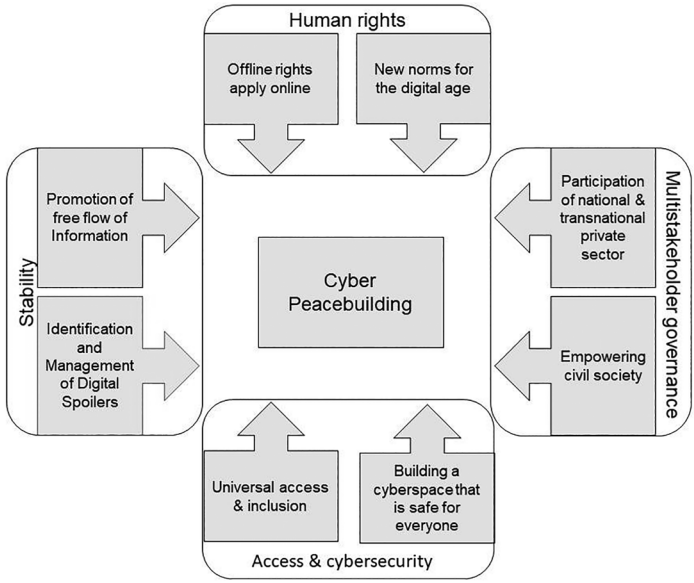

FIGURE 5.1 The contributions of the four pillars of cyber peace to cyber peacebuilding (source: elaborated by the authors [September 21, 2020]).

sensitive issues such hate speech, sexual harassment, and politically driven attacks that foment collective violent responses.

While freedom of expression, privacy, and data protection are covered by International Humanitarian Law and Human Rights Law at the international level (Franklin, 2019; Lubin, 2020), inadequate enforcement mechanisms and profound social issues at the national level, such as a lack of digital literacy and limited Internet access, undermine their implementation (Shackelford, 2019). This difficult adoption of international regulations complicates peacebuilding scenarios because governments regulate freedom of expression to impose an official truth, which sometimes limits the right of expression and association of the opposition sectors. Moreover, in peacebuilding scenarios, some voices, even the official ones, can become radicalized, creating new challenges to stability. In this context, governments can be tempted to prioritize security and stability over freedom of expression and a pluralist dialogue toward peacebuilding.

For example, there is no Internet detailed legal framework in Colombia that guarantees its citizens' fundamental rights in cyberspace. Nevertheless, freedom of speech is viewed comprehensively by the Constitutional Court. It is also backed by Colombia's membership of the Inter-American Human Rights System, which means that this right applies, not only offline, but also in the online world (Dejusticia, Fundación Karisma and Privacy International, 2017). However, the respect of those human rights in cyberspace is often challenged due to the use of a securitization narrative by the current governing party that was an opponent to the peace negotiations

https://doi.org/10.1017/9781108954341.005 Published online by Cambridge University Press

with the FARC rebels. The government perceives peacebuilding as a mere process of disarmament, demobilization, and reintegration of former combatants in order to restore stability. This limited view of the peacebuilding process also justifies the use of online state surveillance actions to guarantee national security, in which political leaders, former government officials, journalists, and humanrights activists are targeted because of their support of the peace agreement (Vyas, 2020). Without a doubt, the respect of human rights in Colombia, through cyberspace interactions, represents a new challenge that has been ignored by policymakers in the reconstruction of the social fabric in this transitional society.

Second, there is a tension in cyberspace on how to handle sensitive issues that could evolve into violent conflicts. In this complex scenario, Big Tech companies play a critical role because they are able to track and censor what people post and share. However, in the Global South, this tension is not a priority (Schia, 2018). On the contrary, Big Tech companies are more concerned with access and digitalization than privacy rights. Many social media companies that operate in developing countries do not have clear policies regarding this issue. Instead, their roles in these societies have been linked to increasing disinformation, inciting violence, and decreasing trust in the media and democratic institutions (Bradshaw & Howard, 2019).

The case of South Africa provides an interesting perspective on the respect of human rights in cyberspace as part of a reconciliation process. Their constitution guarantees the right to freedom of opinion and expression. This topic is mainly addressed under the supervision of the South African Human Rights Commission (SAHRC), which was created by the South African Constitution and the Human Rights Commission Act of 1994. Its aim is linked to promoting human rights through a variety of actions about education and raising community awareness; making recommendations to the Parliament; reviewing legislation; and, most importantly, investigating alleged violations of fundamental rights and assisting those affected to secure redress (Sarkin, 1998). Based on its mandate, this institution had provided significant recommendations in the legislation linked to topics data protection (SAHRC, 2012) and recent cybersecurity issues (SAHRC, 2017). Nevertheless, its main challenge is to address issues concerning hate speech and racism in cyberspace, particularly on social media platforms, in a quick and efficient way. This commission acknowledges the issue, and it has taken some steps to face this challenge recognizing the allegations of racism perpetrated on social media (SAHRC, 2016). Most importantly, it started a multistakeholder dialogue to reach a detailed social media charter, including human rights education at all academic levels, to fight racism in the digital sphere (SAHRC, 2019).

In conclusion, in order to address human rights issues in cyberspace, particularly in peacebuilding scenarios, there is a need for a new social contract that recognizes human rights as digital rights. Human rights are considered a crucial element of peacebuilding, which must include cyberspace activities. To provide an impact on the development of peacebuilding mechanisms, some human rights standards, values, and principles must be included. To accomplish that end, some actions

concerning public policies regarding security and privacy ought to be addressed by governments without exceeding their power. Big Tech companies must provide stricter and more straightforward privacy protocols and conduct codes in layperson's terms based on the local framework in which they operate. Moreover, civil society's role, particularly that of users, must be present to delimitate the scope of the potential legal actions concerning topics linked to privacy rights, freedom of speech, misinformation, and disinformation. This inclusive approach would help to create a healthy environment for the exchange of ideas and information, enabling all members who coexist in a changing society to respect and resolve their differences, even in the context of intrastate armed conflict and peacebuilding scenarios.

3.2 *Multistakeholder Cyber Peacebuilding*

Multistakeholder governance has become a gold standard in Internet governance and regulations of human activities in cyberspace (Scholte, 2020). While not exempt from criticisms in terms of legitimacy and efficiency, the cooperation between public and private actors has become necessary to handle increasingly large amounts of data and regulate private algorithms and infrastructure, leading to a hybridization of governance (Chenou & Radu, 2019).

This hybridization of governance has also transformed the approach to cybersecurity. Cybersecurity, understood as a national security issue, has historically curtailed the space for multistakeholder governance (Dunn Cavelty, 2013; Kuehn, 2014). However, recent developments in the production and governance of cybersecurity showcase different governance structures beyond the hierarchical state-led governance of cybersecurity (Kuerbis & Badiei, 2017; Mueller, 2017; Shires, 2018; Tanczer et al., 2018). A multi-stakeholder governance of cybersecurity is emerging at the global, national, and local levels (Pernice, 2018). According to Pernice, the shared responsibility in the establishment of cybersecurity and cyber peace requires a:

> [...] multilevel and multi-stakeholder system of cybersecurity governance, a system that includes all stakeholders: the individual citizen and civil society, business enterprises, and public authorities, from the local up to the global level (Pernice, 2018, p. 122).

The participation of different sectors in cybersecurity governance is even more important in postconflict contexts, where peacebuilding efforts also require the inclusion of multiple stakeholders (Brzoska et al., 2011; Narten, 2011). Beyond public authorities, three types of actors are of particular importance. First, the private sector plays an essential role in peacebuilding efforts, both during the negotiations and in the implementation of peace agreements (Rettberg, 2007, 2016; Miklian & Schouten, 2019). Second, the media can promote peace and the prevention of incitement to violence (Howard, 2002; Himelfarb & Chabalowski, 2008). Finally, civil society fulfils different functions in peacebuilding, such as: the protection of citizens; the monitoring of human rights violations and the implementation

of peace agreements; advocacy for peace and human rights; socialization to values of peace and democracy; intergroup social cohesion; facilitation of dialogue; and service delivery to create entry points for the other functions (Paffenholz, 2010).

Despite some common requirements and goals, multistakeholder cybersecurity governance and multistakeholder peacebuilding are rarely treated together in practice. For example, South Africa has been one of the pioneering countries and a model of multistakeholder peacebuilding with the establishment of an infrastructure for peace. The 1991 National Peace Accord created Regional and Local Peace Committees that were open to any relevant civil society organization, such as religious organizations, trade unions, business and industry representatives, and traditional authorities (Odendaal, 2010). This multistakeholder infrastructure for peace became a reference for further processes (Preventive Action Working Group, 2015). In 1994, South Africa created the National Economic Development and Labour Council in order to allow for multistakeholder participation in the formulation of economic and social policies. However, multistakeholder participation in the governance of cyberspace is limited in South Africa (Mlonzi, 2017). For example, the National Cybersecurity Policy Framework was drafted under the leadership of the South African Department of Communications between 2009 and 2012, but was later transferred to the Ministry of State Security (Global Partners Digital, 2013). As the responsibility of a civilian Ministry, cybersecurity fell under the category of economic and social policy and was thus, open to multistakeholder participation. However, the leadership of the Ministry of State Security limited the scope of cybersecurity and undermined the participation of diverse stakeholders.

In Colombia, multistakeholder participation became institutionalized in economic and social policies through the Consejo Nacional de Política Económica y Social (National Council of Economic and Social Policy). There is a strong participation of diverse stakeholders in the formulation of Internet governance policies organized around the Mesa Colombiana de Gobernanza de Internet (Colombian Internet Governance Forum). Moreover, the recent peace accord acknowledges that "participation and dialogue between different sectors of society contribute to building trust and promoting a culture of tolerance, respect and coexistence" (República de Colombia, 2016, Introducción, translated by the authors). However, the issue of peacebuilding is hardly included in Internet governance debates that tend to reproduce global discussions. On the other hand, the governance of cyberspace is not among the priorities of peacebuilding efforts beyond the question of access (see the section below).

Multistakeholder cyber peacebuilding represents a step further in the implementation of multistakeholder participation. It requires a multistakeholder dialogue between actors involved in the regulation of cyberspace and the diverse sectors that share a responsibility in peacebuilding activities. The cases of South Africa and Colombia illustrate the necessary participation of social media platforms and search engines in peacebuilding efforts. As the corporate social responsibility of digital platforms in campaigns and elections is being discussed in consolidated democracies, the role of digital platforms in postconflict societies to promote peace and

limit incitement to violence must be put on the agenda. Likewise, the mass media's responsibility in the promotion of a culture of peace is now shared with new media and social media (Stauffacher et al., 2011; Comninos, 2013). As noted by Majcin (2018), modern peace agreements should include the regulation of social media content that may disrupt the peace and promote the resurgence of violence. These rules could even be institutionalized in the form of special commissions to review content on social media and take action when viral publications undermine peacebuilding.

In sum, multistakeholder governance of cyber peacebuilding entails not only the adoption of national cybersecurity policies that allow for the participation and representation of all stakeholders in postconflict societies, it also requires the adoption of multistakeholder mechanisms directly aimed at the promotion of peace and the prevention of violence in cyberspace with the participation of the private sector, digital platforms, academia, and civil society organizations.

3.3 *Redefining Stability in Cyberspace*

To understand the role of stability in cyberspace, we adopt a nuanced definition of stabilization by drawing upon conflict resolution literature to explain how the tensions generated in cyberspace can affect the dynamics and the conclusion of intrastate conflicts and the development of peacebuilding activities.

There are many approaches to the concept of stability to address armed conflicts. They include issues related to statebuilding (Hoddie & Hartzell 2005), international interventions (Belloni & Moro, 2019), and negotiated peace settlements (Hartzell et al., 2001), among other approaches. From the UN Security Council's vision, stability refers to a desired state of affairs, almost as a synonym of "peace" (Kerttunen & Tikk, 2020). Additionally, this concept has a robust state-centric approach (Carter, 2013). To analyze cyberspace's effect in the ending of intrastate conflicts and peacebuilding scenarios, the dynamic definition proposed by Mielke, Mutschler, and Meininghaus (2020) is more useful. They argue that stability is an open-ended and transformative process which accepts changes in social dynamics to keep its forces in equilibrium by constant reconcilement of interests. In a nutshell, the state's role is crucial to address normative rules, but nonstate actors also play a critical role in achieving long-term stability.

Considering that cyberspace is a very dynamic place, stabilization efforts can lead to the transition from intrastate conflicts toward the restoration of the social fabric through peacebuilding actions. This nuanced approach of stability is crucial to understand issues in conflict resolution scenarios, such as the role of spoilers in cyberspace.

Spoilers can be understood as "key individuals and parties to the armed conflict who use violence or other means to shape or destroy the peace process and in doing so jeopardize the peace efforts" (Nilsson & Söderberg, 2011, p. 624; see also Stedman, 1997). This definition serves to understand the impact of those actors in

cyberspace that affect the termination of intrastate conflicts. Digital spoilers are those political actors with relevant influence upon users in cyberspace that exploit their influence to promote violence and spoiling behavior to affect the attempts to achieve peace. They differ from Internet trolls, defined as "unknown online users that create and claim intentionally upsetting statements to enhance strong emotional responses posting offensive or unkind things on the Internet using tactics of disinformation and propaganda" (Petykó, 2018). Digital spoilers are conflicting parties or leaders who use trolling activities, such as the promotion of disinformation and propaganda to affect the achievement of conflict resolution scenarios.

One example of digital spoilers can be found in Colombia, where the opponents of the peace agreement promoted strong and negatively charged hashtags on social media concerning the endorsement of the peace process with the FARC guerilla organization in October 2016 (Nigam et al., 2017). The promotion of these messages, among other factors, affected the perception of the peace negotiations, which was reflected in the rejection of the peace plebiscite by a small margin. The management of spoilers is a daunting task because influential social media platforms users can foment emotions and hostile attitudes against the peacebuilding process. However, these digital spoilers can be tackled when they violate internal regulations of social media platforms (BBC News Mundo, 2019), which highlights the relevance of multistakeholder Internet governance at the national level.

Another relevant example can be found in South Africa, in which political figures use the rhetoric of hate speech toward different communities in order to gain political support (Akhalbey, 2019; Meyer, 2019). The SAHRC has, in the past, analyzed and sanctioned some cases concerning the use of social media to promote hate speech (Geldenhuys and Kelly-Louw, 2020). However, it seems that its mandate does not cover those digital spoilers who express their thoughts in an offensive and disturbing way, pushing the limits of the right to freedom of speech. Their social media statements address critical issues that the peacebuilding process did not solve, such as land reform or race relations, suggesting unpeaceful actions to solve those issues. Additionally, to address the damage that these digital spoilers could make in cyberspace, social media platforms have a key role to play in order to tackle hurtful messages. In this particular case, it seems that there is a misconnection between the conception of the legal rights of freedom of expression provided by the SAHRC and the rules established by social media platforms (Nkanjeni, 2019), which represents a new institutional challenge to address.

In sum, within the framework of cyberspace, stability must be analyzed dynamically. The handling of information plays a critical role because it reflects an age-old tension concerning the relationship between citizens and governments. In that sense, Big Tech companies have become referees and players in a complicated situation. On the one hand, they need to guarantee information and data protection to ensure their legitimacy. On the other hand, they must also respect governmental authority, whose interests are linked to employing surveillance, gathering

data, and performing intelligence through controlled information. Amid intrastate armed conflicts and peacebuilding scenarios, the scope of government surveillance could be enhanced, intensifying asymmetric responses. On the other hand, there are more real threats concerning political motivations to spoil conflict resolution scenarios than the risk of cyberspace's misuse of information beyond the cybersecurity framework. Against this background, the concept of digital spoilers is useful to analyze the behavior of actors whose role could substantially affect the dynamics of stability and conflict resolution efforts. This dynamic approach of stability could lead to the fertile ground to develop cyber peacebuilding actions.

3.4 *Inclusion and Human-Centered Cybersecurity*

Universal Internet access is an enabling condition for cyber peace. It was identified as the first of the five principles for cyber peace by the ITU (International Telecommunication Union, 2011). According to the ITU, providing access to telecommunication technologies is part of the responsibilities of states, which was later translated into the (debated) idea of Internet access as a human right (Tully, 2014). However, the relationship between Internet access and cyber peacebuilding is not direct. Access to the Internet is a necessary, though insufficient, condition to building peace that spans offline and online spaces.

Contrary to the late twentieth century's techno-optimistic visions, the "old" concept of the digital divide remains relevant today (van Dijk, 2020). While early accounts of the digital divide focused on physical access and the divide among countries, contemporary analysis of the digital divide insists on the quality of access and the importance of the gap between Internet access within the same country. This dimension is of utmost importance for cyber peacebuilding (Wilson & Wilson, 2009). Those communities that do not have access to the Internet are generally communities that have been historically marginalized (Tewathia et al., 2020). The digital divide also presents a gender dimension that undermines women's participation in peacebuilding (Njeru, 2009). Moreover, since telecommunication infrastructures are targets and battlegrounds during conflicts, violence-affected regions are likely to suffer from inadequate or unstable connectivity (Onuoha, 2013; Adeleke, 2020). Furthermore, the national digital divide certainly undermines states' capacities and presence on peripheral territories and, subsequently, their legitimacy (Krampe, 2016). This lack of presence and the complicated access to increasingly digitized public services reinforces the perceived abandonment by the states among marginalized communities.

Both South Africa and Colombia have reached significant rates of access at the national level as a result of economic development and ambitious policies. While just over 50 percent of the world population had access to the Internet at the end of 2019 (International Telecommunication Union, 2020), access rates in South Africa were around 65 percent (DANE, 2020; STATSSA, 2020). However, national digital

divides are still important in both countries. For example, over 74 percent of the Gauteng province around Johannesburg and Pretoria benefit from Internet access, compared to just over 46 percent in the poorer province Limpopo, that also has the smallest white South African population in the country (Media Monitoring et al., 2019, p. 12). In Colombia, less than 10 percent of the inhabitants in 700 out of the 1,123 municipalities have Internet access (Quintero & Solano, 2020). These municipalities are located in geographically remote areas that are also the most affected by the internal conflict.

The bridging of the digital divide is related primarily to the telecommunication infrastructure. Another key element is the use of Internet access by individuals and grassroots organizations to participate in the process of peacebuilding through early warnings, grassroots reporting and monitoring, and data collection "from below." Internet access is necessary to engage in political activities, including peacebuilding (Puig Larrauri & Kahl, 2013; Shandler et al., 2019).

While access is a necessary feature to build the conditions for civil society to participate, it is not sufficient to secure meaningful participation. Another crucial condition for cyber peacebuilding is the construction of a cyberspace that is safe for everyone. A broad and emancipatory definition of cybersecurity goes beyond the preservation and defense of critical national infrastructure. It focuses on the general population, both users and nonusers, to build a postconflict cyberspace that is safe for everyone, including former fighters, victims, women, and marginalized communities. However, cybersecurity policies tend to be framed as a response to conflict. For example, research shows that cybersecurity capacity is greater in countries engaged in civil war. However, this capacity seems to aim to crack down on domestic dissent rather than provide secure cyberspace at the national level (Calderaro & Craig, 2020). Even in postconflict contexts, the original state-centered and militarized approach tends to prevail, despite the evolving conditions. As we have seen, the South African National Cybersecurity Policy Framework was first drafted by the Department of Communications. It was later transferred to the Ministry of State Security and finally adopted in 2015 (State Security Agency, 2015). While it briefly mentions "hate speech" and "fundamental rights of South African citizens" (State Security Agency, 2015, pp. 5, 14), the bulk of the document focuses on national security and on the fight against cybercrime. In the same vein, Colombia adopted a Digital Security policy in 2016 that was drafted during the negotiations between the government and the FARC guerrilla organization (CONPES, 2016). However, the document does not mention the postconflict context. It is largely inspired by the OECD discussions on the management of digital risks and thus, focuses on the necessary conditions for the development of trust in Colombian digital markets. On the other hand, the peace accord only mentions ICTs as a way to access public information and public services such as health and education, without acknowledging their role in the peacebuilding process (República de Colombia, 2016).

Contrary to these examples, the institutionalization of cyber peacebuilding should rely on more comprehensive cybersecurity policies that do not reproduce the patterns of great cyber powers to focus on peacebuilding needs in postconflict societies, such as digital literacy and the regulation of hate speech.

4 CONCLUSIONS AND POLICY IMPLICATIONS

South Africa shows us that reconciliation is possible, even in cyberspace. After the violent attacks in Johannesburg mentioned in the chapter introduction, citizens started to promote hashtags and social media campaigns, such as #SayNoToXenophobia, to call for unity, and looking for an end to the violence in this mature peacebuilding scenario (Levitt, 2019). This example also shows us that while cyberspace has undoubtedly affected the dimensions, approaches, and complex dynamics of intrastate conflicts, it can also promote peacebuilding activities to enhance conflict resolution scenarios.

Colombia provides some examples of how transitional justice contributes to cyber peace in terms of Internet access and human rights. Victims and governmental agencies jointly construct the idea of restorative justice through the use of ICTs and digital tools (Chenou, Chaparro-Martínez, & Mora Rubio, 2019). Moreover, this relationship is tested in times of crisis; for example, during the COVID-19 pandemic, where digital tools allow for the continuation of transitional justice (Alfredo Acosta & Zia, 2020). Under certain conditions, the adoption of ICTs by transitional justice tribunals might enhance the efficiency and efficacy of the distribution of justice, allowing both parties to save time by reducing mobilization costs and unnecessary formalities to the minimum. In terms of truth and reconciliation, evidence can be found in the creation of an online news portal that looks to contribute to the reconstruction, preservation, and dissemination of the historical and judicial truth about the Colombian conflict, adopting a bottom-up and in-depth journalism perspective (Verdad Abierta, 2020).

South Africa also provides different examples of cyber peacebuilding. In terms of peaceful social mobilization using ICTs, the use of mobile phones improves organization efficiency, access to information, and strengthens the collective identity of social movements; for example, among members of the Western Cape Anti-Eviction Campaign in 2001 (Chiumbu, 2012). Moreover, in 2015, South African university students protested around the #FeesMustFall hashtag, to demand relevant changes in their education system, such as the decolonization of curricula and a significant increase in government funding for universities (Cini, 2019). But most importantly, with the use of the hashtag #RhodesMustFall, young South Africans provided some analytical elements about how social media could be the way to collectively question the normative memory production to turn the page away from the apartheid era (Bosch, 2017). Despite the criticisms that could be addressed to the SAHRC for the inconsistent sanctioning of hate speech by

political leaders, its contribution to the legislative initiatives concerning data protection, and cybersecurity, respectively, is remarkable (SAHRC, 2012, 2017).

In sum, several contributions to the development of peacebuilding activities are fostered by the linkage between the activities of conflict resolution in cyberspace and in the physical world. This chapter proposed a working definition of cyber peacebuilding in order to provide a broad perspective that reflects changes in the way cyberspace is perceived during interstate armed conflicts and afterwards. ICTs are not only tools, they also constitute and enable the interactions that comprise the lifeblood of cyberspace, transforming the political dynamics of conflict and peacebuilding. Hence, this approach responds to the necessity to implement peacebuilding efforts both in the physical space and in cyberspace. The construction of a stable and lasting peace after intrastate conflicts requires delegitimizing online violence, capacity building within society toward peaceful online communication, and a reduction of the vulnerability to digital spoilers. The structural causes of conflict must also be addressed by eliminating online discrimination and by promoting inclusion and peaceful communication in cyberspace.

The focus on peacebuilding scenarios points to one of the major sources of instability, both online and offline for many countries in the world. While cybersecurity studies tend to focus on state actors that have important capacities, a human-centered perspective on cybersecurity and cyber peace must address the digital dimension of intrastate conflicts as is discussed further in the essays section by the Cyberpeace Institute.

Most intrastate conflicts take place in the Global South. As the majority of Internet users are now located in the Global South, the combination of ICTs and intrastate conflicts is undermining the efforts toward global cyber peace. However, cyberthreats in the Global South are less visible than in the Global North. The focus on commercial threats and on powerful countries obscures the prevalence of cyberthreats against civil society and in the Global South (Maschmeyer et al., 2020). We argue that the concept of cyber peacebuilding sheds light on the relationship between intrastate conflict and global cyber peace and thus contributes to raising awareness about cyberthreats in the Global South.

The four pillars of cyber peace provide a framework to outline comprehensive cyber peacebuilding efforts. As illustrated by Figure 5.1, they highlight the importance of existing human rights and the necessity to create new norms for the digital age. The pillar of multistakeholder governance sheds light on the role of the private sector, and especially of digital platforms and Big Tech companies, along with civil society, to complement and monitor efforts by states and intergovernmental organizations. Stability in postconflict cyberspace can be implemented through the promotion and preservation of a free flow of information and through the identification and management of digital spoilers that undermine the establishment of peace. Finally, the pillar of access and cybersecurity is particularly important in conflict-prone societies where exclusion and marginalization fuel violence. Moreover,

cybersecurity must be understood beyond the implementation by the state of a public policy aimed at the protection of national infrastructure and at the management of digital risk. A human-centered approach is necessary in order to build a cyberspace that is safe for everyone.

This preliminary overview of the different dimensions of cyber peacebuilding in the Colombian and South African cases paves the way for further research on the centrality of cyberspace in the termination of contemporary intrastate conflicts, and for the construction of a stable and lasting peace at a global level. Moreover, it identifies venues for political action. States and international organizations must design new norms of human rights for the digital age along with comprehensive and human-centered cybersecurity policies. Capacity building can empower civil society, foster a safe use of technology, and promote peaceful communication and a culture of peace in cyberspace. Finally, the necessary role of digital platforms must be addressed in order to achieve a meaningful participation and a partnership with states and intergovernmental organizations to tackle online violence.

REFERENCES

Adeleke, R. (2020). Digital divide in Nigeria: The role of regional differentials. *African Journal of Science, Technology, Innovation and Development*, https://doi.org/10.1080/20421338.2020.1748335

Akhalbey, F. (2019). Julius Malema Blames Whites for ongoing xenophobia against African migrants in South Africa. *Face2faceafrica*. Retrieved from: face2faceafrica.com/article/julius-malema-blames-whites-for-ongoing-xenophobia-against-african-migrants-in-south-africa-video [Accessed December 20, 2020].

AlDajani, M. I. (2020). *Internet communication technology (ICT) for reconciliation*. Cham: Springer.

Alfredo Acosta, A., & Zia, M. (2020, June 12). Digital transitions in transitional justice. *DeJusticia*. Retrieved from: www.dejusticia.org/en/column/digital-transitions-in-transitional-justice/

Alexandra, S. (2018). Facebook admits it was used to incite violence in Myanmar. *New York Times*. Retrieved from: www.nytimes.com/2018/11/06/technology/myanmar-facebook.html [Accessed October 5, 2019].

Alliance for Peacebuilding. (2012). *Peacebuilding 2.0: Mapping the boundaries of an expanding field*. Washington, DC: United States Institute of Peace. Fall 2012.

Almutawa, A. (2020). Designing the organisational structure of the UN cyber peacekeeping team. *Journal of Conflict & Security Law*, 25(1), 117–147. https://doi.org/10.1093/jcsl/krz024

Barberá, P. (2020). Social media, echo chambers, and political polarization. In N. Persily, & J. Tucker (Eds.), *Social media and democracy: The state of the field, prospects for reform* (pp. 34–55). Cambridge: Cambridge University Press.

BBC News Mundo. (2019). Álvaro Uribe Denuncia Que Su Cuenta De Twitter Fue "Bloqueada" Durante La Jornada Del Paro Nacional En Colombia. *BBC Mundo*. Retrieved from: www.bbc.com/mundo/noticias-america-latina-50511205 [Accessed September 21, 2020].

Belloni, R., & Moro, F. N. (2019). Stability and Stability Operations: Definitions, Drivers, Approaches. *Ethnopolitics*, 18(5), 445–461. https://doi.org/10.1080/17449057.2019.1640503

Berman, E., Felter, J. H., & Shapiro, J. N. (2020). *Small Wars, Big Data: The Information Revolution in Modern Conflict*. Princeton, NJ: Princeton University Press.

Borris, E. R. (2002). Reconciliation in post conflict peacebuilding: Lessons learned from South Africa? *Second track/citizens' diplomacy: concepts and techniques for conflict transformation*. Lanham, MD and Oxford, 161–181.

Bosch, T. (2017). Twitter activism and youth in South Africa: The case of# RhodesMustFall. *Information, Communication & Society*, *20*(2), 221–232.

Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*. Project on Computational Propaganda. Oxford Internet Institute. University of Oxford. Retrieved from: comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Brzoska, M., Ehrhart, H.-G., & Narten, J. (Eds.). (2011). *Multi-stakeholder security partnerships: A critical assessment with case studies from Afghanistan, DR Congo and Kosovo*. Baden-Baden: Nomos.

Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938.

Carter, W. (2013). War, peace and stabilisation: Critically reconceptualising stability in Southern Afghanistan. *Stability: International Journal of Security & Development*, *2*(1), 15–35.

Cederman, L. E., & Vogt, M. (2017). Dynamics and logics of civil war. *Journal of Conflict Resolution*, *61*(9), 1992–2016.

Chenou, J. M., Chaparro-Martínez, L. P., & Mora Rubio, A. M. (2019). Broadening conceptualizations of transitional justice through using technology: ICTs in the context of justicia y Paz in Colombia. *International Journal of Transitional Justice*, *13*(1), 92–104.

Chenou, J. M., & Cepeda-Másmela, C. (2019). # NiUnaMenos: Data Activism from the Global South. *Television & New Media*, *20*(4), 396–411.

Chenou, J. M., & Radu, R. (2019). The "right to be forgotten": Negotiating public and private ordering in the European Union. *Business & Society*, *58*(1), 74–102.

Chiumbu, S. (2012). Exploring mobile phone practices in social movements in South Africa–the Western Cape Anti-Eviction Campaign. *African Identities*, *10*(2), 193–206.

Choucri, N., & Clark, D. D. (2018). *International relations in the cyber age: The co-evolution dilemma*. Information Policy.

Cini, L. (2019). Disrupting the Neoliberal university in South Africa: The# FeesMustFall Movement in 2015. *Current Sociology*, *67*(7), 942–959.

Collins, A. (2020). Critical human security and cyberspace: Enablement besides constraint. In M. Salminen, G. Zojer, & K. Hossain (Eds.), *Digitalisation and human security. A multi-disciplinary approach to cybersecurity in the European High North* (pp. 83–109). Cham: Springer.

CONPES. (2016). *Política nacional de seguridad digital*. CONPES No. 3854. Bogotá, DC: Consejo Nacional de Política Económica y Social. Available at: colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Comninos, A. (2013). *The role of social media and user-generated content in post-conflict peacebuilding*. Washington, DC: World Bank.

DANE. (2020). *Indicadores básicos de TIC en Hogares*. Bogotá, DC: Departamento Administrativo Nacional de Estadísticas. Available at: www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-hogares

Dejusticia, Fundación Karisma, & Privacy International. (2017). *The right to privacy in Colombia stakeholder report universal periodic review 30th session – Colombia*. Retrieved from: uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=5412&file=English Translation

Deibert, R. (2018). Trajectories for future cybersecurity research. In *The Oxford handbook of international security*. Oxford, UK: Oxford University Press.

van Dijk, J. (2020). *The digital divide*. Hoboken, NJ: John Wiley & Sons.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

du Toit, F. (2017). A broken promise? Evaluating South Africa's reconciliation process twenty years on. *International Political Science Review*, *38*(2), 169–184. https://doi.org/10.1177/0192512115594412

Duncombe, C. (2019). The politics of Twitter: Emotions and the power of social media. *International Political Sociology*, *13*(4), 409–429.

Franklin, M. I. (2019). Human rights futures for the internet. In B. Wagner, M. Kettemann, & K. Vieth (Eds.), *Research handbook on human rights and digital technology* (pp. 5–23). Cheltenham, UK: Edward Elgar Publishing.

Geldenhuys, J., & Kelly-Louw, M. (2020). Demistifying hate speech under the PEPUDA. *Potchefstroom Electronic Law Journal*, *23*, 1–50.

Global Partners Digital. (2013). *Internet governance. Towards greater understanding of global south perspectives*. May 2013 Report. London: Global Partners Digital.

Gohdes, A. R. (2018). Studying the internet and violent conflict. *Conflict Management and Peace Science*, *35*(1), 89–106.

Hartzell, C., Hoddie, M., & Rothchild, D. (2001). Stabilizing the peace after civil war: An investigation of some key variables. *International Organization*, *55*(1), 183–208.

Himelfarb, S., & Chabalowski, M. (2008). *Media, conflict prevention and peacebuilding: Mapping the edges*. Washington, DC: United States Institute of Peace.

Hochwald, T. (2013). How do social media affect intra-state conflicts other than war? *Connections*, *12*(3), 9–38.

Hoddie, M., & Hartzell, C. (2005). Signals of reconciliation: Institution-building and the resolution of civil wars. *International Studies Review*, *7*(1), 21–40.

Holmes, C. (2019). *What's behind South Africa's xenophobic violence last week?* The Washington Post. www.washingtonpost.com/politics/2019/09/09/whats-behind-south-africas-xenophobic-violence-last-week/

Howard, R. (2002). *An operational framework for media and peacebuilding*. Vancouver, BC: Institute for Media, Policy and Civil Society.

International Telecommunication Union. (2011). *The quest for cyber peace*. Geneva, January 2011. Retrieved from: handle.itu.int/11.1002/pub/803f9a60-en

International Telecommunication Union. (2020). *Statistics*. Available at: www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Kaplan, A. M., & Haenlein, M. (2012). Social media: Back to the roots and back to the future. *Journal of Systems and Information Technology*, *14*(2), 101–104.

Karlsrud, J. (2014). Peacekeeping 4.0: Harnessing the potential of big data, social media, and cyber technologies In J. F. Kremer, & B. Müller (Eds.), *Cyberspace and international relations. Theory prospects and challenges* (pp. 141–160). Springer.

Kerttunen, M., & Tikk, E. (2020). The Politics of stability: Cement and change in cyber affairs. In E. Tikk, & M. Kerttunen (Eds.), *Routledge handbook of international cybersecurity*. Oxford, UK: Routledge.

Krampe, F. (2016). Empowering peace: Service provision and state legitimacy in Nepal's peace-building process. *Conflict, Security & Development*, *16*(1), 53–73. https://doi.org/10.1080/14678802.2016.1136138

Kuehn, A. (2014). Extending cybersecurity, securing private internet infrastructure: The US Einstein program and its implications for internet governance. In R. Radu, J. M. Chenou, & R. Weber (Eds.), *The evolution of global internet governance. Principles and policies in the making* (pp. 157–167). Springer.

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance*, *19*(6), 466–492. https://doi.org/10.1108/DPRG-05–2017-0024

Laouris, Y. (2004). Information technology in the service of peacebuilding: The case of cyprus. *World Futures*, *60*(1–2), 67–79. https://doi.org/10.1080/725289197

Levitt, J. (2019, September 4). #SayNoToXenophobia calls for unity as looting and violence rock SA. TimesLIVE. Retrieved from: www.timeslive.co.za/news/south-africa/2019-09-04-saynotoxenophobia-calls-for-unity-as-looting-and-violence-rock-sa/

Lubin, A. (2020). The rights to privacy and data protection under international humanitarian law and human rights Law. Asaf Lubin, the rights to privacy and data protection under international humanitarian law and human rights law. In R. Kolb, G. Gaggioli, & P. Kilibarda (Eds.), *Research handbook on human rights and humanitarian law: Further reflections and perspectives*. Edward Elgar(forthcoming).

Majcin, J. (2018). Social media challenges to peace-making and what can be done about them. *Groningen Journal of International Law*, *6*(2), 242–255.

Margetts, H., John, P., Hale, S., & Yasseri, T. (2015). *Political turbulence: How social media shape collective action*. Princeton, NJ: Princeton University Press.

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2020). A tale of two cybers – how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*. Latest articles, 1–20. https://doi.org/10.1080/19331681.2020.1776658

Mason, T. D., & Mitchell, S. M. (Eds.). (2016). *What do we know about civil wars?* Lanham, MD: Rowman & Littlefield.

Mathew, B., Dutt, R., Goyal, P., & Mukherjee, A. (2019). Spread of hate speech in online social media. In Proceedings of the 10th ACM conference on web science (pp. 173–182).

Media Monitoring Africa, South African National Editors' Forum, Interactive Advertising Bureau of South Africa, Association for Progressive Communications. (2019). *Universal access to the internet and free public access in South Africa*. A Seven-Point Implementation Plan. September, 2019. Available at: internetaccess.africa/wp-content/uploads/2019/10/UA-Report.pdf

Meyer, D. (2019). Julius Malema's 'dead white man' tweet is hate speech, says SAHRC. *Sowetan Live*. Retrieved from: www.sowetanlive.co.za/news/south-africa/2019-09-17-julius-malemas-dead-white-man-tweet-is-hate-speech-says-sahrc/?fbclid=IwAR33FjAxA4L5inYf4njbd--mvVfcxy_AZMS7yvRa4lJWZeQxftfRFOWjPUQ

Mielke, K., Mutschler, M., & Meininghaus, E. (2020). For a dynamic approach to stabilization. *International Peacekeeping*, *27*(5), 810–835. https://doi.org/10.1080/13533312.2020.1733424

Miklian, J., & Schouten, P. (2019). Broadening 'business', widening 'peace': A new research agenda on business and peace-building. *Conflict, Security & Development*, *19*(1), 1–13. https://doi.org/10.1080/14678802.2019.1561612

Mlonzi, Y. (2017). South Africa and internet governance: Are we just ticking a box? *Global information society watch 2017: National and regional internet governance forum initiatives*. Association for Progressive Communications.

Mueller, M. (2017). Is cybersecurity eating Internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415–428. https://doi.org/10.1108/DPRG-05-2017-0025

Mullenbach, M. J. (2005). Deciding to keep peace: An analysis of international influences on the establishment of third-party peacekeeping missions. *International Studies Quarterly*, *49*(3), 539–540.

Narten, J. (2011). Multi-stakeholder security partnerships: Characteristics, processes, dilemmas and impacts. In M. Brzoska, H.-G. Ehrhart, & J. Narten (Eds.), *Multi-stakeholder security partnerships* (pp. 15–37). Baden-Baden: Nomos.

Nkanjeni, U. (2019). Twitter rules Malema's 'only trust a dead white man' Mugabe tribute not violent, despite outrage. *Sunday Times*. Retrieved from: www.timeslive.co.za/news/south-africa/2019-09-17-twitter-rules-malemas-only-trust-a-dead-white-man-mugabe-tribute-not-violent-despite-outrage/

Nigam, A., Dambanemuya, H. K., Joshi, M., & Chawla, N. V. (2017). Harvesting social signals to inform peace processes implementation and monitoring. *Big Data*, *5*(4), 337–355.

Nilsson, D., & Söderberg Kovacs, M. (2011). Revisiting an elusive concept: A review of the debate on spoilers in peace processes. *International Studies Review*, *13*(4), 606–626.

Njeru, S. (2009). Information and communication technology (ICT), gender, and peacebuilding in Africa: A case of missed connections. *Peace and Conflict Review*, *3*(2), 32–40.

Odendaal, A. (2010). *An architecture for building peace at the local level: A comparative study of local peace committees*. New York: UNDP.

Onuoha, F. (2013). *Boko Haram: Anatomy of a crisis*, 1–91. Bristol, UK: e-international relations press. Retrieved from: https://reliefweb.int/report/nigeria/boko-haram-anatomy-crisis

Paffenholz, T. (Ed.). (2010). *Civil society & peacebuilding: A critical assessment*. Boulder, CO: Lynne Rienner.

Parlevliet, M. (2017). Human rights and peacebuilding: Complementary and contradictory, complex and contingent. *Journal of Human Rights Practice*, *9*(3), 333–357. https://doi.org/10.1093/jhuman/hux032

Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism*, *7*(1), 112–141.

Pettersson, T., & Öberg, M. (2020) Organized violence, 1989–2019. *Journal of Peace Research*, *57*(4), 597–613.

Petykó, M. (2018). Troll. In B. Warf (Ed.) *The SAGE encyclopedia of the internet* (pp. 880–882). Thousand Oaks, CA: SAGE Publications.

Preventive Action Working Group. (2015). *Multi-stakeholder processes for conflict prevention and peacebuilding: A manual*. The Hague: Global Partnership for the Prevention of Armed Conflict.

Puig Larrauri, H., & Kahl, A. (2013). Technology for peacebuilding. *Stability: International Journal of Security & Development*, *2*(3), 1–15. https://doi.org/10.5334/sta.cv

Puig, H. (2019). Social networks: Fuel to conflict and tool for transformation. *Peace in progress, 36*. Barcelona: ICIP. www.icipperlapau.cat/numero36/articles_centrals/article_central_7

Quintero, R., & Solano, Y. (2020). *Estudiar en línea en Colombia es un privilegio*. El Tiempo, June 30, 2020. Available at: www.eltiempo.com/datos/asi-es-la-conexion-a-internet-en-colombia-510592

Ramsbotham, O., Miall, H., & Woodhouse, T. (2016). *Contemporary conflict resolution*, 4th ed., Cambridge, UK: Polity.

República de Colombia. (2016). *Acuerdo Final para la terminación del conflicto y la construcción de la Paz Estable y Duradera en Colombia*. November 24, 2016.
Rettberg, A. (2007). The private sector and peace in El Salvador, Guatemala, and Colombia. *Journal of Latin American Studies*, 39(3), 463–494.
Rettberg, A. (2016). Need, creed, and greed: Understanding why business leaders focus on issues of peace. *Business Horizons*, 59(5), 481–492.
Rodríguez-Gómez, D., Foulds, K., & Sayed, Y. (2016). Representations of violence in social science textbooks: Rethinking opportunities for peacebuilding in the Colombian and South African post-conflict scenarios. *Education as Change*, 20(3), 76–97.
Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2019). Developing cyber peacekeeping: Observation, monitoring and reporting. *Government Information Quarterly*, 36(2), 276–293.
Salem, S. (2014). *The 2011 Egyptian uprising. Framing events through the narratives of protesters. Revolution as a process. The case of the Egyptian uprising*. Bremen, Germany: Wiener Verlag für Sozialforschung, 21–47.
Sarkees, M. R., & Wayman, F. W. (2010). *Resort to war: A data guide to inter-state, extra-state, intra-state, and non-state wars, 1816–2007*. Washington, DC: SAGE Publications.
Sarkin, J. (1998). The development of a human rights culture in South Africa. *Human Rights Quarterly*, 20(3), 628–65.
Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly*, 39(5), 821–837.
Scholte, J. A. (2020). Multistakeholderism: Filling the global governance gap? *Global challenges foundation*, April 2020. Retrieved from: globalchallenges.org/wp-content/uploads/Research-review-global-multistakeholderism-scholte-2020.04.06.pdf
Shackelford, S. J. (2019). Should Cybersecurity be a human right: Exploring the shared responsibility of cyber peace. *Stanford Journal of International Law*, 55(1), 155.
Shackelford, S. J. (2020). *Inside the global drive for cyber peace (April 15, 2020)*. Retrieved from SSRN:ssrn.com/abstract=3577161orhttps://doi.org/10.2139/ssrn.3577161
Shandler, R., Gross, M. L., & Canetti, D. (2019). Can you engage in political activity without internet access? The social effects of internet deprivation. *Political Studies Review*, https://doi.org/10.1177/1478929919877600
Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. *Politics and Governance*, 6(2), 31–40.
South African Human Rights Commission. (2012). *SAHRC statement on latest developments regarding the protection of state information bill*. www.sahrc.org.za/index.php/sahrc-media/news-2/item/151-sahrc-statement-on-latest-developments-regarding-the-protection-of-state-information-bill
South African Human Rights Commission. (2016). *Human rights advocacy and communications report 2015–2016*. www.sahrc.org.za/home/21/files/29567%20A4%20adv%20report%20FINAL%20FOR%20PRINT.pdf
South African Human Rights Commission. (2017). *Submission on the cybercrimes and cybersecurity bill [B6-2017]*. www.sahrc.org.za/home/21/files/SAHRC%20Submission%20on%20Cybercrimes%20and%20Cybersecurity%20Bill-%20Aug%202017.pdf
South African Human Rights Commission. (2019). *Stakeholder dialogue on racism and social media in South Africa*. www.sahrc.org.za/home/21/files/Racism%20and%20Social%20Media%20Report.pdf
Spillane, J. (2015). ict4p: Using information and communication technology for peacebuilding in Rwanda. *Journal of Peacebuilding & Development*, 10(3), 97–103.
State Security Agency. (2015). *The national cybersecurity policy framework*. SA Government Gazette No. 39475. December 4, 2015.

STATSSA. (2020). *General household survey 2018*. Pretoria: Statistics South Africa. Available at: www.statssa.gov.za/publications/P0318/P03182018.pdf

Stauffacher, D., Weekes, B., Gasser, U., Maclay, C., & Best, M. (Eds.). (2011). *Peacebuilding in the information age. Shifting hype from reality*. Geneva: ICT4Peace Foundation.

Stedman, S. J. (1997). Spoiler Problems in Peace Processes. *International Security*, *22*(2), 5–53.

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRT s and global cybersecurity: How technical experts support science diplomacy. *Global Policy*, *9*(3), 60–66.

Tellidis, I., & Kappler, S. (2016). Information and communication technologies in peacebuilding: Implications, opportunities and challenges. *Cooperation and Conflict*, *51*(1), 75–93. https://doi.org/10.1177/0010836715603752

Tewathia, N., Kamath, A., & Ilavarasan, P. V. (2020). Social inequalities, fundamental inequities, and recurring of the digital divide: Insights from India. *Technology in Society*, *61*(1), 1–11.

Tully, S. (2014). A human right to access the Internet? Problems and prospects. *Human Rights Law Review*, *14*(2), 175–195.

United Nations. (2005). *Tunis commitment on the information society*. WSIS-05/TUNIS/DOC/7-E. 18 November 2005. Retrieved from: www.itu.int/net/wsis/docs2/tunis/off/7.html

Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security. *The Oxford Handbook of International Political Theory*, 259.

Verdad Abierta. (2020, September 25). *Quienes somos*. Retrieved from: verdadabierta.com/quienes-somos/

Vyas, K. (2020). *Colombian intelligence unit used U.S. equipment to spy on politicians, journalists*. Retrieved from: www.wsj.com/articles/colombian-intelligence-unit-used-u-s-equipment-to-spy-on-politicians-journalists-11588635893

Wallensteen, P. (2018). *Understanding conflict resolution*. Washington, DC: SAGE Publications.

Walter, B. F. (2017). The new civil wars. *Annual Review of Political Science*, *20*, 469–486.

Weimann, G. (2016). The emerging role of social media in the recruitment of foreign fighters. In A. de Guttry, F. Capone, & C. Paulussen (Eds.), *Foreign fighters under international law and beyond* (pp. 77–95). The Hague: TMC Asser Press.

Wilson, J., & Wilson, H. (2009). Digital divide: Impediment to ICT and peace building in developing countries. *American Communication Journal*, *11*(2), 1–9.

Young, O., & Young, E. (2016). Technology for peacebuilding in divided societies: *ICTs and peacebuilding in Northern Ireland. TRANSCOM (Transformative Connections)*.

Zaum, D. (2012). Beyond the "liberal peace". *Global Governance: A Review of Multilateralism and International Organization*, *18*(1), 121–132.

Zeitzoff, T. (2017). How social media is changing conflict. *Journal of Conflict Resolution*, *61*(9), 1970–1991.